IPFire Intrusion Prevention Alert Report

ipfire-test2.localdomain

26 October 2025

Generated 27 October 2025 11:03

Alert Summary

This is a summary of all alerts of High Severity.

	Signature	Total Hits
	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain Activity: 2025-10-26 - 2025-10-26	417
	ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394) [1:2044008:2] - Attempted Administrator Privilege Gain Activity: 2025-10-26 - 2025-10-26	1

Alerts from Sunday, 26 October 2025

Time	Signature	Protocol	Source / Destination
00:00:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.15:26200 172.28.1.7:21315
00:00:32	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.212:52744 172.28.1.7:50116
00:02:23	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.18:49539 172.28.1.7:33244
00:02:37	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	TCP	47.91.30.193:46170 172.28.1.7:10028
00:02:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:3395
00:02:44	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.175.52:49622 172.28.1.7:8090
00:03:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.237:53412 172.28.1.7:8005
00:03:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:9140
00:04:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:49502
00:04:31	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.91.249:54526 172.28.1.7:9515
00:04:45	ET CINS Active Threat Intelligence Poor Reputation IP group 89 [1:2403388:104040] - Misc Attack	TCP	54.196.48.232:51927 172.28.1.7:2181
00:05:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:43389
00:05:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:7801
00:06:42	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:30878 172.28.1.7:11288
00:07:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	147.185.132.27:55342 172.28.1.7:88
00:08:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.186:2438 172.28.1.7:443
00:09:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.193:55020 172.28.1.7:4432
00:09:58	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.169:49817 172.28.1.7:3078
00:11:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.76:49158 172.28.1.7:60000
00:11:38	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.71:50638 172.28.1.7:45085
00:11:43	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.57:51560 172.28.1.7:9704
00:12:28	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.5:52067 172.28.1.7:9127
00:12:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.248:56226 172.28.1.7:8000

	Time	Signature	Protocol	Source / Destination
	00:13:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.221:57305 172.28.1.7:22000
	00:13:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.138:54073 172.28.1.7:38520
	00:13:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.8:51708 172.28.1.7:8595
	00:13:47	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.42.134:50167 172.28.1.7:8846
	00:14:38	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.170:49888 172.28.1.7:16097
	00:14:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.245:49969 172.28.1.7:9168
	00:17:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.209:55640 172.28.1.7:49846
	00:17:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.195:55129 172.28.1.7:2160
	00:20:21	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.30:60729 172.28.1.7:5660
	00:21:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:785
	00:21:17	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.246:50966 172.28.1.7:51805
	00:21:30	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.188.81.67:33843 172.28.1.7:9200
	00:21:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8800
	00:21:39	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8800
	00:22:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	118.196.23.222:38278 172.28.1.7:22
	00:22:53	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.115:49538 172.28.1.7:48289
	00:23:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.179:57138 172.28.1.7:8888
	00:23:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:3176
	00:24:11	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.65.195.53:55375 172.28.1.7:8983
	00:24:18	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.139.32.206:57460 172.28.1.7:445
	00:26:18	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.220:54541 172.28.1.7:9719
	00:27:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:42802 172.28.1.7:427
	00:28:06	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	UDP	47.251.36.190:54779 172.28.1.7:427
	00:29:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.235:54705 172.28.1.7:51200

	Time	Signature	Protocol	Source / Destination
	00:29:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.64:56923 172.28.1.7:5903
	00:30:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.66:53521 172.28.1.7:444
	00:30:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.159:51005 172.28.1.7:22
	00:31:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.126:53122 172.28.1.7:9083
	00:31:32	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.126:53122 172.28.1.7:9083
	00:31:36	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	109.125.139.68:40038 172.28.1.7:1433
	00:31:40	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:56606 172.28.1.7:888
	00:32:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:1291
	00:32:28	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.131:50472 172.28.1.7:45118
	00:32:43	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.237.173.220:34227 172.28.1.7:5800
	00:32:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.106:25404 172.28.1.7:54175
	00:32:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.22:16086 172.28.1.7:6881
	00:33:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.245:55670 172.28.1.7:5061
	00:33:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.191:9770 172.28.1.7:5984
	00:33:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.145:25833 172.28.1.7:83
	00:33:28	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.30:50918 172.28.1.7:46874
	00:33:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.88:49915 172.28.1.7:20257
	00:34:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.108:52742 172.28.1.7:2083
	00:34:35	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.106.206.47:41755 172.28.1.7:8945
	00:34:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:12255
	00:34:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.204:51994 172.28.1.7:500
	00:35:32	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.213:42675 172.28.1.7:443
	00:36:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.56:50620 172.28.1.7:10443
	00:36:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.205:53720 172.28.1.7:46522

	Time	Signature	Protocol	Source / Destination
	00:37:12	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	40.124.186.100:50865 172.28.1.7:3306
	00:37:12	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.186.100:50865 172.28.1.7:3306
	00:37:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.155:46733 172.28.1.7:60443
	00:38:22	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:48797 172.28.1.7:8015
	00:38:23	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.123:49858 172.28.1.7:8141
	00:38:36	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.121.140:57633 172.28.1.7:2525
	00:38:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.229:49397 172.28.1.7:8333
	00:38:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.87:54198 172.28.1.7:3975
	00:39:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:8150
	00:39:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.58:52191 172.28.1.7:9042
	00:39:25	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.52:43225 172.28.1.7:60000
	00:39:48	ET CINS Active Threat Intelligence Poor Reputation IP group 57 [1:2403356:104040] - Misc Attack	TCP	39.107.103.199:33916 172.28.1.7:6379
	00:39:50	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:51957 172.28.1.7:110
	00:40:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.221:50419 172.28.1.7:118
	00:40:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:17774
	00:40:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:38510 172.28.1.7:10116
	00:41:16	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:35030 172.28.1.7:8181
	00:41:23	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.64:53054 172.28.1.7:24443
	00:41:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.245:37974 172.28.1.7:9923
	00:41:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.11:30991 172.28.1.7:554
	00:41:54	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	UDP	20.168.7.214:37767 172.28.1.7:15672
	00:42:27	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:26200 172.28.1.7:55081
	00:42:46	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:34656 172.28.1.7:9080
	00:43:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.240:52620 172.28.1.7:443

	Time	Signature	Protocol	Source / Destination
	00:43:11	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.169.104.218:43333 172.28.1.7:427
	00:43:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9323
	00:43:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:34959 172.28.1.7:4371
	00:43:39	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	47.251.92.52:54595 172.28.1.7:161
	00:43:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.190:56102 172.28.1.7:1194
	00:44:11	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.163.6.253:35691 172.28.1.7:11740
	00:44:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.145:49311 172.28.1.7:9431
	00:44:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.78:49188 172.28.1.7:68
	00:44:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:46925 172.28.1.7:30038
	00:44:59	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:8436
	00:45:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.171:49242 172.28.1.7:993
	00:46:18	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.116:50100 172.28.1.7:9891
	00:46:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.231:42802 172.28.1.7:60000
	00:46:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:19222
	00:47:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:58046 172.28.1.7:22
	00:47:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.132:55458 172.28.1.7:50995
	00:47:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.157:4723 172.28.1.7:2380
	00:47:51	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.208:53411 172.28.1.7:48946
	00:48:22	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:49453 172.28.1.7:91
	00:48:39	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5060 172.28.1.7:5060
	00:48:39	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5060 172.28.1.7:5060
	00:49:53	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:47836 172.28.1.7:22
	00:50:38	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:49347 172.28.1.7:9300
	00:50:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.140:17455 172.28.1.7:16992

	Time	Signature	Protocol	Source / Destination
	00:51:09	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:60601 172.28.1.7:3377
	00:51:17	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:2232
	00:51:25	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.108:43659 172.28.1.7:80
	00:51:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.36:56676 172.28.1.7:37443
	00:51:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:34570 172.28.1.7:22
	00:52:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.155:53407 172.28.1.7:60443
	00:52:44	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	UDP	20.169.104.203:37649 172.28.1.7:23
	00:54:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:52814 172.28.1.7:22
	00:54:05	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	UDP	20.84.51.4:42280 172.28.1.7:5222
	00:54:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.216:55090 172.28.1.7:3389
	00:54:35	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.63:37366 172.28.1.7:16010
	00:54:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.177:51561 172.28.1.7:5555
	00:55:33	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.190:51765 172.28.1.7:49221
	00:56:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:32916 172.28.1.7:22
	00:56:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.78:50301 172.28.1.7:49501
	00:56:53	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.37:55677 172.28.1.7:49803
	00:57:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.51:55254 172.28.1.7:30006
	00:57:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.252:51909 172.28.1.7:43676
	00:58:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.147:54102 172.28.1.7:6002
	00:59:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:40928 172.28.1.7:22
	00:59:03	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.110:55247 172.28.1.7:45992
	01:00:15	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	198.27.77.9:42188 172.28.1.7:1433
	01:00:55	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.87:47500 172.28.1.7:7634
	01:01:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:36232 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	01:01:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.18:26200 172.28.1.7:31017
	01:02:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.235:55486 172.28.1.7:2082
	01:02:15	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.188.189.7:56525 172.28.1.7:4848
	01:03:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.134:19920 172.28.1.7:41795
	01:03:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.183:15156 172.28.1.7:6699
	01:03:58	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.251:49873 172.28.1.7:18392
	01:04:00	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.45.194:48856 172.28.1.7:111
	01:04:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:34282 172.28.1.7:22
	01:04:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:16027
	01:05:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:21281
	01:05:18	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.170:56906 172.28.1.7:1196
	01:05:30	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.148.168:46501 172.28.1.7:9393
	01:06:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:60278 172.28.1.7:22
	01:06:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.43:38926 172.28.1.7:60002
	01:06:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:38448 172.28.1.7:5900
	01:06:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.153:4646 172.28.1.7:20000
	01:06:53	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	UDP	47.251.73.94:32776 172.28.1.7:520
	01:07:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	147.185.132.108:54033 172.28.1.7:4800
	01:08:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.19:53150 172.28.1.7:18206
	01:08:40	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.19:53150 172.28.1.7:18206
	01:09:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:47770 172.28.1.7:22
	01:09:35	ET CINS Active Threat Intelligence Poor Reputation IP group 90 [1:2403389:104040] - Misc Attack	TCP	54.37.196.208:53613 172.28.1.7:2375
	01:10:15	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.182.10:41305 172.28.1.7:8169
	01:10:32	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.6.240:56713 172.28.1.7:53

	Time	Signature	Protocol	Source / Destination
	01:11:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:54120 172.28.1.7:22
	01:11:25	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.216.65.177:16647 172.28.1.7:8191
	01:11:53	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.182:56461 172.28.1.7:9556
	01:12:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.228:56743 172.28.1.7:1521
	01:12:17	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	205.210.31.228:56743 172.28.1.7:1521
	01:13:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.239:52711 172.28.1.7:2043
	01:13:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:9447
	01:13:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.152:13472 172.28.1.7:2181
	01:13:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:45597 172.28.1.7:22
	01:13:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.101:27529 172.28.1.7:13062
	01:14:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:44808 172.28.1.7:22
	01:15:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.220:48831 172.28.1.7:25487
	01:15:28	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.10:56281 172.28.1.7:18576
	01:16:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.249:54592 172.28.1.7:3389
	01:16:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:36118 172.28.1.7:22
	01:16:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.142:40029 172.28.1.7:51200
	01:16:45	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:49709 172.28.1.7:6443
	01:17:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:10001
	01:17:13	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.126:55802 172.28.1.7:9295
	01:17:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:19330 172.28.1.7:2345
	01:19:02	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:47278 172.28.1.7:22
	01:19:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	180.76.96.235:41928 172.28.1.7:22
	01:19:26	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.48.165:11855 172.28.1.7:8875
	01:19:43	ET CINS Active Threat Intelligence Poor Reputation IP group 89 [1:2403388:104040] - Misc Attack	TCP	54.234.80.128:48107 172.28.1.7:6379

	Time	Signature	Protocol	Source / Destination
	01:20:38	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	137.184.32.56:31667 172.28.1.7:5432
	01:20:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.53:56562 172.28.1.7:5688
	01:21:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:45540 172.28.1.7:22
	01:22:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.229:49896 172.28.1.7:1717
	01:22:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.197:54714 172.28.1.7:44818
	01:22:33	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.115.42:30066 172.28.1.7:12123
	01:22:36	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.60:37596 172.28.1.7:55554
	01:23:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.151:5168 172.28.1.7:11000
	01:23:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:42470 172.28.1.7:22
	01:23:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:33891
	01:24:05	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.32.168:50559 172.28.1.7:5357
	01:24:22	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.140.140.15:47568 172.28.1.7:22
	01:25:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:9203
	01:25:50	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:49120 172.28.1.7:22
	01:26:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.148:28630 172.28.1.7:6007
	01:26:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.114:54541 172.28.1.7:5905
	01:26:39	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.207.44:55794 172.28.1.7:6363
	01:27:10	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:16063
	01:28:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:37582 172.28.1.7:22
	01:29:50	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.15.201.64:54959 172.28.1.7:1433
	01:29:50	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	20.15.201.64:54959 172.28.1.7:1433
	01:30:14	ET CINS Active Threat Intelligence Poor Reputation IP group 88 [1:2403387:104040] - Misc Attack	TCP	54.172.76.147:33860 172.28.1.7:9200
	01:30:23	ET CINS Active Threat Intelligence Poor Reputation IP group 56 [1:2403355:104040] - Misc Attack	TCP	39.104.134.58:49664 172.28.1.7:8088
	01:30:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.106:50918 172.28.1.7:1234

	Time	Signature	Protocol	Source / Destination
	01:30:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:40936 172.28.1.7:22
	01:32:23	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.169.80.121:44314 172.28.1.7:2404
	01:33:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:36586 172.28.1.7:22
	01:33:30	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.83.145.39:41428 172.28.1.7:30303
	01:34:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.22:30227 172.28.1.7:2152
	01:34:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.40:54979 172.28.1.7:10257
	01:35:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.60:56192 172.28.1.7:5800
	01:35:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:40804 172.28.1.7:22
	01:35:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.182:54950 172.28.1.7:6000
	01:36:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.139:37329 172.28.1.7:5901
	01:37:22	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.118.32.59:33149 172.28.1.7:3128
	01:37:34	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.102.43.161:47707 172.28.1.7:80
	01:37:41	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:3791
	01:37:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.223:37151 172.28.1.7:20190
	01:38:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:56358 172.28.1.7:22
	01:38:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:5090
	01:38:23	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.52:55229 172.28.1.7:48749
	01:40:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:44050 172.28.1.7:22
	01:40:13	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.217:52778 172.28.1.7:46386
	01:40:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:3115
	01:40:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.54:54632 172.28.1.7:5901
	01:40:42	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.72.118:37174 172.28.1.7:8172
	01:42:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.168:49547 172.28.1.7:60243
	01:42:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:45102 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	01:43:09	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.45.42:57738 172.28.1.7:52951
	01:44:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.220:53593 172.28.1.7:5908
	01:44:46	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.114.166:27772 172.28.1.7:179
	01:44:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:54884 172.28.1.7:22
	01:44:54	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.29.58.2:47689 172.28.1.7:7443
	01:45:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:23320 172.28.1.7:7434
	01:45:18	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.186:55078 172.28.1.7:9090
	01:46:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.246:50294 172.28.1.7:81
	01:46:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:41602 172.28.1.7:70
	01:46:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.240:55780 172.28.1.7:2096
	01:47:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:39078 172.28.1.7:22
	01:47:23	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.246:54337 172.28.1.7:8423
	01:47:29	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.221.69.50:38195 172.28.1.7:520
	01:48:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.150:52172 172.28.1.7:51005
	01:49:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.60:51295 172.28.1.7:943
	01:49:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.144:52826 172.28.1.7:1963
	01:49:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.171:56684 172.28.1.7:54041
	01:49:23	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.124:49317 172.28.1.7:9897
	01:49:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.222:57002 172.28.1.7:50049
	01:49:27	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	UDP	20.168.120.249:57961 172.28.1.7:123
	01:49:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:47180 172.28.1.7:11210
	01:50:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.196:50763 172.28.1.7:8084
	01:50:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:48402 172.28.1.7:22
	01:50:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:29011 172.28.1.7:8080

	Time	Signature	Protocol	Source / Destination
	01:50:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.115:54467 172.28.1.7:587
	01:51:22	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	UDP	47.237.21.35:59773 172.28.1.7:30312
	01:51:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.184:49718 172.28.1.7:1000
	01:52:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:41964 172.28.1.7:22
	01:52:30	ET CINS Active Threat Intelligence Poor Reputation IP group 84 [1:2403383:104040] - Misc Attack	TCP	48.217.84.135:48915 172.28.1.7:47808
	01:52:58	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.102:54011 172.28.1.7:29997
	01:54:34	ET CINS Active Threat Intelligence Poor Reputation IP group 66 [1:2403365:104040] - Misc Attack	TCP	45.156.128.154:40371 172.28.1.7:7777
	01:54:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:51088 172.28.1.7:22
	01:54:53	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.94:52179 172.28.1.7:631
	01:55:18	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	199.45.154.185:46529 172.28.1.7:111
	01:55:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	199.45.154.185:46529 172.28.1.7:111
	01:55:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.159:8050 172.28.1.7:26257
	01:56:21	ET CINS Active Threat Intelligence Poor Reputation IP group 15 [1:2403314:104040] - Misc Attack	TCP	20.106.48.199:35667 172.28.1.7:11741
	01:56:25	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.67:52179 172.28.1.7:9100
	01:57:41	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.169.104.203:45107 172.28.1.7:10443
	01:57:53	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.227.67.171:50578 172.28.1.7:22
	01:58:04	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.67.161.178:47810 172.28.1.7:9300
	01:58:13	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	UDP	20.168.0.84:43089 172.28.1.7:21
	01:58:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.215:54215 172.28.1.7:990
	01:58:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.126:53122 172.28.1.7:69
	01:58:41	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.126:53122 172.28.1.7:69
	01:59:28	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.137.196:44712 172.28.1.7:8184
	01:59:33	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.32:46974 172.28.1.7:5223
	01:59:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.145:30155 172.28.1.7:5222

	Time	Signature	Protocol	Source / Destination
	02:00:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.39:51150 172.28.1.7:88
	02:00:54	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.108:52852 172.28.1.7:9819
	02:00:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:57929 172.28.1.7:18080
	02:01:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.63:54603 172.28.1.7:80
	02:01:58	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.205:54857 172.28.1.7:45807
	02:02:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.107:52438 172.28.1.7:2323
	02:02:20	ET CINS Active Threat Intelligence Poor Reputation IP group 85 [1:2403384:104040] - Misc Attack	UDP	50.7.220.50:1434 172.28.1.7:1434
	02:02:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.71:56921 172.28.1.7:82
	02:02:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.106:53537 172.28.1.7:888
	02:02:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.174:52167 172.28.1.7:8899
	02:02:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.132:40691 172.28.1.7:8000
	02:02:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.245:54036 172.28.1.7:2086
	02:02:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.87:51839 172.28.1.7:54498
	02:03:02	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.106.206.77:46199 172.28.1.7:45000
	02:03:19	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.115.242:40232 172.28.1.7:9018
	02:03:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12121
	02:03:38	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12121
	02:04:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.179:54358 172.28.1.7:4343
	02:04:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.186:55999 172.28.1.7:501
	02:04:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.41:53068 172.28.1.7:5938
	02:05:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.26:26865 172.28.1.7:3702
	02:05:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.72:3427 172.28.1.7:1434
	02:05:39	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.169.50.188:37018 172.28.1.7:5984
	02:06:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.150:61011 172.28.1.7:4840

	Time	Signature	Protocol	Source / Destination
	02:06:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.171:51102 172.28.1.7:7580
	02:06:41	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	TCP	20.169.107.4:36619 172.28.1.7:8980
	02:06:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.200:53444 172.28.1.7:59630
	02:06:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.161:60991 172.28.1.7:88
	02:07:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:5907
	02:07:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.223:36762 172.28.1.7:1985
	02:07:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.170:42894 172.28.1.7:89
	02:07:59	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.170:42894 172.28.1.7:89
	02:08:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:40984 172.28.1.7:6010
	02:08:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.219:52396 172.28.1.7:8081
	02:08:47	ET CINS Active Threat Intelligence Poor Reputation IP group 71 [1:2403370:104040] - Misc Attack	TCP	45.43.63.38:38525 172.28.1.7:2333
	02:08:54	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	TCP	20.169.107.169:58387 172.28.1.7:9080
	02:09:32	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.140.140.15:44044 172.28.1.7:22
	02:09:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.170:56435 172.28.1.7:34475
	02:09:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.213:49774 172.28.1.7:143
	02:09:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.69:52100 172.28.1.7:5984
	02:10:02	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	147.182.137.157:40552 172.28.1.7:5432
	02:10:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.88:50983 172.28.1.7:7001
	02:10:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:51238 172.28.1.7:50000
	02:10:58	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.248:51988 172.28.1.7:1081
	02:11:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.248:43554 172.28.1.7:9003
	02:11:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:45666
	02:11:15	ET CINS Active Threat Intelligence Poor Reputation IP group 17 [1:2403316:104040] - Misc Attack	TCP	20.14.74.210:56495 172.28.1.7:79
	02:11:40	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:15673

	Time	Signature	Protocol	Source / Destination
	02:12:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.167:59980 172.28.1.7:5986
	02:12:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.255:54802 172.28.1.7:9002
	02:12:38	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.23:51543 172.28.1.7:30331
	02:12:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:56971 172.28.1.7:3393
	02:13:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.179:17090 172.28.1.7:22522
	02:13:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.210:52548 172.28.1.7:2323
	02:14:02	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:23320 172.28.1.7:5986
	02:15:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.207:54798 172.28.1.7:82
	02:15:19	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.64.104.114:58724 172.28.1.7:443
	02:16:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.97:52192 172.28.1.7:36235
	02:16:53	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.16:54442 172.28.1.7:47099
	02:16:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.42:16757 172.28.1.7:69
	02:17:08	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.130:54060 172.28.1.7:17518
	02:17:14	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.62:43817 172.28.1.7:2200
	02:17:40	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.88:43817 172.28.1.7:6379
	02:17:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.182:50835 172.28.1.7:45636
	02:18:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.6:26200 172.28.1.7:12321
	02:18:53	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.172:55933 172.28.1.7:9912
	02:18:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.143:45188 172.28.1.7:44819
	02:19:05	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.139.116:47529 172.28.1.7:8142
	02:19:06	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:22000
	02:19:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.113:51494 172.28.1.7:20257
	02:19:26	ET CINS Active Threat Intelligence Poor Reputation IP group 31 [1:2403330:104040] - Misc Attack	TCP	20.64.105.81:38504 172.28.1.7:2455
	02:19:28	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.118:50592 172.28.1.7:5445

	Time	Signature	Protocol	Source / Destination
	02:19:31	ET CINS Active Threat Intelligence Poor Reputation IP group 55 [1:2403354:104040] - Misc Attack	TCP	36.7.107.206:18387 172.28.1.7:8088
	02:19:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.223:50526 172.28.1.7:18080
	02:20:11	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:55231 172.28.1.7:24001
	02:20:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:8686
	02:20:13	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.51:54065 172.28.1.7:9628
	02:20:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.77:54502 172.28.1.7:2013
	02:20:23	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.249:50967 172.28.1.7:47844
	02:20:38	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.233:55070 172.28.1.7:20678
	02:20:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.19:53562 172.28.1.7:8081
	02:20:59	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	TCP	47.96.228.248:47346 172.28.1.7:6379
	02:21:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:14562 172.28.1.7:18245
	02:21:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.115:52765 172.28.1.7:5909
	02:21:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.176:37427 172.28.1.7:20000
	02:22:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:591
	02:22:08	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.53:53048 172.28.1.7:2229
	02:22:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:36534 172.28.1.7:54
	02:23:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.181:38047 172.28.1.7:4786
	02:23:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:7998
	02:23:49	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.93.118:36194 172.28.1.7:10045
	02:23:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:42479 172.28.1.7:5900
	02:24:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:53389
	02:24:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.238:51125 172.28.1.7:9443
	02:24:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.176:44549 172.28.1.7:6513
	02:24:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.79:50454 172.28.1.7:32400

	Time	Signature	Protocol	Source / Destination
	02:24:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.125:46687 172.28.1.7:8880
	02:24:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.99:11586 172.28.1.7:26649
	02:25:04	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	UDP	64.62.197.174:2210 172.28.1.7:3702
	02:25:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.174:2210 172.28.1.7:3702
	02:25:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.27:48446 172.28.1.7:8010
	02:25:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.112:56580 172.28.1.7:50805
	02:25:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.92:51438 172.28.1.7:123
	02:26:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:30878 172.28.1.7:1080
	02:26:23	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.119:53841 172.28.1.7:2345
	02:26:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.86:49576 172.28.1.7:6443
	02:27:30	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:58899 172.28.1.7:6667
	02:27:37	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.154.146:46420 172.28.1.7:5007
	02:27:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:47913 172.28.1.7:12004
	02:27:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.213:49836 172.28.1.7:9200
	02:27:49	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.213:49836 172.28.1.7:9200
	02:27:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:57785
	02:28:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	147.185.132.53:50862 172.28.1.7:48808
	02:28:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.11:40307 172.28.1.7:8020
	02:28:23	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.214:55667 172.28.1.7:28800
	02:28:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.167:50510 172.28.1.7:9115
	02:29:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.188:56065 172.28.1.7:18246
	02:29:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.150:18623 172.28.1.7:2363
	02:29:33	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.41:55011 172.28.1.7:55498
	02:29:42	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.32:58389 172.28.1.7:3306

	Time	Signature	Protocol	Source / Destination
	02:29:56	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.195.155:17005 172.28.1.7:9001
	02:30:03	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.60:56939 172.28.1.7:28980
	02:30:09	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.79:36125 172.28.1.7:9042
	02:30:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:5915
	02:30:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:3000
	02:30:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.216:53787 172.28.1.7:1911
	02:30:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.68:52645 172.28.1.7:6363
	02:31:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:3082 172.28.1.7:1911
	02:31:03	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:35387 172.28.1.7:8291
	02:31:12	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.74.41.172:25415 172.28.1.7:9028
	02:31:18	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.11:52929 172.28.1.7:18083
	02:31:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:29011 172.28.1.7:52311
	02:31:20	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:58796 172.28.1.7:24000
	02:31:22	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	147.182.137.157:37280 172.28.1.7:3306
	02:31:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.237:54347 172.28.1.7:9418
	02:31:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.163:63990 172.28.1.7:8040
	02:32:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.49:50166 172.28.1.7:8080
	02:33:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.138:40295 172.28.1.7:104
	02:33:07	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	3.136.67.107:35445 172.28.1.7:3306
	02:33:07	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:35445 172.28.1.7:3306
	02:33:15	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.84.48.201:33058 172.28.1.7:1389
	02:33:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:29011 172.28.1.7:8008
	02:34:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:9084
	02:35:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2095

	Time	Signature	Protocol	Source / Destination
	02:35:09	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2095
	02:35:18	ET CINS Active Threat Intelligence Poor Reputation IP group 55 [1:2403354:104040] - Misc Attack	UDP	37.202.239.11:5353 172.28.1.7:4000
	02:35:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.92:53961 172.28.1.7:37777
	02:35:41	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:38230 172.28.1.7:9300
	02:36:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:10023
	02:36:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:16046
	02:36:24	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:54759 172.28.1.7:83
	02:36:37	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:58971 172.28.1.7:4444
	02:36:39	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:56835 172.28.1.7:23
	02:36:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.231:56189 172.28.1.7:2085
	02:36:59	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	88.247.20.79:44637 172.28.1.7:1433
	02:37:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.63:53135 172.28.1.7:3388
	02:37:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.10:54114 172.28.1.7:1024
	02:37:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:12238
	02:37:41	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.185.240:44147 172.28.1.7:9443
	02:37:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.42:55559 172.28.1.7:7547
	02:38:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.50:55748 172.28.1.7:11553
	02:38:07	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:44343 172.28.1.7:25
	02:38:13	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.14:55854 172.28.1.7:55443
	02:38:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:12416
	02:38:46	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:40351 172.28.1.7:3377
	02:38:57	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:47093 172.28.1.7:8008
	02:39:03	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:51224 172.28.1.7:2078
	02:39:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.180:30842 172.28.1.7:18245

	Time	Signature	Protocol	Source / Destination
	02:39:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:10380
	02:39:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.105:52655 172.28.1.7:4786
	02:40:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.99:44263 172.28.1.7:8089
	02:40:33	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.216:52742 172.28.1.7:47506
	02:40:42	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	108.176.102.58:59239 172.28.1.7:3306
	02:40:43	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.59:50969 172.28.1.7:9846
	02:40:44	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.239:52011 172.28.1.7:9812
	02:40:55	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.206:51701 172.28.1.7:49695
	02:41:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:19015
	02:41:27	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:43868 172.28.1.7:55756
	02:41:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:57177 172.28.1.7:2022
	02:41:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.217:42771 172.28.1.7:9999
	02:42:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.212:51132 172.28.1.7:4117
	02:42:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:42802 172.28.1.7:3306
	02:42:23	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	193.163.125.238:42802 172.28.1.7:3306
	02:43:16	ET SCAN HID VertX and Edge door controllers discover [1:2025822:2] - Attempted Information Leak	UDP	207.90.244.23:20365 172.28.1.7:4070
	02:43:33	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.139.21:27739 172.28.1.7:8814
	02:43:58	ET CINS Active Threat Intelligence Poor Reputation IP group 58 [1:2403357:104040] - Misc Attack	TCP	40.124.172.100:49387 172.28.1.7:554
	02:44:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.93:55252 172.28.1.7:8880
	02:44:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:29011 172.28.1.7:9295
	02:44:28	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.106:54581 172.28.1.7:45666
	02:44:42	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.1.17:39881 172.28.1.7:7210
	02:44:44	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:30705 172.28.1.7:2000
	02:45:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.70:56823 172.28.1.7:20257

	Time	Signature	Protocol	Source / Destination
	02:46:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9225
	02:46:25	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	185.94.111.1:38764 172.28.1.7:111
	02:46:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.104:48102 172.28.1.7:59665
	02:47:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.252:50547 172.28.1.7:18091
	02:47:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.56:50756 172.28.1.7:8991
	02:48:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.19:26200 172.28.1.7:9550
	02:49:09	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:1966
	02:49:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.175:49810 172.28.1.7:10010
	02:49:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.240:55193 172.28.1.7:9000
	02:49:18	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.38:40006 172.28.1.7:5672
	02:49:18	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	4.227.178.194:56716 172.28.1.7:1433
	02:49:18	ET CINS Active Threat Intelligence Poor Reputation IP group 5 [1:2403304:104040] - Misc Attack	TCP	4.227.178.194:56716 172.28.1.7:1433
	02:49:19	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.86:37000 172.28.1.7:7001
	02:49:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.52:33093 172.28.1.7:5683
	02:49:53	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.116:56923 172.28.1.7:58585
	02:50:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.194:55015 172.28.1.7:8013
	02:50:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.108:47486 172.28.1.7:10934
	02:51:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.111:1915 172.28.1.7:46459
	02:51:22	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	147.182.137.157:51656 172.28.1.7:1433
	02:52:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.244:54940 172.28.1.7:25025
	02:52:13	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.152:50788 172.28.1.7:47961
	02:52:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.146:46987 172.28.1.7:8015
	02:52:18	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.146:46987 172.28.1.7:8015
	02:52:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.246:55980 172.28.1.7:44818

	Time	Signature	Protocol	Source / Destination
	02:52:24	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	UDP	20.55.84.43:35473 172.28.1.7:443
	02:52:46	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.76.116.33:53479 172.28.1.7:8008
	02:53:15	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.188.231.113:55485 172.28.1.7:5432
	02:53:15	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	52.188.231.113:55485 172.28.1.7:5432
	02:53:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.111:39253 172.28.1.7:22
	02:54:03	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.54:49337 172.28.1.7:8444
	02:54:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.156:12973 172.28.1.7:2323
	02:54:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:12166
	02:54:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.214:50513 172.28.1.7:52951
	02:54:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.217:53797 172.28.1.7:13929
	02:54:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.129:37259 172.28.1.7:11103
	02:54:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.76:54762 172.28.1.7:2161
	02:54:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.134:7430 172.28.1.7:5432
	02:54:56	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	167.94.138.134:7430 172.28.1.7:5432
	02:54:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:16081
	02:55:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.232:37640 172.28.1.7:21230
	02:55:03	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.4:51207 172.28.1.7:8284
	02:55:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.117:53156 172.28.1.7:12366
	02:55:17	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.117:53156 172.28.1.7:12366
	02:55:36	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	23.95.132.51:42984 172.28.1.7:3389
	02:55:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.57:52023 172.28.1.7:1311
	02:55:58	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.194:49672 172.28.1.7:20
	02:56:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.127:50498 172.28.1.7:9865
	02:57:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:10864 172.28.1.7:53

	Time	Signature	Protocol	Source / Destination
	02:57:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.238:56952 172.28.1.7:9151
	02:58:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	193.163.125.182:21549 172.28.1.7:1812
	02:58:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.253:51049 172.28.1.7:4410
	02:58:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.98:41162 172.28.1.7:9643
	02:58:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.19:53166 172.28.1.7:28759
	02:58:38	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.19:53166 172.28.1.7:28759
	02:58:50	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.49:52937 172.28.1.7:6004
	02:59:28	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.160:53569 172.28.1.7:34566
	02:59:37	ET CINS Active Threat Intelligence Poor Reputation IP group 95 [1:2403394:104040] - Misc Attack	TCP	61.40.158.106:47241 172.28.1.7:22
	02:59:53	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.36:50767 172.28.1.7:61234
	03:00:20	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	207.90.244.22:28821 172.28.1.7:1521
	03:01:41	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:12393
	03:01:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.157:57195 172.28.1.7:62337
	03:01:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.47:52777 172.28.1.7:8083
	03:02:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.9:56039 172.28.1.7:987
	03:03:18	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.169.51.3:59576 172.28.1.7:5222
	03:03:21	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.136.10:37132 172.28.1.7:7000
	03:03:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.85:60231 172.28.1.7:1521
	03:03:54	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	64.62.156.85:60231 172.28.1.7:1521
	03:06:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.218:48069 172.28.1.7:5522
	03:06:03	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.126:53122 172.28.1.7:40081
	03:06:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.126:53122 172.28.1.7:40081
	03:06:32	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.67:48819 172.28.1.7:1344
	03:06:34	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:8428

	Time	Signature	Protocol	Source / Destination
	03:06:47	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:53580 172.28.1.7:8069
	03:07:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.80:55644 172.28.1.7:2087
	03:07:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.51:13084 172.28.1.7:7548
	03:07:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.152:35137 172.28.1.7:8070
	03:07:53	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:45745 172.28.1.7:12321
	03:09:01	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:33215 172.28.1.7:554
	03:09:26	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.105.169:50600 172.28.1.7:53
	03:09:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.132:45107 172.28.1.7:6699
	03:10:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.233:38498 172.28.1.7:3535
	03:10:16	ET CINS Active Threat Intelligence Poor Reputation IP group 56 [1:2403355:104040] - Misc Attack	TCP	38.132.109.106:37652 172.28.1.7:3389
	03:10:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.210:54034 172.28.1.7:58000
	03:10:57	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.141.145:41385 172.28.1.7:11065
	03:11:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:53389
	03:11:29	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.124:49233 172.28.1.7:5081
	03:11:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.124:49233 172.28.1.7:5081
	03:11:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:60844 172.28.1.7:5900
	03:11:43	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:3155
	03:11:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	66.132.153.147:62745 172.28.1.7:1812
	03:11:48	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.123:53385 172.28.1.7:48428
	03:11:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.213:52686 172.28.1.7:5986
	03:13:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.237:44160 172.28.1.7:4081
	03:13:42	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.59.190:54225 172.28.1.7:22
	03:13:43	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:44384 172.28.1.7:1443
	03:13:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.135:53208 172.28.1.7:6080

	Time	Signature	Protocol	Source / Destination
	03:13:59	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.135:53208 172.28.1.7:6080
	03:15:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.174:53713 172.28.1.7:6081
	03:15:31	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:2568
	03:15:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.59:22348 172.28.1.7:789
	03:16:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.242:51635 172.28.1.7:25789
	03:16:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.74:51759 172.28.1.7:20121
	03:16:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:18035
	03:17:08	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:40707 172.28.1.7:30080
	03:17:16	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:36129 172.28.1.7:8010
	03:18:16	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:40203 172.28.1.7:8084
	03:18:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.147:13717 172.28.1.7:6002
	03:18:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.79:57300 172.28.1.7:22460
	03:18:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.216:52095 172.28.1.7:7047
	03:18:58	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:52966 172.28.1.7:5060
	03:19:21	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:34734 172.28.1.7:1024
	03:19:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.154:18970 172.28.1.7:20548
	03:19:50	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:26200 172.28.1.7:12108
	03:22:15	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.66:47171 172.28.1.7:8081
	03:22:40	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.67.161.178:53350 172.28.1.7:808
	03:22:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.197:54848 172.28.1.7:4026
	03:22:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.143:53178 172.28.1.7:26371
	03:22:56	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.143:53178 172.28.1.7:26371
	03:23:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.98:51499 172.28.1.7:28055
	03:23:25	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:43060 172.28.1.7:49153

	Time	Signature	Protocol	Source / Destination
	03:23:38	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	201.132.11.46:56159 172.28.1.7:1433
	03:23:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.108:41147 172.28.1.7:8006
	03:24:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.32:52702 172.28.1.7:49873
	03:24:53	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.237:53299 172.28.1.7:49864
	03:25:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.205:50268 172.28.1.7:7443
	03:25:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.39:57260 172.28.1.7:12443
	03:26:38	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:52738 172.28.1.7:4449
	03:27:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.26:25195 172.28.1.7:1900
	03:28:01	ET CINS Active Threat Intelligence Poor Reputation IP group 17 [1:2403316:104040] - Misc Attack	TCP	20.14.73.168:36218 172.28.1.7:8084
	03:29:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.123:45164 172.28.1.7:65422
	03:29:38	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.150.202.39:41258 172.28.1.7:4330
	03:30:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:12400
	03:30:36	ET CINS Active Threat Intelligence Poor Reputation IP group 58 [1:2403357:104040] - Misc Attack	TCP	40.124.171.173:50486 172.28.1.7:23
	03:30:38	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.15.150:29245 172.28.1.7:7687
	03:31:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.119:51591 172.28.1.7:33459
	03:31:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	199.45.154.183:53433 172.28.1.7:5353
	03:31:59	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.161.50.108:60023 172.28.1.7:27017
	03:32:05	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.111.86:32170 172.28.1.7:8834
	03:32:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.134:54531 172.28.1.7:9775
	03:33:22	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.202:50780 172.28.1.7:46989
	03:33:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.101:53944 172.28.1.7:9582
	03:33:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:8198
	03:35:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.193:50734 172.28.1.7:943
	03:36:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:9000

	Time	Signature	Protocol	Source / Destination
	03:36:30	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:9000
	03:36:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:7070
	03:38:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.129:44944 172.28.1.7:9000
	03:38:16	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.129:44944 172.28.1.7:9000
	03:38:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:7605 172.28.1.7:1599
	03:39:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.145:2325 172.28.1.7:2362
	03:40:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:9510
	03:41:27	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:52837 172.28.1.7:11211
	03:42:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.96:24552 172.28.1.7:13303
	03:42:18	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:36361 172.28.1.7:53
	03:42:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.172:55186 172.28.1.7:49390
	03:42:58	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	UDP	20.171.25.13:60515 172.28.1.7:5060
	03:43:58	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.196:50520 172.28.1.7:32010
	03:44:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.102:51998 172.28.1.7:65530
	03:44:23	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.63:57259 172.28.1.7:10123
	03:44:44	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.14:55648 172.28.1.7:47935
	03:45:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:49767
	03:45:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.112:55098 172.28.1.7:8443
	03:46:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.237:50343 172.28.1.7:17516
	03:46:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.109:57333 172.28.1.7:8090
	03:48:18	ET CINS Active Threat Intelligence Poor Reputation IP group 15 [1:2403314:104040] - Misc Attack	TCP	20.106.57.141:50277 172.28.1.7:7001
	03:49:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.251:44071 172.28.1.7:52232
	03:49:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.148:20303 172.28.1.7:50580
	03:51:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:21515

	Time	Signature	Protocol	Source / Destination
	03:52:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.215:57338 172.28.1.7:31337
	03:52:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.107:50732 172.28.1.7:49365
	03:53:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.105:54488 172.28.1.7:30303
	03:53:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.185:50042 172.28.1.7:1913
	03:53:55	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	71.6.199.23:14903 172.28.1.7:111
	03:54:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.158:63927 172.28.1.7:631
	03:54:17	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.106.17.55:33572 172.28.1.7:512
	03:55:44	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	TCP	20.169.106.171:43315 172.28.1.7:162
	03:56:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.53:51366 172.28.1.7:11010
	03:56:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.231:55169 172.28.1.7:3929
	03:56:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.178:23987 172.28.1.7:13000
	03:57:29	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.84.60.216:57948 172.28.1.7:9443
	03:58:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.3:9421 172.28.1.7:8015
	03:58:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.136:31920 172.28.1.7:10260
	03:59:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.120:55684 172.28.1.7:27017
	03:59:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:1388
	03:59:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:59548 172.28.1.7:22
	03:59:55	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.105.85:11211 172.28.1.7:7500
	03:59:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.104:12000 172.28.1.7:50114
	04:00:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.19:53166 172.28.1.7:13393
	04:00:28	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.19:53166 172.28.1.7:13393
	04:00:33	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.252:52700 172.28.1.7:49041
	04:00:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.178:53478 172.28.1.7:13020
	04:01:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.249:56523 172.28.1.7:9092

	Time	Signature	Protocol	Source / Destination
	04:03:06	ET CINS Active Threat Intelligence Poor Reputation IP group 40 [1:2403339:104040] - Misc Attack	UDP	31.187.74.235:19510 172.28.1.7:5060
	04:03:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.230:55228 172.28.1.7:10255
	04:03:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:18113
	04:03:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	139.19.117.130:58484 172.28.1.7:22
	04:04:09	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.55.35.217:36762 172.28.1.7:5222
	04:05:33	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.105:57306 172.28.1.7:21
	04:06:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.146:60847 172.28.1.7:10252
	04:07:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.136:55882 172.28.1.7:15378
	04:08:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.215:55823 172.28.1.7:9444
	04:08:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.137:52642 172.28.1.7:389
	04:08:50	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	UDP	64.62.197.137:52642 172.28.1.7:389
	04:09:18	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.167:50128 172.28.1.7:9216
	04:09:28	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.197:54254 172.28.1.7:50895
	04:09:42	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.32:40271 172.28.1.7:10048
	04:09:52	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.45:53859 172.28.1.7:52309
	04:10:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.81:53986 172.28.1.7:53300
	04:10:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.250:52456 172.28.1.7:17185
	04:10:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:9328 172.28.1.7:8200
	04:11:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.133:10055 172.28.1.7:53
	04:12:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.218:59667 172.28.1.7:6203
	04:12:50	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	23.95.186.189:45759 172.28.1.7:5589
	04:13:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.167:9206 172.28.1.7:111
	04:13:17	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	64.62.197.167:9206 172.28.1.7:111
	04:13:17	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	UDP	64.62.197.167:9206 172.28.1.7:111

	Time	Signature	Protocol	Source / Destination
	04:14:38	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.74:52642 172.28.1.7:17780
	04:14:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.243:56732 172.28.1.7:2084
	04:14:58	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:5905
	04:16:00	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.243.4.163:43569 172.28.1.7:8088
	04:16:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:3110
	04:16:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.211:54510 172.28.1.7:5985
	04:16:41	ET CINS Active Threat Intelligence Poor Reputation IP group 2 [1:2403301:104040] - Misc Attack	TCP	1.24.78.26:36774 172.28.1.7:5555
	04:16:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.146:45385 172.28.1.7:20001
	04:17:43	ET CINS Active Threat Intelligence Poor Reputation IP group 67 [1:2403366:104040] - Misc Attack	TCP	45.156.128.87:35451 172.28.1.7:53
	04:17:51	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.57.20:24961 172.28.1.7:80
	04:18:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.117:51243 172.28.1.7:143
	04:18:23	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.71:49568 172.28.1.7:8086
	04:19:00	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.74.44.18:20302 172.28.1.7:9205
	04:19:20	ET CINS Active Threat Intelligence Poor Reputation IP group 58 [1:2403357:104040] - Misc Attack	TCP	40.124.174.187:50821 172.28.1.7:47808
	04:19:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:21307
	04:20:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.207:54011 172.28.1.7:135
	04:20:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.67:46908 172.28.1.7:7547
	04:20:17	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	UDP	20.55.84.43:56087 172.28.1.7:873
	04:21:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9405
	04:21:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.74:49289 172.28.1.7:30083
	04:22:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.157:61459 172.28.1.7:18244
	04:22:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:54600 172.28.1.7:25962
	04:23:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.245:51831 172.28.1.7:4100
	04:23:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.223:52643 172.28.1.7:80

	Time	Signature	Protocol	Source / Destination
	04:24:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.73:49370 172.28.1.7:8088
	04:24:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.99:55435 172.28.1.7:50997
	04:24:48	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.28:55566 172.28.1.7:8010
	04:24:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.111:49990 172.28.1.7:47808
	04:25:28	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:16698 172.28.1.7:4000
	04:25:40	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.28:56114 172.28.1.7:8080
	04:29:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.78:55745 172.28.1.7:8445
	04:29:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:1111
	04:30:45	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:9097
	04:31:02	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.143.143:47981 172.28.1.7:8123
	04:32:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.201:53629 172.28.1.7:2080
	04:32:32	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.6.210:36446 172.28.1.7:8181
	04:33:00	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	186.193.187.63:46527 172.28.1.7:1433
	04:33:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.243:56400 172.28.1.7:137
	04:34:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.143:53089 172.28.1.7:49431
	04:34:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:33797 172.28.1.7:5900
	04:34:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:8900
	04:35:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:6070
	04:35:53	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.25:54657 172.28.1.7:46359
	04:36:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.248:51549 172.28.1.7:88
	04:36:30	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:55941 172.28.1.7:8094
	04:36:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:35118 172.28.1.7:9096
	04:37:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.115:53262 172.28.1.7:49502
	04:37:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.244:43622 172.28.1.7:10114

	Time	Signature	Protocol	Source / Destination
	04:37:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.27:63324 172.28.1.7:7170
	04:37:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.140:18432 172.28.1.7:22222
	04:38:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.223:57314 172.28.1.7:8009
	04:38:29	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:33232 172.28.1.7:1000
	04:38:58	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.82:56213 172.28.1.7:8158
	04:39:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.91:49526 172.28.1.7:1028
	04:39:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.49:54671 172.28.1.7:8088
	04:40:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:50642 172.28.1.7:10123
	04:41:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:3570
	04:41:38	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.41:56254 172.28.1.7:47715
	04:41:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.32:56431 172.28.1.7:31005
	04:42:14	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.192.33:35767 172.28.1.7:443
	04:43:13	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.3:56479 172.28.1.7:110
	04:43:32	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.148:52425 172.28.1.7:9489
	04:44:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.71:50233 172.28.1.7:9629
	04:44:39	ET CINS Active Threat Intelligence Poor Reputation IP group 42 [1:2403341:104040] - Misc Attack	TCP	34.59.175.189:58830 172.28.1.7:443
	04:44:39	ET COMPROMISED Known Compromised or Hostile Host Traffic group 9 [1:2500016:7420] - Misc Attack	TCP	34.59.175.189:58830 172.28.1.7:443
	04:45:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:56971 172.28.1.7:3397
	04:46:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:9312
	04:46:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.185:54550 172.28.1.7:911
	04:47:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.55:43094 172.28.1.7:5353
	04:47:22	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:54305 172.28.1.7:9800
	04:47:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.175:51917 172.28.1.7:1521
	04:47:29	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	198.235.24.175:51917 172.28.1.7:1521

	Time	Signature	Protocol	Source / Destination
	04:47:34	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	108.181.57.157:5071 172.28.1.7:5060
	04:47:34	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	108.181.57.157:5071 172.28.1.7:5060
	04:47:35	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:5231
	04:47:48	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.227.41.39:34139 172.28.1.7:8000
	04:48:03	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.70:54514 172.28.1.7:8934
	04:48:18	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.157:49256 172.28.1.7:8501
	04:48:23	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.247:50424 172.28.1.7:7078
	04:49:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.200:57354 172.28.1.7:4117
	04:49:19	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.200:57354 172.28.1.7:4117
	04:50:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.211:54878 172.28.1.7:8008
	04:50:46	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.14.103:59242 172.28.1.7:88
	04:51:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:50005
	04:52:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.216:49878 172.28.1.7:7443
	04:52:21	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.216:49878 172.28.1.7:7443
	04:52:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.149:19452 172.28.1.7:44818
	04:52:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.5:17553 172.28.1.7:3483
	04:52:53	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:48505 172.28.1.7:443
	04:54:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:44681 172.28.1.7:17001
	04:54:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.45:53561 172.28.1.7:2455
	04:54:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12125
	04:54:47	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12125
	04:55:19	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:51482 172.28.1.7:2404
	04:55:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.157:52285 172.28.1.7:9643
	04:56:34	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:46162 172.28.1.7:82

	Time	Signature	Protocol	Source / Destination
	04:56:36	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.43:36836 172.28.1.7:443
	04:58:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.241:56702 172.28.1.7:5001
	04:58:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.207:50967 172.28.1.7:5916
	04:58:53	ET CINS Active Threat Intelligence Poor Reputation IP group 40 [1:2403339:104040] - Misc Attack	UDP	34.122.156.88:15907 172.28.1.7:8080
	04:59:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.95:52342 172.28.1.7:8333
	05:00:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.22:18211 172.28.1.7:3283
	05:01:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.9:49684 172.28.1.7:22
	05:01:35	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:54289 172.28.1.7:15672
	05:02:20	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.137.226:45174 172.28.1.7:5004
	05:02:31	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	184.105.247.208:47988 172.28.1.7:5432
	05:03:04	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:34008 172.28.1.7:22227
	05:03:08	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:45564 172.28.1.7:8011
	05:04:24	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.61.119:33038 172.28.1.7:8080
	05:04:28	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.124.93.107:43417 172.28.1.7:4443
	05:04:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	134.209.83.10:38834 172.28.1.7:22
	05:04:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.187:3409 172.28.1.7:57722
	05:04:44	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:48831 172.28.1.7:3000
	05:05:49	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:32970 172.28.1.7:80
	05:06:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.46:37052 172.28.1.7:81
	05:06:14	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:59349 172.28.1.7:3001
	05:06:19	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.221.68.115:47636 172.28.1.7:5431
	05:06:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	134.209.83.10:37576 172.28.1.7:22
	05:06:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.129:9698 172.28.1.7:5902
	05:07:26	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:49561 172.28.1.7:51005

	Time	Signature	Protocol	Source / Destination
	05:07:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:9222
	05:07:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.79:56586 172.28.1.7:2121
	05:08:03	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.238:54924 172.28.1.7:49499
	05:08:18	ET CINS Active Threat Intelligence Poor Reputation IP group 31 [1:2403330:104040] - Misc Attack	TCP	20.64.106.38:50051 172.28.1.7:8118
	05:08:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.246:35251 172.28.1.7:21322
	05:08:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.176:41220 172.28.1.7:84
	05:08:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	134.209.83.10:60456 172.28.1.7:22
	05:09:05	ET CINS Active Threat Intelligence Poor Reputation IP group 11 [1:2403310:104040] - Misc Attack	TCP	13.89.121.92:35487 172.28.1.7:5938
	05:09:08	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.85.121:38216 172.28.1.7:6011
	05:09:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.180:25121 172.28.1.7:50580
	05:09:30	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.77:35870 172.28.1.7:58603
	05:09:48	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.158:52409 172.28.1.7:9518
	05:10:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.192:47866 172.28.1.7:86
	05:10:45	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.29:51522 172.28.1.7:3306
	05:10:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.242:41601 172.28.1.7:8088
	05:11:48	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.105:53623 172.28.1.7:9313
	05:13:05	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	UDP	20.168.6.84:40868 172.28.1.7:502
	05:14:28	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.210:56910 172.28.1.7:3120
	05:14:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:29011 172.28.1.7:82
	05:14:42	ET CINS Active Threat Intelligence Poor Reputation IP group 6 [1:2403305:104040] - Misc Attack	TCP	8.210.20.168:46975 172.28.1.7:8088
	05:15:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:8178
	05:16:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26673 172.28.1.7:5435
	05:16:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.134:46656 172.28.1.7:5000
	05:17:29	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.91:42549 172.28.1.7:1200

	Time	Signature	Protocol	Source / Destination
	05:18:01	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.186.155:58632 172.28.1.7:4848
	05:19:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.109:50122 172.28.1.7:636
	05:19:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:3500
	05:21:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.6:4089 172.28.1.7:34980
	05:21:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:21290
	05:21:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.108:55550 172.28.1.7:5906
	05:21:53	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.32:52489 172.28.1.7:3306
	05:23:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:8494
	05:23:18	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.42:49592 172.28.1.7:48622
	05:24:11	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:29011 172.28.1.7:4567
	05:25:24	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.175.30:57554 172.28.1.7:119
	05:25:43	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.72:46701 172.28.1.7:4369
	05:27:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.83:51613 172.28.1.7:42420
	05:27:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.187:54030 172.28.1.7:16993
	05:27:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.151:4940 172.28.1.7:11
	05:28:46	ET CINS Active Threat Intelligence Poor Reputation IP group 56 [1:2403355:104040] - Misc Attack	TCP	38.76.73.6:59472 172.28.1.7:445
	05:29:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.97:58037 172.28.1.7:6080
	05:30:04	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:23183 172.28.1.7:37777
	05:30:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.175:46481 172.28.1.7:31337
	05:31:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.11:14073 172.28.1.7:50805
	05:31:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.239:52809 172.28.1.7:46655
	05:33:03	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.67:50955 172.28.1.7:49018
	05:33:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.84:57179 172.28.1.7:20249
	05:35:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.194:48163 172.28.1.7:20020

	Time	Signature	Protocol	Source / Destination
	05:35:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.172:40848 172.28.1.7:4443
	05:36:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9394
	05:36:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.193:55226 172.28.1.7:9700
	05:37:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.222:39113 172.28.1.7:8580
	05:37:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.167:35461 172.28.1.7:80
	05:38:33	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.164:51110 172.28.1.7:1930
	05:39:10	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.213.148.191:56790 172.28.1.7:23
	05:39:29	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.59.63:29709 172.28.1.7:30083
	05:39:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.94:49215 172.28.1.7:8085
	05:41:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.77:52203 172.28.1.7:3389
	05:41:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.140:32196 172.28.1.7:9090
	05:42:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.240:56526 172.28.1.7:6660
	05:42:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:1454
	05:43:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.86:54795 172.28.1.7:9000
	05:44:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.93:56644 172.28.1.7:3909
	05:44:27	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	UDP	51.159.54.94:32546 172.28.1.7:8082
	05:44:28	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.234:56147 172.28.1.7:51399
	05:44:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.143:49720 172.28.1.7:31711
	05:44:48	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.143:49720 172.28.1.7:31711
	05:45:19	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.1.211:57776 172.28.1.7:9443
	05:47:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:29011 172.28.1.7:50050
	05:47:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:33138 172.28.1.7:22
	05:47:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:15704 172.28.1.7:3050
	05:47:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.139:45374 172.28.1.7:55443

	Time	Signature	Protocol	Source / Destination
	05:48:00	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.165.88.155:59147 172.28.1.7:8443
	05:48:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.235:56938 172.28.1.7:49577
	05:49:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.220:32770 172.28.1.7:6379
	05:49:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:43940 172.28.1.7:5900
	05:50:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:48194 172.28.1.7:22
	05:50:44	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.12:54472 172.28.1.7:5343
	05:51:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.3:37514 172.28.1.7:55555
	05:51:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	199.45.154.183:10163 172.28.1.7:2361
	05:52:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.19:49692 172.28.1.7:6789
	05:52:14	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.19:49692 172.28.1.7:6789
	05:52:14	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.253:52207 172.28.1.7:46956
	05:52:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.103:41707 172.28.1.7:2095
	05:52:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.253:42234 172.28.1.7:1830
	05:52:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.94:55026 172.28.1.7:8444
	05:53:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:47392 172.28.1.7:22
	05:53:38	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.116:54567 172.28.1.7:47053
	05:54:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:9999
	05:54:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.155:55035 172.28.1.7:6060
	05:54:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.107:55338 172.28.1.7:23000
	05:55:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.228:47459 172.28.1.7:3001
	05:55:33	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.84.118.60:52247 172.28.1.7:8089
	05:55:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.244:32988 172.28.1.7:3389
	05:55:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.172:33562 172.28.1.7:13
	05:55:56	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	UDP	64.62.197.172:33562 172.28.1.7:13

	Time	Signature	Protocol	Source / Destination
	05:56:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.165:52315 172.28.1.7:51200
	05:56:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:48562 172.28.1.7:22
	05:57:37	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.102.116.62:50610 172.28.1.7:1723
	05:57:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.230:56544 172.28.1.7:40005
	05:58:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.159:62739 172.28.1.7:2052
	05:58:48	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.15.164.165:42971 172.28.1.7:11742
	05:59:08	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.210.94:52609 172.28.1.7:10091
	05:59:16	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:47960 172.28.1.7:22
	05:59:17	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:58474 172.28.1.7:1337
	05:59:28	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.0.133:55652 172.28.1.7:8081
	05:59:34	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:25600 172.28.1.7:8500
	06:00:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.239:56599 172.28.1.7:22
	06:01:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.91:52661 172.28.1.7:7080
	06:01:07	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.84.38.245:9503 172.28.1.7:22
	06:01:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.234:54683 172.28.1.7:2078
	06:02:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:57212 172.28.1.7:22
	06:02:58	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.72:56891 172.28.1.7:9061
	06:03:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2222
	06:03:46	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2222
	06:03:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.99:59550 172.28.1.7:9642
	06:04:11	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.254.131.109:33156 172.28.1.7:12354
	06:04:34	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.81.203:23191 172.28.1.7:9383
	06:05:02	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	104.248.202.166:50470 172.28.1.7:22
	06:05:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.155:65089 172.28.1.7:6060

	Time	Signature	Protocol	Source / Destination
	06:05:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	66.132.153.157:63430 172.28.1.7:443
	06:05:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.67:44213 172.28.1.7:135
	06:06:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.31:60976 172.28.1.7:143
	06:06:55	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:843
	06:08:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.240:50215 172.28.1.7:4172
	06:08:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.121:58914 172.28.1.7:22122
	06:08:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:953
	06:09:00	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.118.32.47:47434 172.28.1.7:27017
	06:09:11	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.52.121:20005 172.28.1.7:8980
	06:10:25	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:48304 172.28.1.7:9002
	06:10:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.10:47972 172.28.1.7:32414
	06:10:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.103:56028 172.28.1.7:8094
	06:10:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.147:31441 172.28.1.7:6080
	06:11:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.107:29252 172.28.1.7:8775
	06:11:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.127:54208 172.28.1.7:8030
	06:11:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.60:56955 172.28.1.7:4430
	06:11:58	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.84.117.55:49909 172.28.1.7:7337
	06:12:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.177:47314 172.28.1.7:8060
	06:13:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.92:51508 172.28.1.7:12345
	06:14:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.167:52721 172.28.1.7:46574
	06:15:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:42802 172.28.1.7:3269
	06:15:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.211:53349 172.28.1.7:9093
	06:15:59	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:451
	06:16:16	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.143:52925 172.28.1.7:5900

	Time	Signature	Protocol	Source / Destination
	06:17:17	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.114:54410 172.28.1.7:8074
	06:18:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.155:57186 172.28.1.7:1636
	06:18:13	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.102:50518 172.28.1.7:9972
	06:18:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.184:49373 172.28.1.7:18574
	06:19:04	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.34:50613 172.28.1.7:23023
	06:19:35	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.210.99:56394 172.28.1.7:51023
	06:19:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:12296
	06:21:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.121:55755 172.28.1.7:50053
	06:21:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:27571
	06:22:20	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.188.189.6:54308 172.28.1.7:4118
	06:22:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:48526 172.28.1.7:58222
	06:22:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.176:53442 172.28.1.7:6601
	06:22:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:10123
	06:23:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:3665 172.28.1.7:20880
	06:23:28	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:46716 172.28.1.7:49152
	06:23:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.43:62936 172.28.1.7:61000
	06:24:03	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.35:56179 172.28.1.7:3306
	06:24:08	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.79:51983 172.28.1.7:46307
	06:24:27	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	139.59.170.85:26312 172.28.1.7:1433
	06:24:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.43:56686 172.28.1.7:2083
	06:25:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	ICMP	207.90.244.29:0 172.28.1.7:8
	06:25:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.173:50739 172.28.1.7:33066
	06:25:29	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.42.91:26109 172.28.1.7:6588
	06:25:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.227:50822 172.28.1.7:9100

	Time	Signature	Protocol	Source / Destination
	06:26:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.205:51867 172.28.1.7:995
	06:27:27	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.67.177.206:59409 172.28.1.7:30001
	06:27:40	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.72:36457 172.28.1.7:119
	06:28:19	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.161.50.108:60023 172.28.1.7:80
	06:28:19	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:42338 172.28.1.7:8585
	06:28:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.91:53654 172.28.1.7:49667
	06:29:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.227:53167 172.28.1.7:179
	06:29:37	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.29.19.243:37021 172.28.1.7:771
	06:29:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.229:50361 172.28.1.7:2001
	06:29:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.162:47901 172.28.1.7:8873
	06:30:41	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.251:52114 172.28.1.7:49751
	06:31:04	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:42588 172.28.1.7:2079
	06:31:24	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.7.149:53030 172.28.1.7:9529
	06:31:47	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.217:54449 172.28.1.7:19443
	06:31:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.190:3938 172.28.1.7:47001
	06:32:01	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:26200 172.28.1.7:3078
	06:33:48	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:52616 172.28.1.7:3702
	06:33:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.52:53063 172.28.1.7:5000
	06:34:07	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.52.82:59862 172.28.1.7:12134
	06:34:53	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:60588 172.28.1.7:9090
	06:35:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.252:51647 172.28.1.7:58603
	06:35:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.231:55245 172.28.1.7:2443
	06:36:00	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.218:54176 172.28.1.7:8806
	06:36:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.221:46194 172.28.1.7:25162

	Time	Signature	Protocol	Source / Destination
	06:36:26	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:8988
	06:37:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.127:50457 172.28.1.7:46331
	06:37:28	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.152:56996 172.28.1.7:45444
	06:38:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	147.185.132.54:54523 172.28.1.7:5060
	06:38:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.179:54088 172.28.1.7:16010
	06:39:14	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:35977 172.28.1.7:465
	06:40:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.246:50689 172.28.1.7:8139
	06:40:20	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.29.8.147:36833 172.28.1.7:80
	06:40:46	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.215.181:30188 172.28.1.7:12195
	06:41:34	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	UDP	47.254.215.105:36154 172.28.1.7:6881
	06:41:50	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.195.157:32797 172.28.1.7:3443
	06:42:19	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	18.217.194.148:45580 172.28.1.7:1521
	06:42:19	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:45580 172.28.1.7:1521
	06:42:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.158:14421 172.28.1.7:15000
	06:43:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:4401
	06:43:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:8811
	06:43:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:9923
	06:44:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.103:33117 172.28.1.7:830
	06:44:48	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:35139 172.28.1.7:4433
	06:45:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.24:20252 172.28.1.7:161
	06:45:19	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	64.62.156.24:20252 172.28.1.7:161
	06:46:12	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:49447 172.28.1.7:50000
	06:46:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.110:55484 172.28.1.7:1026
	06:46:22	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.14.234:53979 172.28.1.7:2000

	Time	Signature	Protocol	Source / Destination
	06:46:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.19:26200 172.28.1.7:5904
	06:46:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.61:50769 172.28.1.7:53413
	06:47:10	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	62.210.6.159:5069 172.28.1.7:5060
	06:47:10	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	62.210.6.159:5069 172.28.1.7:5060
	06:47:10	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	UDP	62.210.6.159:5069 172.28.1.7:5060
	06:47:26	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:57026 172.28.1.7:8888
	06:48:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.104:36996 172.28.1.7:57124
	06:48:31	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:53722 172.28.1.7:477
	06:48:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.177:56048 172.28.1.7:20000
	06:48:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.166:50776 172.28.1.7:9481
	06:49:00	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.30:57534 172.28.1.7:3306
	06:49:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.161:49176 172.28.1.7:13137
	06:50:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.87:50584 172.28.1.7:1194
	06:51:18	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.136:49313 172.28.1.7:45749
	06:51:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.241:33595 172.28.1.7:21
	06:53:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.201:44890 172.28.1.7:11453
	06:54:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:12462
	06:54:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.70:56336 172.28.1.7:2525
	06:55:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.253:51096 172.28.1.7:80
	06:56:26	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.93:35922 172.28.1.7:9633
	06:56:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:46984 172.28.1.7:8888
	06:56:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.18:56058 172.28.1.7:111
	06:57:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:8110
	06:57:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.211:55368 172.28.1.7:44344

	Time	Signature	Protocol	Source / Destination
	06:57:27	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	TCP	47.88.30.160:17050 172.28.1.7:49501
	06:57:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.237:56164 172.28.1.7:10000
	06:58:25	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.51.234.214:59806 172.28.1.7:7777
	07:00:03	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.180:55116 172.28.1.7:9028
	07:00:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.157:43729 172.28.1.7:10001
	07:00:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.166:50372 172.28.1.7:5351
	07:01:23	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.23:54567 172.28.1.7:49998
	07:01:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.247:49227 172.28.1.7:2379
	07:03:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.161:45216 172.28.1.7:20001
	07:03:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:18063
	07:03:40	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.34.74:44708 172.28.1.7:8200
	07:03:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9044
	07:04:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.209:56049 172.28.1.7:17778
	07:04:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:9221
	07:05:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.155:34791 172.28.1.7:5986
	07:06:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.225:49728 172.28.1.7:138
	07:06:27	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	207.90.244.2:29538 172.28.1.7:161
	07:07:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.139:13670 172.28.1.7:2181
	07:09:40	ET CINS Active Threat Intelligence Poor Reputation IP group 5 [1:2403304:104040] - Misc Attack	UDP	5.135.15.20:4040 172.28.1.7:5060
	07:10:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.118:55680 172.28.1.7:443
	07:10:22	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.94:33911 172.28.1.7:4500
	07:12:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.150:54928 172.28.1.7:20257
	07:12:28	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.127.157.56:33184 172.28.1.7:8140
	07:12:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.176:51562 172.28.1.7:3917

	Time	Signature	Protocol	Source / Destination
	07:12:48	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.148.168:58053 172.28.1.7:5010
	07:13:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.110:51945 172.28.1.7:5001
	07:13:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:8866
	07:15:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.103:20849 172.28.1.7:65057
	07:15:54	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.213.148.191:32890 172.28.1.7:2375
	07:16:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.64:49412 172.28.1.7:30005
	07:16:38	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.105.132.32:36518 172.28.1.7:27017
	07:16:43	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.150:53760 172.28.1.7:9811
	07:17:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:46810 172.28.1.7:50997
	07:17:15	ET CINS Active Threat Intelligence Poor Reputation IP group 60 [1:2403359:104040] - Misc Attack	TCP	41.228.170.122:45342 172.28.1.7:445
	07:18:18	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.179:49725 172.28.1.7:45194
	07:18:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:42680 172.28.1.7:5900
	07:18:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:23320 172.28.1.7:1926
	07:19:11	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.105.112:40132 172.28.1.7:8443
	07:19:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.15:19468 172.28.1.7:17
	07:19:15	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	UDP	64.62.197.15:19468 172.28.1.7:17
	07:19:39	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:23696 172.28.1.7:4899
	07:20:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.250:50280 172.28.1.7:46205
	07:20:18	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.211:57260 172.28.1.7:8845
	07:20:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.223:52321 172.28.1.7:6019
	07:21:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.243:54411 172.28.1.7:8888
	07:21:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.246:53536 172.28.1.7:11740
	07:21:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.222:52097 172.28.1.7:5353
	07:21:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:12455

	Time	Signature	Protocol	Source / Destination
	07:22:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.140:50623 172.28.1.7:51122
	07:23:03	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.153:50876 172.28.1.7:9852
	07:24:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:777
	07:24:38	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:42757 172.28.1.7:587
	07:24:50	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	159.89.115.26:61015 172.28.1.7:3306
	07:26:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.193:41429 172.28.1.7:30005
	07:26:31	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.193:41429 172.28.1.7:30005
	07:27:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.106:33242 172.28.1.7:5585
	07:28:05	ET CINS Active Threat Intelligence Poor Reputation IP group 60 [1:2403359:104040] - Misc Attack	TCP	40.76.99.43:35322 172.28.1.7:2052
	07:29:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.6:26200 172.28.1.7:8382
	07:30:18	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.79:57280 172.28.1.7:9930
	07:30:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.164:54871 172.28.1.7:50052
	07:31:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.149:34515 172.28.1.7:9601
	07:31:24	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.122.53:49136 172.28.1.7:9002
	07:31:43	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:14101
	07:32:11	ET CINS Active Threat Intelligence Poor Reputation IP group 31 [1:2403330:104040] - Misc Attack	TCP	20.64.96.205:37106 172.28.1.7:4840
	07:32:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:31674 172.28.1.7:4369
	07:33:53	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	182.9.33.245:9259 172.28.1.7:1433
	07:34:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.32:49629 172.28.1.7:49719
	07:34:27	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	UDP	20.168.122.61:37821 172.28.1.7:9200
	07:34:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:9022
	07:35:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.19:6681 172.28.1.7:8800
	07:36:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.251:49579 172.28.1.7:50001
	07:37:18	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.199:57279 172.28.1.7:17000

	Time	Signature	Protocol	Source / Destination
	07:37:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.138:2744 172.28.1.7:2087
	07:38:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.80:53017 172.28.1.7:5904
	07:38:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.229:52129 172.28.1.7:4911
	07:39:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.212:51733 172.28.1.7:8442
	07:39:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.131:5614 172.28.1.7:1962
	07:40:23	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.180.159.71:33150 172.28.1.7:8098
	07:42:24	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.51.118:43198 172.28.1.7:10012
	07:43:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.27:39236 172.28.1.7:8089
	07:43:21	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	UDP	20.169.107.188:44381 172.28.1.7:1400
	07:43:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.95:42876 172.28.1.7:4899
	07:44:00	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.175.52:37539 172.28.1.7:9300
	07:44:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:50341 172.28.1.7:2107
	07:45:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.145:47657 172.28.1.7:4840
	07:45:11	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.99:35043 172.28.1.7:6664
	07:45:25	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	UDP	8.221.141.224:34665 172.28.1.7:47808
	07:46:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.40:37170 172.28.1.7:6443
	07:47:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.87:51004 172.28.1.7:32569
	07:48:04	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.215:47167 172.28.1.7:8072
	07:48:52	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	24.43.161.216:47779 172.28.1.7:1433
	07:48:52	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.43.161.216:47779 172.28.1.7:1433
	07:49:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.230:43880 172.28.1.7:7013
	07:49:43	ET CINS Active Threat Intelligence Poor Reputation IP group 31 [1:2403330:104040] - Misc Attack	TCP	20.64.105.244:36918 172.28.1.7:5223
	07:51:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.228:50398 172.28.1.7:30050
	07:51:53	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:7349 172.28.1.7:3269

	Time	Signature	Protocol	Source / Destination
	07:51:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.71:49929 172.28.1.7:6568
	07:52:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.255:49588 172.28.1.7:102
	07:52:21	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:60731 172.28.1.7:54321
	07:52:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.48:54936 172.28.1.7:52311
	07:53:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.194:32929 172.28.1.7:18245
	07:54:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.129:47929 172.28.1.7:9001
	07:54:39	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.129:47929 172.28.1.7:9001
	07:55:23	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.106:54819 172.28.1.7:45452
	07:55:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.19:49708 172.28.1.7:50002
	07:55:51	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.19:49708 172.28.1.7:50002
	07:56:17	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.80.105.157:58155 172.28.1.7:7443
	07:56:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.253:52237 172.28.1.7:8020
	07:57:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.94:55621 172.28.1.7:20123
	07:58:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.52:34221 172.28.1.7:8010
	07:58:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:20202
	07:59:20	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.80.250:46867 172.28.1.7:11741
	07:59:36	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	51.158.61.186:61001 172.28.1.7:80
	08:00:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.251:52501 172.28.1.7:25791
	08:00:42	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:60614 172.28.1.7:51080
	08:00:59	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:3190
	08:01:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.190:56648 172.28.1.7:447
	08:01:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.153:4959 172.28.1.7:55615
	08:01:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.128:36497 172.28.1.7:8090
	08:01:55	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.128:36497 172.28.1.7:8090

	Time	Signature	Protocol	Source / Destination
	08:02:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.215:48647 172.28.1.7:8090
	08:02:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.2:26810 172.28.1.7:5060
	08:02:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.86:56839 172.28.1.7:8159
	08:03:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:29011 172.28.1.7:52869
	08:03:45	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.148:49246 172.28.1.7:23942
	08:04:10	ET CINS Active Threat Intelligence Poor Reputation IP group 38 [1:2403337:104040] - Misc Attack	TCP	20.98.137.25:46646 172.28.1.7:8443
	08:04:20	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.79.149.213:43117 172.28.1.7:2222
	08:05:03	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.136:55481 172.28.1.7:1086
	08:06:21	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:37745 172.28.1.7:8100
	08:08:44	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:40840 172.28.1.7:161
	08:08:49	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	198.98.59.238:5067 172.28.1.7:5060
	08:08:49	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	198.98.59.238:5067 172.28.1.7:5060
	08:09:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.109:49807 172.28.1.7:53524
	08:09:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:3333
	08:09:29	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.91.249:53594 172.28.1.7:8900
	08:09:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.27:53353 172.28.1.7:64719
	08:10:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.151:44879 172.28.1.7:85
	08:10:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.155:27409 172.28.1.7:15000
	08:10:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.162:52247 172.28.1.7:23
	08:11:03	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.34:57191 172.28.1.7:45315
	08:11:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:62080
	08:11:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.216:40319 172.28.1.7:87
	08:12:23	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.253:53481 172.28.1.7:47687
	08:14:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.104:46082 172.28.1.7:42767

	Time	Signature	Protocol	Source / Destination
	08:15:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.242:39786 172.28.1.7:2191
	08:16:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.197:55098 172.28.1.7:13978
	08:16:10	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.49.185:38558 172.28.1.7:8464
	08:16:14	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	TCP	47.88.6.181:54003 172.28.1.7:11027
	08:16:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9246
	08:16:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.130:54337 172.28.1.7:19422
	08:16:58	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.133:50574 172.28.1.7:9860
	08:17:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.75:56355 172.28.1.7:4332
	08:17:27	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:33418 172.28.1.7:3333
	08:17:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.104:56341 172.28.1.7:1434
	08:17:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.85:52651 172.28.1.7:3978
	08:17:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.88:53666 172.28.1.7:8800
	08:19:19	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:38568 172.28.1.7:24003
	08:19:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.67:23367 172.28.1.7:623
	08:19:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.220:52815 172.28.1.7:465
	08:19:30	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.5.243:60324 172.28.1.7:9042
	08:19:58	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.52.128:23573 172.28.1.7:12313
	08:20:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.102:54388 172.28.1.7:12025
	08:20:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.184:53833 172.28.1.7:30010
	08:20:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.126:49667 172.28.1.7:995
	08:20:36	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.126:49667 172.28.1.7:995
	08:21:47	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	218.1.144.181:54381 172.28.1.7:1433
	08:21:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.63:60437 172.28.1.7:2031
	08:22:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	113.141.171.139:56012 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	08:22:45	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:59907 172.28.1.7:8087
	08:22:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:56639 172.28.1.7:22222
	08:22:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.25:8584 172.28.1.7:3391
	08:23:18	ET CINS Active Threat Intelligence Poor Reputation IP group 93 [1:2403392:104040] - Misc Attack	UDP	59.55.128.147:1434 172.28.1.7:8082
	08:23:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	113.141.171.139:34102 172.28.1.7:22
	08:23:55	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	113.141.171.139:37263 172.28.1.7:22
	08:24:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:12293
	08:25:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.188:41124 172.28.1.7:800
	08:26:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	113.141.171.139:53075 172.28.1.7:22
	08:26:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.95:51177 172.28.1.7:4018
	08:26:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.147:56484 172.28.1.7:808
	08:27:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:1444
	08:27:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.171:52584 172.28.1.7:2484
	08:28:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.168:55770 172.28.1.7:20256
	08:29:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.64:51112 172.28.1.7:3905
	08:30:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:9054
	08:31:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.68:49285 172.28.1.7:5902
	08:31:24	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	113.141.171.139:56501 172.28.1.7:22
	08:32:36	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:55964 172.28.1.7:8117
	08:32:43	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:36153 172.28.1.7:7547
	08:33:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.251:53155 172.28.1.7:9443
	08:33:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.231:37259 172.28.1.7:3351
	08:33:53	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.127.104:43072 172.28.1.7:3001
	08:34:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:10009

	Time	Signature	Protocol	Source / Destination
	08:34:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.50:30192 172.28.1.7:3478
	08:34:42	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:47691 172.28.1.7:476
	08:35:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.169:50121 172.28.1.7:12443
	08:35:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.124:50919 172.28.1.7:9501
	08:35:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.90:50099 172.28.1.7:139
	08:35:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:37727 172.28.1.7:5900
	08:35:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:9198
	08:36:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.181:52282 172.28.1.7:10252
	08:36:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:35002
	08:36:50	ET CINS Active Threat Intelligence Poor Reputation IP group 58 [1:2403357:104040] - Misc Attack	TCP	40.124.174.207:52055 172.28.1.7:8888
	08:36:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	193.163.125.202:20885 172.28.1.7:44317
	08:37:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:5544
	08:37:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:48949 172.28.1.7:2096
	08:37:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.247:48949 172.28.1.7:80
	08:38:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:4443
	08:38:51	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:4443
	08:38:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.108:50520 172.28.1.7:1244
	08:39:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.226:51390 172.28.1.7:5001
	08:39:01	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:36245 172.28.1.7:445
	08:39:51	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.60.206:36693 172.28.1.7:8581
	08:40:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.89:55810 172.28.1.7:9468
	08:41:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.159:54683 172.28.1.7:4444
	08:41:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	114.242.61.9:35948 172.28.1.7:22
	08:41:58	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.49:49572 172.28.1.7:9440

	Time	Signature	Protocol	Source / Destination
	08:42:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.40:49774 172.28.1.7:8081
	08:43:18	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.25:49156 172.28.1.7:9396
	08:43:30	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.140.140.15:34435 172.28.1.7:2222
	08:43:31	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	114.242.61.9:57878 172.28.1.7:22
	08:43:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.156:52334 172.28.1.7:9090
	08:43:36	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.156:52334 172.28.1.7:9090
	08:43:54	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.39.178:43964 172.28.1.7:2070
	08:44:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.186:56295 172.28.1.7:3306
	08:44:10	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	205.210.31.186:56295 172.28.1.7:3306
	08:45:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.212:55126 172.28.1.7:389
	08:45:45	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.105.85:14832 172.28.1.7:9100
	08:46:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.11:57951 172.28.1.7:8083
	08:47:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.182:29870 172.28.1.7:16992
	08:47:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.117:44690 172.28.1.7:3389
	08:47:07	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.117:44690 172.28.1.7:3389
	08:47:08	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.3:54676 172.28.1.7:47522
	08:47:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.179:27280 172.28.1.7:445
	08:48:23	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.194:52936 172.28.1.7:48180
	08:49:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:9043
	08:49:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.188:19354 172.28.1.7:28080
	08:50:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12141
	08:50:01	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12141
	08:50:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.144:54252 172.28.1.7:2079
	08:51:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.220:50252 172.28.1.7:45691

	Time	Signature	Protocol	Source / Destination
	08:51:39	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	188.136.222.140:56908 172.28.1.7:1433
	08:51:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.99:9580 172.28.1.7:8090
	08:52:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.91:49600 172.28.1.7:52200
	08:53:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.190:56903 172.28.1.7:45595
	08:53:13	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	UDP	20.168.7.215:50707 172.28.1.7:80
	08:53:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.155:47508 172.28.1.7:1913
	08:54:18	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.252:50900 172.28.1.7:23502
	08:55:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.47:53478 172.28.1.7:51007
	08:55:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.30:47079 172.28.1.7:53
	08:55:37	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:43080
	08:56:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.218:50935 172.28.1.7:5632
	08:56:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.255:51404 172.28.1.7:1112
	08:57:11	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	79.124.49.134:43331 172.28.1.7:1433
	08:57:29	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	UDP	20.168.7.149:59625 172.28.1.7:981
	08:57:51	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:57740 172.28.1.7:31112
	08:58:55	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	46.101.112.70:45240 172.28.1.7:11000
	08:58:56	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.84.165:28736 172.28.1.7:9094
	08:59:25	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.64.104.155:46214 172.28.1.7:5903
	09:00:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.82:53093 172.28.1.7:161
	09:01:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.59:51540 172.28.1.7:4434
	09:02:39	ET CINS Active Threat Intelligence Poor Reputation IP group 15 [1:2403314:104040] - Misc Attack	TCP	20.118.225.13:53276 172.28.1.7:2049
	09:04:18	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.165:56251 172.28.1.7:49171
	09:04:21	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.169.104.179:51540 172.28.1.7:8083
	09:04:27	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:52329 172.28.1.7:60000

	Time	Signature	Protocol	Source / Destination
	09:07:07	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.109:49280 172.28.1.7:46581
	09:07:40	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:14898 172.28.1.7:5222
	09:08:51	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	UDP	47.251.92.171:500 172.28.1.7:500
	09:09:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.178:56895 172.28.1.7:9766
	09:09:43	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.136:56014 172.28.1.7:73
	09:10:12	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.216.83.147:51715 172.28.1.7:23
	09:10:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.14:51022 172.28.1.7:177
	09:10:19	GPL RPC xdmcp info query [1:2101867:2] - Attempted Information Leak	UDP	64.62.156.14:51022 172.28.1.7:177
	09:11:16	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.32:45990 172.28.1.7:3306
	09:12:17	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.161:46745 172.28.1.7:8022
	09:13:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.19:26200 172.28.1.7:5239
	09:13:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.230:53376 172.28.1.7:47001
	09:14:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.163:33576 172.28.1.7:8041
	09:14:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.251:42469 172.28.1.7:1992
	09:14:39	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.59:55143 172.28.1.7:23107
	09:15:35	ET CINS Active Threat Intelligence Poor Reputation IP group 60 [1:2403359:104040] - Misc Attack	TCP	40.80.206.215:36035 172.28.1.7:2083
	09:15:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.74:57136 172.28.1.7:5910
	09:16:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:52965 172.28.1.7:7711
	09:16:22	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	UDP	47.251.73.174:22159 172.28.1.7:2123
	09:17:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:56579 172.28.1.7:8102
	09:17:58	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.108:50213 172.28.1.7:30220
	09:18:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.181:55932 172.28.1.7:2002
	09:19:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.27:51348 172.28.1.7:5080
	09:19:50	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.99:51790 172.28.1.7:4282

	Time	Signature	Protocol	Source / Destination
	09:20:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:8195
	09:20:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.141:3719 172.28.1.7:143
	09:21:28	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.103:49478 172.28.1.7:49689
	09:21:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.204:51084 172.28.1.7:4080
	09:22:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.51:19137 172.28.1.7:7549
	09:22:57	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	UDP	8.219.8.175:54686 172.28.1.7:1900
	09:23:00	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.194.88:42470 172.28.1.7:3389
	09:23:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.211:56239 172.28.1.7:20211
	09:24:13	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.28:49737 172.28.1.7:12019
	09:25:53	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.251:52874 172.28.1.7:31642
	09:26:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.217:51336 172.28.1.7:61616
	09:26:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.51:59367 172.28.1.7:4433
	09:26:53	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.116:49281 172.28.1.7:9209
	09:27:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.227:43871 172.28.1.7:139
	09:27:24	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:29011 172.28.1.7:1925
	09:28:22	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.150.201.181:48944 172.28.1.7:1194
	09:28:31	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.45.170:47087 172.28.1.7:8991
	09:29:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.10:14903 172.28.1.7:111
	09:29:01	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	207.90.244.10:14903 172.28.1.7:111
	09:29:01	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.75:45076 172.28.1.7:21025
	09:30:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:12243
	09:30:18	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.8:57133 172.28.1.7:9657
	09:30:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.59:61733 172.28.1.7:8001
	09:30:46	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.36:47267 172.28.1.7:3306

	Time	Signature	Protocol	Source / Destination
	09:30:48	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.82.243:54650 172.28.1.7:7776
	09:31:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.147:47422 172.28.1.7:8001
	09:31:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:6861 172.28.1.7:110
	09:32:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.102:49407 172.28.1.7:53631
	09:32:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.202:60890 172.28.1.7:49668
	09:33:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9496
	09:33:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:8444
	09:34:01	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.189:55179 172.28.1.7:4786
	09:34:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.232:49171 172.28.1.7:21242
	09:34:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:29011 172.28.1.7:8090
	09:35:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:21314
	09:35:13	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.171.30.213:43737 172.28.1.7:6066
	09:35:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.65:51205 172.28.1.7:11443
	09:36:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.239:52124 172.28.1.7:15276
	09:36:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.155:57546 172.28.1.7:51005
	09:36:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.222:43357 172.28.1.7:3369
	09:37:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.147:40677 172.28.1.7:6080
	09:37:21	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	UDP	8.216.65.177:18317 172.28.1.7:17185
	09:37:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.236:53521 172.28.1.7:83
	09:38:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.225:34244 172.28.1.7:135
	09:38:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.230:55367 172.28.1.7:7682
	09:38:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.135:26549 172.28.1.7:17185
	09:39:35	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	88.147.153.84:30170 172.28.1.7:3306
	09:39:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:24404 172.28.1.7:7634

	Time	Signature	Protocol	Source / Destination
	09:39:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.44:56370 172.28.1.7:7547
	09:40:47	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:56418 172.28.1.7:666
	09:41:06	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	88.147.153.84:31031 172.28.1.7:1433
	09:42:19	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.150.201.239:48624 172.28.1.7:435
	09:42:40	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	45.142.154.10:58914 172.28.1.7:53
	09:42:40	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	UDP	45.142.154.10:58914 172.28.1.7:53
	09:42:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	45.142.154.10:58914 172.28.1.7:53
	09:43:11	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	UDP	20.169.105.41:56859 172.28.1.7:5093
	09:43:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:22367 172.28.1.7:14265
	09:44:10	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:39495 172.28.1.7:85
	09:44:12	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:18044
	09:45:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.50:27670 172.28.1.7:19
	09:45:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:45556 172.28.1.7:3389
	09:45:34	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.73:43456 172.28.1.7:6668
	09:45:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.65:53293 172.28.1.7:11495
	09:45:49	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:43165 172.28.1.7:1701
	09:46:34	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:20018
	09:46:40	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	106.58.117.72:3534 172.28.1.7:1433
	09:47:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.19:50189 172.28.1.7:17689
	09:48:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.171:57909 172.28.1.7:800
	09:48:46	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.89:38996 172.28.1.7:31337
	09:49:09	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.87:39002 172.28.1.7:10324
	09:49:11	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.68:38992 172.28.1.7:25105
	09:50:04	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.127.185.20:40531 172.28.1.7:8981

	Time	Signature	Protocol	Source / Destination
	09:50:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.35:33190 172.28.1.7:3000
	09:50:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:9044
	09:51:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.119:51900 172.28.1.7:9278
	09:51:55	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:51519 172.28.1.7:30002
	09:52:07	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	146.190.223.163:40491 172.28.1.7:5432
	09:52:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:9169
	09:52:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.229:50423 172.28.1.7:111
	09:55:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.118:55742 172.28.1.7:20257
	09:55:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.107:55538 172.28.1.7:60241
	09:56:07	ET INFO User-Agent (python-requests) Inbound to Webserver [1:2017515:8] - Misc activity	TCP	34.79.159.68:46476 172.28.1.7:444
	09:56:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.101:55578 172.28.1.7:1701
	09:56:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:59888 172.28.1.7:60022
	09:57:06	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:8641
	09:57:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.139:38518 172.28.1.7:2
	09:58:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.185:39180 172.28.1.7:11453
	09:59:54	ET CINS Active Threat Intelligence Poor Reputation IP group 15 [1:2403314:104040] - Misc Attack	TCP	20.118.224.96:42613 172.28.1.7:80
	10:00:17	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:52500 172.28.1.7:988
	10:00:28	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.221:56151 172.28.1.7:10038
	10:01:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.120:51984 172.28.1.7:3443
	10:01:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:8056
	10:02:15	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.42.108.100:35432 172.28.1.7:7574
	10:02:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:34600 172.28.1.7:5900
	10:03:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.253:51127 172.28.1.7:45560
	10:05:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.16:26200 172.28.1.7:8867

	Time	Signature	Protocol	Source / Destination
	10:05:47	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	52.14.58.0:57147 172.28.1.7:1433
	10:05:47	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:57147 172.28.1.7:1433
	10:07:23	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:46607 172.28.1.7:65535
	10:07:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.249:56452 172.28.1.7:7001
	10:07:56	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:55293 172.28.1.7:10003
	10:08:07	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	2.59.22.234:23320 172.28.1.7:2376
	10:08:10	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.187:49754 172.28.1.7:34423
	10:08:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.234:53654 172.28.1.7:10259
	10:08:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	46.4.85.81:5440 172.28.1.7:22
	10:08:52	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:51526 172.28.1.7:22226
	10:09:06	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	46.4.85.81:64924 172.28.1.7:22
	10:09:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.129:13453 172.28.1.7:20546
	10:10:15	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:51825 172.28.1.7:24002
	10:10:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.113:51395 172.28.1.7:20256
	10:11:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	46.4.85.81:54118 172.28.1.7:22
	10:11:09	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.192.214:53342 172.28.1.7:8181
	10:11:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.212:41550 172.28.1.7:8531
	10:12:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.3:34584 172.28.1.7:8082
	10:12:14	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:42320 172.28.1.7:30001
	10:12:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.134:50703 172.28.1.7:15588
	10:12:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.66:52479 172.28.1.7:1200
	10:12:43	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.62:56144 172.28.1.7:28140
	10:12:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.219:53105 172.28.1.7:4567
	10:13:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.162:50982 172.28.1.7:1883

	Time	Signature	Protocol	Source / Destination
	10:13:56	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.8.207:35566 172.28.1.7:8165
	10:15:48	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.210.99:56285 172.28.1.7:46865
	10:15:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.113:51690 172.28.1.7:11211
	10:15:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.107:14412 172.28.1.7:28470
	10:16:34	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:42267 172.28.1.7:60000
	10:17:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:45225 172.28.1.7:6000
	10:17:50	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.0.72:52267 172.28.1.7:8005
	10:18:00	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5578 172.28.1.7:5060
	10:18:00	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5578 172.28.1.7:5060
	10:18:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:8833
	10:18:38	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.32.79:39927 172.28.1.7:1527
	10:18:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.58:52820 172.28.1.7:12694
	10:19:43	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.78:53312 172.28.1.7:8841
	10:20:54	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	TCP	20.169.107.169:59239 172.28.1.7:1311
	10:21:35	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	185.243.5.136:5068 172.28.1.7:5060
	10:21:35	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	185.243.5.136:5068 172.28.1.7:5060
	10:22:18	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.80:34411 172.28.1.7:195
	10:23:08	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.135:55512 172.28.1.7:12222
	10:23:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	140.246.235.47:41858 172.28.1.7:22
	10:23:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.37:58524 172.28.1.7:3389
	10:24:57	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	185.243.5.106:5611 172.28.1.7:5060
	10:24:57	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	185.243.5.106:5611 172.28.1.7:5060
	10:27:14	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	146.88.241.63:58074 172.28.1.7:111
	10:27:25	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.90:43043 172.28.1.7:20256

	Time	Signature	Protocol	Source / Destination
	10:27:32	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.78.164:59962 172.28.1.7:12382
	10:27:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.99:52400 172.28.1.7:2087
	10:28:04	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.83:43036 172.28.1.7:11371
	10:28:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	140.246.235.47:57406 172.28.1.7:22
	10:28:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.244:55512 172.28.1.7:808
	10:28:56	ET CINS Active Threat Intelligence Poor Reputation IP group 69 [1:2403368:104040] - Misc Attack	TCP	45.156.129.96:35451 172.28.1.7:53
	10:29:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.106:55048 172.28.1.7:502
	10:29:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:1207
	10:31:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.150:22499 172.28.1.7:9201
	10:31:58	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:26200 172.28.1.7:15151
	10:32:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.241:56027 172.28.1.7:54528
	10:32:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.254:49179 172.28.1.7:3344
	10:32:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.200:55017 172.28.1.7:4020
	10:33:04	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:42000 172.28.1.7:8000
	10:33:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.39:56575 172.28.1.7:9192
	10:33:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.149:42343 172.28.1.7:53
	10:33:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:49238 172.28.1.7:3389
	10:34:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.97:57099 172.28.1.7:9001
	10:34:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.213:49457 172.28.1.7:427
	10:35:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.194:49226 172.28.1.7:5672
	10:35:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.30:55925 172.28.1.7:427
	10:36:06	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.171.8.87:53620 172.28.1.7:8889
	10:36:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.223:56523 172.28.1.7:9100
	10:37:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.15:26200 172.28.1.7:12575

	Time	Signature	Protocol	Source / Destination
	10:37:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8181
	10:37:39	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8181
	10:38:04	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.56:15448 172.28.1.7:8237
	10:38:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.110:53116 172.28.1.7:50003
	10:39:12	ET CINS Active Threat Intelligence Poor Reputation IP group 57 [1:2403356:104040] - Misc Attack	TCP	40.119.46.97:39280 172.28.1.7:1212
	10:39:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:45141 172.28.1.7:1748
	10:40:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.91:49629 172.28.1.7:9002
	10:40:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.73:51729 172.28.1.7:38080
	10:43:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.39:56070 172.28.1.7:10255
	10:43:15	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.105.127:36927 172.28.1.7:554
	10:44:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:12191
	10:44:42	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.12.240.9:51287 172.28.1.7:995
	10:44:44	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	45.135.95.25:39140 172.28.1.7:111
	10:45:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:9710
	10:45:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.203:54834 172.28.1.7:9002
	10:45:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.84:51159 172.28.1.7:20122
	10:46:03	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.182:53457 172.28.1.7:9181
	10:46:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.168:13079 172.28.1.7:10161
	10:46:05	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	UDP	64.62.197.168:13079 172.28.1.7:10161
	10:46:06	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	74.63.235.245:5060 172.28.1.7:5060
	10:46:06	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	74.63.235.245:5060 172.28.1.7:5060
	10:46:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.158:15702 172.28.1.7:623
	10:46:30	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:21249
	10:46:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:3151

	Time	Signature	Protocol	Source / Destination
	10:47:51	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.121.45.222:38755 172.28.1.7:5181
	10:49:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:52060 172.28.1.7:22
	10:49:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.84:49268 172.28.1.7:2001
	10:49:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.73:60115 172.28.1.7:3389
	10:49:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:7980
	10:49:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:8189
	10:49:50	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	UDP	46.23.108.218:48481 172.28.1.7:30301
	10:50:38	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.157:52283 172.28.1.7:28420
	10:51:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.130:52510 172.28.1.7:26363
	10:52:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:12194
	10:52:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.42:52269 172.28.1.7:9191
	10:53:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.170:57121 172.28.1.7:45604
	10:53:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.47:52461 172.28.1.7:143
	10:53:44	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.73.94:14404 172.28.1.7:10018
	10:54:08	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.127:56793 172.28.1.7:9625
	10:54:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.220:48704 172.28.1.7:8089
	10:55:08	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.72.122:47695 172.28.1.7:10080
	10:55:57	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:40380 172.28.1.7:2049
	10:56:30	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.142.108:48116 172.28.1.7:12558
	10:56:38	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	51.79.2.27:52536 172.28.1.7:6000
	10:59:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	139.19.117.130:38492 172.28.1.7:22
	10:59:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.247:35772 172.28.1.7:31781
	11:00:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:8412
	11:00:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.54:23214 172.28.1.7:2123

	Time	Signature	Protocol	Source / Destination
	11:00:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.46:51697 172.28.1.7:7070
	11:01:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.106:49400 172.28.1.7:1723
	11:02:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.223:52350 172.28.1.7:6002
	11:03:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.251:33921 172.28.1.7:27006
	11:03:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.157:15710 172.28.1.7:1000
	11:04:05	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.121:49604 172.28.1.7:34471
	11:04:06	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.243.250:12674 172.28.1.7:8117
	11:05:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.18:48294 172.28.1.7:2152
	11:05:18	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.111:50794 172.28.1.7:47864
	11:05:28	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.177:49579 172.28.1.7:20193
	11:05:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:10100
	11:05:46	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.42.61.148:58403 172.28.1.7:123
	11:07:13	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:37863 172.28.1.7:81
	11:07:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.241:56122 172.28.1.7:28729
	11:07:16	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:8383
	11:07:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.229:35129 172.28.1.7:8081
	11:07:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.97:53540 172.28.1.7:4022
	11:07:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:29011 172.28.1.7:51106
	11:08:00	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.156.128.129:33413 172.28.1.7:503
	11:08:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.155:41298 172.28.1.7:8001
	11:08:43	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.193:49679 172.28.1.7:48088
	11:08:59	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.55.35.217:37415 172.28.1.7:2077
	11:09:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.70:54148 172.28.1.7:5351
	11:10:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.2:21442 172.28.1.7:10001

	Time	Signature	Protocol	Source / Destination
	11:10:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.250:54774 172.28.1.7:6001
	11:10:11	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.180:55242 172.28.1.7:8091
	11:10:23	ET CINS Active Threat Intelligence Poor Reputation IP group 57 [1:2403356:104040] - Misc Attack	TCP	40.124.120.52:42972 172.28.1.7:7473
	11:12:18	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.211:53513 172.28.1.7:46688
	11:13:08	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.11:57151 172.28.1.7:9237
	11:13:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.163:49836 172.28.1.7:5050
	11:13:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.222:34047 172.28.1.7:13411
	11:16:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.202:54247 172.28.1.7:33889
	11:16:36	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	207.90.244.21:20270 172.28.1.7:3306
	11:17:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.118:56301 172.28.1.7:51401
	11:17:39	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:52736 172.28.1.7:8880
	11:18:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.94:52049 172.28.1.7:8888
	11:18:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.243:54859 172.28.1.7:20256
	11:18:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.12:38945 172.28.1.7:8888
	11:19:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.100:33954 172.28.1.7:5985
	11:19:08	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.62.197.100:33954 172.28.1.7:5985
	11:20:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.90:52515 172.28.1.7:4025
	11:21:02	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.117:47348 172.28.1.7:8000
	11:21:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.200:34520 172.28.1.7:2121
	11:21:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.103:30631 172.28.1.7:3620
	11:22:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.246:55618 172.28.1.7:59382
	11:22:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.207:52112 172.28.1.7:3128
	11:22:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:37386 172.28.1.7:5900
	11:22:58	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.150.201.239:42693 172.28.1.7:83

	Time	Signature	Protocol	Source / Destination
	11:24:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.195:38940 172.28.1.7:2031
	11:24:41	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.195:38940 172.28.1.7:2031
	11:25:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.16:26200 172.28.1.7:7018
	11:26:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9421
	11:26:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:20
	11:26:28	ET CINS Active Threat Intelligence Poor Reputation IP group 57 [1:2403356:104040] - Misc Attack	TCP	40.119.33.98:47870 172.28.1.7:60001
	11:26:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.62:36720 172.28.1.7:2087
	11:26:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.189:55910 172.28.1.7:2096
	11:27:31	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	115.190.12.52:49394 172.28.1.7:22
	11:30:01	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:53829 172.28.1.7:4443
	11:30:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:24858 172.28.1.7:33060
	11:31:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:23320 172.28.1.7:47990
	11:32:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.139:57818 172.28.1.7:830
	11:32:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.101:4138 172.28.1.7:19736
	11:32:41	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.141.82:18435 172.28.1.7:3100
	11:33:03	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.139:54507 172.28.1.7:9511
	11:33:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.140:2379 172.28.1.7:3390
	11:33:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.207:35062 172.28.1.7:9990
	11:34:27	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.95:50684 172.28.1.7:63322
	11:35:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.155:55756 172.28.1.7:6380
	11:35:58	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.43.53:37210 172.28.1.7:8445
	11:36:07	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.92:45767 172.28.1.7:1443
	11:36:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.161:53300 172.28.1.7:9200
	11:36:14	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.161:53300 172.28.1.7:9200

	Time	Signature	Protocol	Source / Destination
	11:38:43	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.189:51711 172.28.1.7:55916
	11:39:02	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.237.115.77:19169 172.28.1.7:6308
	11:39:24	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:18104 172.28.1.7:2003
	11:39:49	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:58028 172.28.1.7:9595
	11:40:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.116:54468 172.28.1.7:57998
	11:40:56	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.88.12:46021 172.28.1.7:8061
	11:41:20	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.237.86.37:31092 172.28.1.7:8842
	11:43:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.61:55760 172.28.1.7:22
	11:43:28	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	UDP	35.203.210.249:53949 172.28.1.7:24800
	11:43:48	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.192.151:53913 172.28.1.7:3479
	11:44:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.227:47127 172.28.1.7:9001
	11:45:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.227:51309 172.28.1.7:48523
	11:45:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:49002 172.28.1.7:22
	11:46:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.159:58449 172.28.1.7:44817
	11:46:22	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.104.5:36242 172.28.1.7:502
	11:46:26	ET CINS Active Threat Intelligence Poor Reputation IP group 85 [1:2403384:104040] - Misc Attack	TCP	51.15.220.227:55581 172.28.1.7:408
	11:46:26	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	212.200.127.112:59781 172.28.1.7:1433
	11:46:29	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	212.200.127.112:59781 172.28.1.7:1433
	11:46:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.154:5292 172.28.1.7:8888
	11:46:40	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	212.200.127.112:62715 172.28.1.7:3306
	11:46:43	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	212.200.127.112:62715 172.28.1.7:3306
	11:47:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.219:39860 172.28.1.7:8123
	11:47:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.217:50701 172.28.1.7:45271
	11:47:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.8.202:36760 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	11:47:59	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.122.19:48715 172.28.1.7:2455
	11:47:59	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.169.49.63:54021 172.28.1.7:3000
	11:48:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.189:50957 172.28.1.7:2086
	11:48:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.38:59997 172.28.1.7:8123
	11:48:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:60356 172.28.1.7:22
	11:48:41	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	TCP	47.93.97.12:42132 172.28.1.7:2222
	11:48:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.36:43584 172.28.1.7:3000
	11:49:11	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:38341 172.28.1.7:9020
	11:49:28	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.185:54749 172.28.1.7:9633
	11:49:37	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	197.39.208.98:50694 172.28.1.7:1433
	11:50:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.8.202:44544 172.28.1.7:22
	11:50:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:42786 172.28.1.7:22
	11:50:44	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.90:50950 172.28.1.7:7013
	11:51:11	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:39049 172.28.1.7:8001
	11:51:28	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.123:54951 172.28.1.7:18094
	11:51:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.230:38449 172.28.1.7:32802
	11:51:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:42802 172.28.1.7:1801
	11:52:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:9073
	11:52:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.8.202:38816 172.28.1.7:22
	11:52:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:44234 172.28.1.7:22
	11:54:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.27:64358 172.28.1.7:80
	11:54:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.8.202:57522 172.28.1.7:22
	11:54:25	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:53791 172.28.1.7:7777
	11:54:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.185:56580 172.28.1.7:3389

	Time	Signature	Protocol	Source / Destination
	11:54:34	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5724 172.28.1.7:5060
	11:54:34	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5724 172.28.1.7:5060
	11:54:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:38004 172.28.1.7:22
	11:55:07	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:42792 172.28.1.7:8083
	11:56:20	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.127.149:33894 172.28.1.7:8880
	11:56:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.18:26200 172.28.1.7:5070
	11:56:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:47850 172.28.1.7:22
	11:58:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.221:57020 172.28.1.7:45826
	11:58:40	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:43570 172.28.1.7:22
	11:58:51	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:49358 172.28.1.7:1080
	11:59:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.28:20041 172.28.1.7:22
	11:59:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:17340 172.28.1.7:80
	12:00:33	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.81:50146 172.28.1.7:46827
	12:00:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:48076 172.28.1.7:22
	12:01:21	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.84:37694 172.28.1.7:2000
	12:01:53	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.19:54288 172.28.1.7:21600
	12:02:03	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.194:51980 172.28.1.7:61022
	12:02:11	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:51875 172.28.1.7:1080
	12:02:14	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:54330 172.28.1.7:9999
	12:02:33	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.85:51727 172.28.1.7:9444
	12:03:16	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:44244 172.28.1.7:22
	12:04:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.31:10602 172.28.1.7:10001
	12:04:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.222:48252 172.28.1.7:8086
	12:04:18	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.222:48252 172.28.1.7:8086

	Time	Signature	Protocol	Source / Destination
	12:04:21	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:45924 172.28.1.7:790
	12:04:24	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.141.173:58130 172.28.1.7:2051
	12:04:43	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:30007
	12:05:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:58450 172.28.1.7:22
	12:06:56	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.136.87:41726 172.28.1.7:10000
	12:07:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:45004 172.28.1.7:22
	12:08:35	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	UDP	8.211.51.190:57445 172.28.1.7:10001
	12:08:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.155:31415 172.28.1.7:61610
	12:08:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.35:56901 172.28.1.7:7777
	12:09:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:41164 172.28.1.7:22
	12:09:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:12109
	12:09:58	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:60879 172.28.1.7:8099
	12:11:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:35899 172.28.1.7:2259
	12:11:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.30:15875 172.28.1.7:523
	12:11:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:41664 172.28.1.7:22
	12:11:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:8536
	12:11:45	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.71:50875 172.28.1.7:8885
	12:11:48	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	UDP	20.169.104.179:50037 172.28.1.7:22
	12:13:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8088
	12:13:00	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8088
	12:13:03	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5122 172.28.1.7:5060
	12:13:03	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5122 172.28.1.7:5060
	12:13:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.235:42802 172.28.1.7:30005
	12:13:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:50224 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	12:15:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:57286 172.28.1.7:22
	12:16:52	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.34:50724 172.28.1.7:48967
	12:17:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.155:35345 172.28.1.7:61610
	12:17:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:41658 172.28.1.7:22
	12:18:03	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.105:48581 172.28.1.7:21
	12:18:32	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.86:57262 172.28.1.7:9612
	12:19:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:20325
	12:19:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.12:55133 172.28.1.7:5081
	12:20:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:46276 172.28.1.7:22
	12:20:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.114:8040 172.28.1.7:137
	12:20:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:54923 172.28.1.7:3389
	12:21:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.232:42802 172.28.1.7:104
	12:21:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.50:58053 172.28.1.7:4080
	12:21:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:53813 172.28.1.7:22
	12:22:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:55084 172.28.1.7:22
	12:22:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:8551
	12:22:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.67:9272 172.28.1.7:500
	12:22:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.250:43381 172.28.1.7:65002
	12:23:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.147:43657 172.28.1.7:6134
	12:23:47	ET CINS Active Threat Intelligence Poor Reputation IP group 68 [1:2403367:104040] - Misc Attack	TCP	45.156.129.48:17134 172.28.1.7:502
	12:24:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:34284 172.28.1.7:22
	12:24:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.200:39166 172.28.1.7:6081
	12:24:37	ET CINS Active Threat Intelligence Poor Reputation IP group 15 [1:2403314:104040] - Misc Attack	TCP	20.106.57.122:38716 172.28.1.7:10250
	12:26:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:53508 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	12:26:25	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.140.140.15:42718 172.28.1.7:80
	12:26:33	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.63:51124 172.28.1.7:10050
	12:27:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:29921 172.28.1.7:19
	12:27:13	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.8:49353 172.28.1.7:49855
	12:27:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2087
	12:27:23	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2087
	12:27:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:55445 172.28.1.7:3389
	12:28:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:58722 172.28.1.7:22
	12:28:30	ET CINS Active Threat Intelligence Poor Reputation IP group 57 [1:2403356:104040] - Misc Attack	TCP	40.124.120.41:55830 172.28.1.7:514
	12:28:46	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.156.128.150:17758 172.28.1.7:4434
	12:29:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.119:54910 172.28.1.7:9869
	12:29:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:51314 172.28.1.7:22
	12:29:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:8475
	12:30:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.48:35104 172.28.1.7:4646
	12:30:21	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.144.90:58120 172.28.1.7:445
	12:30:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:57834 172.28.1.7:22
	12:30:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:56696 172.28.1.7:264
	12:31:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.180:53319 172.28.1.7:44819
	12:31:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:30991 172.28.1.7:8554
	12:32:08	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.6.241:40447 172.28.1.7:8983
	12:32:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.252:50992 172.28.1.7:22
	12:32:36	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:49850 172.28.1.7:22
	12:32:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:51680 172.28.1.7:3388
	12:32:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.133:56890 172.28.1.7:1322

	Time	Signature	Protocol	Source / Destination
	12:33:18	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.72:53271 172.28.1.7:49160
	12:34:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:38778 172.28.1.7:22
	12:35:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.242:34902 172.28.1.7:51443
	12:35:19	ET CINS Active Threat Intelligence Poor Reputation IP group 94 [1:2403393:104040] - Misc Attack	TCP	60.191.125.35:56983 172.28.1.7:8888
	12:35:41	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.48.165:53821 172.28.1.7:7805
	12:36:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:10020
	12:36:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:48486 172.28.1.7:22
	12:37:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.235:36781 172.28.1.7:13443
	12:37:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.150:34144 172.28.1.7:14443
	12:38:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.43:44894 172.28.1.7:61620
	12:38:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:41072 172.28.1.7:22
	12:38:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:8528
	12:39:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.191:35448 172.28.1.7:58000
	12:39:57	ET CINS Active Threat Intelligence Poor Reputation IP group 17 [1:2403316:104040] - Misc Attack	TCP	20.127.186.138:33531 172.28.1.7:623
	12:40:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.153:57239 172.28.1.7:4000
	12:40:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.77:50223 172.28.1.7:48759
	12:40:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:36708 172.28.1.7:22
	12:40:50	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.65.195.61:46161 172.28.1.7:515
	12:40:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.146:12525 172.28.1.7:18444
	12:41:49	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.105.132.35:38853 172.28.1.7:873
	12:41:50	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	23.95.186.189:58643 172.28.1.7:6689
	12:42:38	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.80:36502 172.28.1.7:1521
	12:42:38	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	45.82.76.80:36502 172.28.1.7:1521
	12:42:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:52446 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	12:42:51	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	47.91.30.193:42002 172.28.1.7:53
	12:42:51	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	UDP	47.91.30.193:42002 172.28.1.7:53
	12:42:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.218:35204 172.28.1.7:8443
	12:43:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:56895 172.28.1.7:5900
	12:44:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.4:26200 172.28.1.7:16051
	12:44:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:5439
	12:44:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9009
	12:44:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.149:39773 172.28.1.7:4730
	12:44:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:34612 172.28.1.7:22
	12:44:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.231:54724 172.28.1.7:403
	12:45:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.11:20007 172.28.1.7:6466
	12:45:14	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:5620
	12:45:20	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.121.119:43546 172.28.1.7:9443
	12:45:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.179:53362 172.28.1.7:5443
	12:46:19	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.44.115:44829 172.28.1.7:8666
	12:46:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:60430 172.28.1.7:22
	12:46:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.137:37064 172.28.1.7:6000
	12:47:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.15:54553 172.28.1.7:5801
	12:49:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:36044 172.28.1.7:22
	12:49:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.129:52419 172.28.1.7:4444
	12:49:38	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.129:52419 172.28.1.7:4444
	12:49:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.131:60466 172.28.1.7:10051
	12:50:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.35:50574 172.28.1.7:50807
	12:50:47	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:43430 172.28.1.7:8899

	Time	Signature	Protocol	Source / Destination
	12:50:49	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	UDP	8.211.43.53:15218 172.28.1.7:3671
	12:51:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:33352 172.28.1.7:22
	12:51:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.181:56493 172.28.1.7:46439
	12:52:24	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:48318 172.28.1.7:8443
	12:53:25	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.14.119:41432 172.28.1.7:10943
	12:53:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:33850 172.28.1.7:22
	12:54:43	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.203:49932 172.28.1.7:45792
	12:54:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.156:40258 172.28.1.7:57722
	12:55:40	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:40468 172.28.1.7:22
	12:55:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.15:26200 172.28.1.7:32102
	12:57:27	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.168:50132 172.28.1.7:36370
	12:57:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:36612 172.28.1.7:22
	13:00:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:42676 172.28.1.7:22
	13:00:26	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.13.222:34015 172.28.1.7:2304
	13:01:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.100:25319 172.28.1.7:42705
	13:02:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:36746 172.28.1.7:22
	13:03:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.114:34630 172.28.1.7:10000
	13:03:25	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.114:34630 172.28.1.7:10000
	13:03:28	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.121.139.167:60637 172.28.1.7:9060
	13:04:29	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.12.240.178:34580 172.28.1.7:27017
	13:04:29	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.30.205:37673 172.28.1.7:119
	13:04:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.241:54458 172.28.1.7:46693
	13:04:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:42404 172.28.1.7:22
	13:04:56	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5421 172.28.1.7:5060

	Time	Signature	Protocol	Source / Destination
	13:04:56	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5421 172.28.1.7:5060
	13:05:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.12:38015 172.28.1.7:4500
	13:05:11	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	UDP	64.62.197.12:38015 172.28.1.7:4500
	13:05:28	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.19:52344 172.28.1.7:9761
	13:06:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:12352
	13:06:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.3:22301 172.28.1.7:58603
	13:06:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:38588 172.28.1.7:22
	13:06:48	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.80.88.7:51849 172.28.1.7:5900
	13:07:43	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.148:50957 172.28.1.7:10032
	13:07:59	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	UDP	35.203.210.23:50549 172.28.1.7:6060
	13:08:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	199.45.154.185:3979 172.28.1.7:2363
	13:08:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:54604 172.28.1.7:22
	13:08:55	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:18003
	13:08:57	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.73:33200 172.28.1.7:8060
	13:09:12	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.64:56522 172.28.1.7:14433
	13:09:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.5:48042 172.28.1.7:8530
	13:10:16	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:44671 172.28.1.7:1723
	13:11:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:48974 172.28.1.7:22
	13:12:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.133:46565 172.28.1.7:5903
	13:13:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.20:32523 172.28.1.7:3283
	13:13:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:57784 172.28.1.7:22
	13:13:49	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:49688
	13:15:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:36732 172.28.1.7:22
	13:15:33	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.82:53183 172.28.1.7:55123

	Time	Signature	Protocol	Source / Destination
	13:16:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:34618 172.28.1.7:873
	13:17:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:57408 172.28.1.7:22
	13:17:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:23320 172.28.1.7:4434
	13:17:52	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.124:54672 172.28.1.7:12553
	13:18:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:12544
	13:18:22	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.157:49560 172.28.1.7:9990
	13:19:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.134:60864 172.28.1.7:853
	13:19:17	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.208:55653 172.28.1.7:37445
	13:19:45	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.15.123:49323 172.28.1.7:5353
	13:19:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:47124 172.28.1.7:22
	13:19:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.64:42850 172.28.1.7:37
	13:19:53	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.194:54541 172.28.1.7:34210
	13:20:18	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.155:43090 172.28.1.7:8899
	13:20:27	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:38566 172.28.1.7:8020
	13:20:35	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:47153 172.28.1.7:19000
	13:20:35	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.43.157:24794 172.28.1.7:8381
	13:21:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:57919 172.28.1.7:3389
	13:21:37	ET CINS Active Threat Intelligence Poor Reputation IP group 17 [1:2403316:104040] - Misc Attack	TCP	20.14.73.63:48415 172.28.1.7:7777
	13:21:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.229:54546 172.28.1.7:4443
	13:21:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:37058 172.28.1.7:22
	13:22:21	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.74.208.9:40896 172.28.1.7:5000
	13:22:28	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.240:54139 172.28.1.7:10024
	13:22:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:21295
	13:22:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.200:56632 172.28.1.7:27017

	Time	Signature	Protocol	Source / Destination
	13:22:58	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.9:51808 172.28.1.7:48722
	13:22:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:45561 172.28.1.7:161
	13:24:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:45240 172.28.1.7:22
	13:25:07	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.84:50630 172.28.1.7:20200
	13:25:23	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:49204 172.28.1.7:37777
	13:26:02	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.244:56806 172.28.1.7:19999
	13:26:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:38632 172.28.1.7:22
	13:26:42	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.135:52562 172.28.1.7:9610
	13:26:46	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.83:35574 172.28.1.7:123
	13:26:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.228:47896 172.28.1.7:32750
	13:27:30	ET CINS Active Threat Intelligence Poor Reputation IP group 64 [1:2403363:104040] - Misc Attack	TCP	45.114.127.228:62350 172.28.1.7:80
	13:27:48	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.14:57241 172.28.1.7:46113
	13:28:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.34:5435 172.28.1.7:37810
	13:28:18	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.53:54314 172.28.1.7:23909
	13:28:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.98:23353 172.28.1.7:11082
	13:28:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.127:49174 172.28.1.7:8448
	13:28:27	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:46352 172.28.1.7:10000
	13:28:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:43210 172.28.1.7:22
	13:28:51	ET CINS Active Threat Intelligence Poor Reputation IP group 84 [1:2403383:104040] - Misc Attack	TCP	48.217.82.99:44979 172.28.1.7:8998
	13:29:34	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.221.57.26:36568 172.28.1.7:2222
	13:29:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.139:53127 172.28.1.7:563
	13:30:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.104:56173 172.28.1.7:47753
	13:30:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:57522 172.28.1.7:22
	13:30:57	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	46.101.112.70:40790 172.28.1.7:12000

	Time	Signature	Protocol	Source / Destination
	13:31:13	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.123:49537 172.28.1.7:49888
	13:31:37	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:8239
	13:32:01	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	51.158.205.203:61000 172.28.1.7:22
	13:32:04	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	TCP	47.89.255.7:29504 172.28.1.7:2087
	13:32:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.155:47675 172.28.1.7:888
	13:32:50	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:58788 172.28.1.7:22
	13:32:59	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.83.167.28:35064 172.28.1.7:25565
	13:34:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.56:32923 172.28.1.7:8080
	13:34:41	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.254.148.248:12287 172.28.1.7:8005
	13:34:42	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.216.66.248:25648 172.28.1.7:10038
	13:34:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:8172
	13:34:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:49216 172.28.1.7:22
	13:35:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.197.57:43869 172.28.1.7:10074
	13:36:19	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.52:47225 172.28.1.7:139
	13:36:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.136:33017 172.28.1.7:8883
	13:37:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:60052 172.28.1.7:22
	13:37:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.75:56400 172.28.1.7:9600
	13:38:45	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.32.168:51931 172.28.1.7:61616
	13:38:55	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.156.128.112:34417 172.28.1.7:18081
	13:39:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:37320 172.28.1.7:22
	13:39:18	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.138:54851 172.28.1.7:12021
	13:39:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.148:13131 172.28.1.7:20000
	13:39:52	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:40051 172.28.1.7:3389
	13:40:53	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:34298 172.28.1.7:5672

	Time	Signature	Protocol	Source / Destination
	13:41:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:8002
	13:41:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:51938 172.28.1.7:22
	13:41:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.45:35007 172.28.1.7:8443
	13:41:22	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:49551 172.28.1.7:22
	13:41:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.25:3034 172.28.1.7:20002
	13:42:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:8108 172.28.1.7:9999
	13:42:25	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:33046 172.28.1.7:993
	13:42:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.197:57335 172.28.1.7:45111
	13:42:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.200:54226 172.28.1.7:58443
	13:43:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:52654 172.28.1.7:22
	13:43:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.240:33200 172.28.1.7:52229
	13:44:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.189:41570 172.28.1.7:4460
	13:44:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.94:43913 172.28.1.7:548
	13:44:44	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:58587 172.28.1.7:10080
	13:44:53	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.75:54857 172.28.1.7:6316
	13:45:12	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.11:50533 172.28.1.7:8415
	13:45:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.188:51260 172.28.1.7:9750
	13:45:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:49578 172.28.1.7:22
	13:46:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:189
	13:47:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:51680 172.28.1.7:3702
	13:47:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:53608 172.28.1.7:22
	13:47:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.93:45927 172.28.1.7:8000
	13:47:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.19:64009 172.28.1.7:8880
	13:48:13	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.81.196:53756 172.28.1.7:9212

	Time	Signature	Protocol	Source / Destination
	13:48:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	66.132.153.155:60921 172.28.1.7:2362
	13:48:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.241:52918 172.28.1.7:5679
	13:48:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:21001
	13:48:47	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.74.44.18:58671 172.28.1.7:50002
	13:49:34	ET CINS Active Threat Intelligence Poor Reputation IP group 71 [1:2403370:104040] - Misc Attack	TCP	45.55.133.93:60000 172.28.1.7:5418
	13:49:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:36122 172.28.1.7:22
	13:50:59	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	78.128.114.38:51680 172.28.1.7:1433
	13:51:32	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.65.195.63:55801 172.28.1.7:50070
	13:51:53	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:54270 172.28.1.7:22
	13:53:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:34294 172.28.1.7:5900
	13:53:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:50344 172.28.1.7:22
	13:54:18	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.236.24.25:30669 172.28.1.7:50901
	13:54:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.237:59400 172.28.1.7:2129
	13:54:51	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:16014
	13:55:31	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5073 172.28.1.7:5060
	13:55:31	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5073 172.28.1.7:5060
	13:56:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:49406 172.28.1.7:22
	13:56:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:43057 172.28.1.7:4022
	13:57:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.251:43141 172.28.1.7:60011
	13:57:51	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.122.3:49803 172.28.1.7:9200
	13:58:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:43272 172.28.1.7:22
	13:58:06	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:55431 172.28.1.7:5986
	13:58:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.242:37195 172.28.1.7:4503
	13:58:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.27:48182 172.28.1.7:8090

	Time	Signature	Protocol	Source / Destination
	13:58:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.189:60022 172.28.1.7:7170
	13:58:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.221:50590 172.28.1.7:449
	13:59:12	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.209:56970 172.28.1.7:9463
	13:59:21	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.156.128.114:40818 172.28.1.7:2018
	14:00:08	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.189:56590 172.28.1.7:38522
	14:00:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.234.9:48014 172.28.1.7:22
	14:00:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:14897
	14:00:58	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.206:56758 172.28.1.7:46615
	14:01:01	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:26200 172.28.1.7:12379
	14:01:07	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.67:49794 172.28.1.7:53667
	14:02:12	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.179:50665 172.28.1.7:2098
	14:02:20	ET CINS Active Threat Intelligence Poor Reputation IP group 6 [1:2403305:104040] - Misc Attack	TCP	8.211.37.65:25475 172.28.1.7:52200
	14:02:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.223:60768 172.28.1.7:4433
	14:02:54	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	34.39.183.56:45432 172.28.1.7:3306
	14:03:17	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.180.158.248:52728 172.28.1.7:1830
	14:03:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:28961 172.28.1.7:771
	14:03:29	ET CINS Active Threat Intelligence Poor Reputation IP group 10 [1:2403309:104040] - Misc Attack	TCP	9.234.8.67:43883 172.28.1.7:6667
	14:03:59	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.122:42251 172.28.1.7:8087
	14:04:02	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	TCP	20.169.107.188:51919 172.28.1.7:10000
	14:04:02	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	40.124.185.206:33499 172.28.1.7:5432
	14:04:02	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.185.206:33499 172.28.1.7:5432
	14:06:47	ET CINS Active Threat Intelligence Poor Reputation IP group 84 [1:2403383:104040] - Misc Attack	TCP	48.214.144.125:38460 172.28.1.7:28017
	14:07:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:41667 172.28.1.7:3389
	14:08:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.220:52553 172.28.1.7:4900

	Time	Signature	Protocol	Source / Destination
	14:09:04	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.16.228:58629 172.28.1.7:7443
	14:09:53	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	37.232.159.243:13567 172.28.1.7:1433
	14:09:56	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	37.232.159.243:13567 172.28.1.7:1433
	14:10:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.96:2629 172.28.1.7:5060
	14:11:59	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.12:33518 172.28.1.7:83
	14:11:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.12:33518 172.28.1.7:83
	14:13:38	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.13:50272 172.28.1.7:36963
	14:13:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.142:49278 172.28.1.7:49152
	14:13:57	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.59:51583 172.28.1.7:52007
	14:14:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:58352 172.28.1.7:22
	14:14:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.190:43127 172.28.1.7:6667
	14:15:53	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.170:55675 172.28.1.7:8113
	14:16:10	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.119.99.194:48017 172.28.1.7:27018
	14:16:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:35024 172.28.1.7:22
	14:16:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	209.141.43.77:42190 172.28.1.7:22
	14:17:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.93:60235 172.28.1.7:90
	14:18:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:38468 172.28.1.7:22
	14:19:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.147:64537 172.28.1.7:10258
	14:20:13	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.93:50284 172.28.1.7:7080
	14:20:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:51332 172.28.1.7:22
	14:20:54	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	87.255.195.66:5102 172.28.1.7:5060
	14:20:54	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	87.255.195.66:5102 172.28.1.7:5060
	14:21:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.44:55769 172.28.1.7:34409
	14:21:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:12461

	Time	Signature	Protocol	Source / Destination
	14:22:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:41064 172.28.1.7:22
	14:23:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.97:31816 172.28.1.7:38763
	14:23:46	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:6007
	14:24:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:54460 172.28.1.7:22
	14:24:47	ET CINS Active Threat Intelligence Poor Reputation IP group 85 [1:2403384:104040] - Misc Attack	TCP	51.15.92.117:45092 172.28.1.7:12746
	14:24:48	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.149:51002 172.28.1.7:9729
	14:25:27	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:56314 172.28.1.7:9700
	14:26:27	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.202:49912 172.28.1.7:31113
	14:26:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:35324 172.28.1.7:22
	14:26:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.226:53926 172.28.1.7:2177
	14:27:22	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.102.88.108:55148 172.28.1.7:6379
	14:27:28	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.219:56167 172.28.1.7:22223
	14:27:38	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.115:55600 172.28.1.7:56002
	14:27:39	ET CINS Active Threat Intelligence Poor Reputation IP group 18 [1:2403317:104040] - Misc Attack	TCP	20.150.201.163:60338 172.28.1.7:15672
	14:28:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.131:33850 172.28.1.7:5351
	14:28:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.223:39920 172.28.1.7:5302
	14:28:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:60196 172.28.1.7:22
	14:29:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.178:2959 172.28.1.7:1911
	14:29:29	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.121.46:53723 172.28.1.7:55554
	14:30:15	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:46078 172.28.1.7:500
	14:30:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:32303
	14:30:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:52614 172.28.1.7:22
	14:31:13	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.94:51302 172.28.1.7:9699
	14:31:31	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.146.90.191:51074 172.28.1.7:9042

	Time	Signature	Protocol	Source / Destination
	14:32:05	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:44303 172.28.1.7:717
	14:33:03	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	64.225.74.178:31667 172.28.1.7:5432
	14:33:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:59860 172.28.1.7:22
	14:33:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.139:10131 172.28.1.7:222
	14:33:27	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:20041 172.28.1.7:122
	14:34:17	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.28:45443 172.28.1.7:3306
	14:34:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9064
	14:35:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:60508 172.28.1.7:22
	14:37:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.51:57141 172.28.1.7:1337
	14:37:18	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.65:40814 172.28.1.7:9398
	14:37:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.71.65.205:54648 172.28.1.7:22
	14:38:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.153:37673 172.28.1.7:44819
	14:38:49	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	88.218.193.163:37599 172.28.1.7:5432
	14:39:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.15:26200 172.28.1.7:5597
	14:39:48	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.105:56555 172.28.1.7:48477
	14:39:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:16016
	14:40:46	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.98:40806 172.28.1.7:8069
	14:41:07	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.19:56494 172.28.1.7:8011
	14:41:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.48:40376 172.28.1.7:2123
	14:43:08	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.181:51867 172.28.1.7:9299
	14:46:29	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:47994 172.28.1.7:8079
	14:47:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.141:47343 172.28.1.7:9090
	14:47:13	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.141:47343 172.28.1.7:9090
	14:47:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:23320 172.28.1.7:10000

	Time	Signature	Protocol	Source / Destination
	14:47:32	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.210:54887 172.28.1.7:9717
	14:48:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:33914 172.28.1.7:50000
	14:48:25	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	UDP	2.59.22.234:19243 172.28.1.7:17185
	14:50:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.171:46118 172.28.1.7:427
	14:50:44	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	UDP	47.251.82.144:21736 172.28.1.7:64738
	14:50:45	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.99:49634 172.28.1.7:5357
	14:50:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.29:36919 172.28.1.7:1900
	14:51:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.21:56082 172.28.1.7:7777
	14:51:31	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.63:49639 172.28.1.7:4190
	14:52:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.168:52973 172.28.1.7:4444
	14:54:18	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.30:53112 172.28.1.7:21279
	14:54:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.113:55664 172.28.1.7:9192
	14:55:03	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.15:56690 172.28.1.7:46747
	14:55:20	ET CINS Active Threat Intelligence Poor Reputation IP group 57 [1:2403356:104040] - Misc Attack	TCP	40.124.116.246:35163 172.28.1.7:7547
	14:55:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.84:58115 172.28.1.7:8111
	14:56:58	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.210:54023 172.28.1.7:48972
	14:57:23	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.96:52769 172.28.1.7:62333
	14:57:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.6:26200 172.28.1.7:36984
	14:57:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.245:49246 172.28.1.7:46130
	14:57:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:51108 172.28.1.7:22
	14:58:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.100:51531 172.28.1.7:8040
	14:58:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.130:17402 172.28.1.7:8088
	14:58:48	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	62.210.6.159:5563 172.28.1.7:5060
	14:58:48	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	62.210.6.159:5563 172.28.1.7:5060

	Time	Signature	Protocol	Source / Destination
	14:58:48	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	UDP	62.210.6.159:5563 172.28.1.7:5060
	14:59:07	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:60741 172.28.1.7:8050
	14:59:22	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	23.95.132.51:43015 172.28.1.7:3389
	14:59:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:1187
	14:59:45	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:1187
	14:59:47	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.113.228:47863 172.28.1.7:8181
	15:00:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:36250 172.28.1.7:22
	15:01:33	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.84:51140 172.28.1.7:60001
	15:01:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:5272
	15:02:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:45210 172.28.1.7:3389
	15:02:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	116.110.218.206:47010 172.28.1.7:22
	15:02:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:57912 172.28.1.7:22
	15:02:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.11:16663 172.28.1.7:81
	15:02:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:42944 172.28.1.7:22
	15:03:28	ET CINS Active Threat Intelligence Poor Reputation IP group 70 [1:2403369:104040] - Misc Attack	TCP	45.249.246.196:58096 172.28.1.7:2404
	15:04:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:8883
	15:04:32	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:51138 172.28.1.7:143
	15:05:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:54614 172.28.1.7:22
	15:05:14	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	219.139.83.165:51511 172.28.1.7:1433
	15:06:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:58060 172.28.1.7:22
	15:06:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:29011 172.28.1.7:4782
	15:06:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:29842
	15:07:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:47260 172.28.1.7:22
	15:07:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:51680 172.28.1.7:515

	Time	Signature	Protocol	Source / Destination
	15:08:53	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.86:51496 172.28.1.7:51334
	15:09:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:54950 172.28.1.7:22
	15:09:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:59382 172.28.1.7:22
	15:09:44	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.33.23:35627 172.28.1.7:5800
	15:09:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.167:49421 172.28.1.7:45519
	15:10:18	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.235:55031 172.28.1.7:45877
	15:10:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.154:10380 172.28.1.7:11103
	15:10:51	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.222:56586 172.28.1.7:5000
	15:10:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.222:56586 172.28.1.7:5000
	15:10:59	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.96:33694 172.28.1.7:20020
	15:11:53	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:46292 172.28.1.7:22
	15:12:16	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:40084 172.28.1.7:22
	15:13:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:8839
	15:13:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.67:57335 172.28.1.7:8020
	15:13:51	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:8899
	15:14:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:37784 172.28.1.7:22
	15:14:22	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:48045 172.28.1.7:84
	15:14:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:33362 172.28.1.7:22
	15:15:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.190:53729 172.28.1.7:1521
	15:15:16	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	65.49.1.190:53729 172.28.1.7:1521
	15:15:46	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:54033 172.28.1.7:8554
	15:15:56	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:41312 172.28.1.7:58000
	15:16:02	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:55536 172.28.1.7:22
	15:16:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.18:26200 172.28.1.7:8124

	Time	Signature	Protocol	Source / Destination
	15:17:03	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:50570 172.28.1.7:9001
	15:17:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:59280 172.28.1.7:22
	15:17:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:9161
	15:17:46	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	UDP	45.135.95.25:56326 172.28.1.7:5683
	15:17:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.233:36325 172.28.1.7:2525
	15:18:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:51924 172.28.1.7:22
	15:18:33	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.61:49548 172.28.1.7:49103
	15:18:58	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.250:53905 172.28.1.7:50993
	15:19:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.218:52358 172.28.1.7:33079
	15:19:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:43730 172.28.1.7:22
	15:19:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.245:32916 172.28.1.7:25227
	15:20:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:42870 172.28.1.7:22
	15:21:04	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:44730 172.28.1.7:8086
	15:21:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:45366 172.28.1.7:22
	15:21:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.248:36082 172.28.1.7:7026
	15:22:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:38680 172.28.1.7:22
	15:22:15	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	UDP	51.158.205.203:61000 172.28.1.7:53
	15:22:15	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	51.158.205.203:61000 172.28.1.7:53
	15:22:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.194:49588 172.28.1.7:8250
	15:22:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.239:48231 172.28.1.7:4081
	15:23:43	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	116.62.205.156:43625 172.28.1.7:1433
	15:23:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:6581
	15:24:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:33650 172.28.1.7:22
	15:24:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:44904 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	15:25:07	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:47684 172.28.1.7:22999
	15:25:20	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.58.125:50458 172.28.1.7:2049
	15:25:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:480
	15:26:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:55976 172.28.1.7:22
	15:26:45	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:37732 172.28.1.7:22
	15:26:53	ET CINS Active Threat Intelligence Poor Reputation IP group 5 [1:2403304:104040] - Misc Attack	UDP	5.181.188.210:40574 172.28.1.7:8080
	15:28:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.127:33089 172.28.1.7:7047
	15:28:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:44604 172.28.1.7:5900
	15:28:36	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.15.174:35006 172.28.1.7:109
	15:28:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:44778 172.28.1.7:22
	15:28:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.101:34319 172.28.1.7:39011
	15:29:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:12487
	15:29:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:45940 172.28.1.7:22
	15:29:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.154:4523 172.28.1.7:8000
	15:30:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8082
	15:30:04	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8082
	15:30:19	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.93.165:35901 172.28.1.7:18073
	15:30:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:52374 172.28.1.7:22
	15:31:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:18062
	15:31:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:40030 172.28.1.7:22
	15:32:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:54184 172.28.1.7:22
	15:33:04	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.139.9:42239 172.28.1.7:8529
	15:33:18	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.135:53109 172.28.1.7:9826
	15:33:20	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.80.223:26503 172.28.1.7:1022

	Time	Signature	Protocol	Source / Destination
	15:33:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.51:51959 172.28.1.7:7578
	15:34:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:42160 172.28.1.7:22
	15:34:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:43570 172.28.1.7:2222
	15:34:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:50200 172.28.1.7:22
	15:35:00	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.188:51099 172.28.1.7:636
	15:36:06	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:12272
	15:36:14	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:56816 172.28.1.7:92
	15:36:53	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	207.90.244.25:20270 172.28.1.7:3306
	15:36:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:42450 172.28.1.7:22
	15:37:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:35544 172.28.1.7:22
	15:37:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.111:63450 172.28.1.7:6291
	15:38:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.150:35247 172.28.1.7:3390
	15:38:18	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.218:56263 172.28.1.7:48668
	15:38:58	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:59604 172.28.1.7:22
	15:39:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:55642 172.28.1.7:22
	15:40:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.143:57074 172.28.1.7:7000
	15:41:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:45958 172.28.1.7:22
	15:41:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.124:56050 172.28.1.7:47389
	15:41:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.59:35439 172.28.1.7:8002
	15:41:48	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.227:51598 172.28.1.7:63422
	15:41:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:50334 172.28.1.7:22
	15:42:23	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.253:56864 172.28.1.7:49305
	15:43:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:34816 172.28.1.7:22
	15:43:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.176:8207 172.28.1.7:5903

	Time	Signature	Protocol	Source / Destination
	15:43:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:14401 172.28.1.7:6668
	15:43:51	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.7.24:53937 172.28.1.7:989
	15:44:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:56842 172.28.1.7:22
	15:45:18	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.184:55647 172.28.1.7:9114
	15:45:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:53044 172.28.1.7:22
	15:45:40	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	114.104.188.248:46461 172.28.1.7:1433
	15:46:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.110:21131 172.28.1.7:49938
	15:46:56	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5065 172.28.1.7:5060
	15:46:56	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5065 172.28.1.7:5060
	15:46:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:34010 172.28.1.7:22
	15:47:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:60070 172.28.1.7:22
	15:47:37	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.118:54753 172.28.1.7:46900
	15:47:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:47908 172.28.1.7:3389
	15:47:54	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	220.112.207.212:4997 172.28.1.7:1433
	15:47:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.80:49690 172.28.1.7:12654
	15:49:28	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:47434 172.28.1.7:22
	15:49:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:49836 172.28.1.7:22
	15:49:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.147:2721 172.28.1.7:6134
	15:50:24	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.71:35725 172.28.1.7:3388
	15:50:36	ET CINS Active Threat Intelligence Poor Reputation IP group 31 [1:2403330:104040] - Misc Attack	TCP	20.64.105.252:54081 172.28.1.7:9000
	15:51:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:49980 172.28.1.7:22
	15:51:53	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	UDP	20.168.127.148:45272 172.28.1.7:8087
	15:51:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:48378 172.28.1.7:22
	15:52:52	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	37.232.159.243:6997 172.28.1.7:3306

	Time	Signature	Protocol	Source / Destination
	15:53:28	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.234:49414 172.28.1.7:9790
	15:53:33	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	190.57.171.200:54929 172.28.1.7:1433
	15:53:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:45750 172.28.1.7:22
	15:54:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.185:48765 172.28.1.7:9060
	15:54:16	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:36626 172.28.1.7:22
	15:54:25	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	UDP	20.169.107.67:48761 172.28.1.7:5432
	15:55:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:33142 172.28.1.7:22
	15:55:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.13:47381 172.28.1.7:9060
	15:55:47	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.13:47381 172.28.1.7:9060
	15:55:48	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.169.105.85:36985 172.28.1.7:8009
	15:56:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.178:35127 172.28.1.7:4002
	15:56:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:56310 172.28.1.7:22
	15:56:38	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.63.50:43255 172.28.1.7:6775
	15:56:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.129:63928 172.28.1.7:37215
	15:57:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.126:58926 172.28.1.7:3790
	15:57:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:34532 172.28.1.7:22
	15:58:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.174:36302 172.28.1.7:6516
	15:58:44	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.174:36302 172.28.1.7:6516
	15:58:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:59560 172.28.1.7:22
	15:58:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.205:60658 172.28.1.7:32400
	15:58:59	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:12230
	15:59:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:50850 172.28.1.7:22
	15:59:58	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.66:56643 172.28.1.7:49304
	16:00:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.238:40575 172.28.1.7:5801

	Time	Signature	Protocol	Source / Destination
	16:00:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:19443
	16:00:44	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:60081 172.28.1.7:502
	16:00:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:48616 172.28.1.7:22
	16:01:00	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.177.158:50378 172.28.1.7:1337
	16:01:41	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.118.24.61:42352 172.28.1.7:28015
	16:01:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9080
	16:01:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:52394 172.28.1.7:22
	16:02:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:12165
	16:03:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:48508 172.28.1.7:22
	16:03:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:3169
	16:04:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:44902 172.28.1.7:22
	16:04:38	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:36156 172.28.1.7:8088
	16:04:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	193.163.125.197:24667 172.28.1.7:1967
	16:05:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:53700 172.28.1.7:22
	16:05:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.105:28368 172.28.1.7:27222
	16:06:06	ET INFO User-Agent (python-requests) Inbound to Webserver [1:2017515:8] - Misc activity	TCP	34.38.55.189:54280 172.28.1.7:444
	16:06:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:35862 172.28.1.7:22
	16:06:53	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.46.204:15992 172.28.1.7:10044
	16:07:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:32828 172.28.1.7:22
	16:07:44	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.86:37856 172.28.1.7:6080
	16:08:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:42891 172.28.1.7:4911
	16:08:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	IP-in-IP	64.62.156.145:None 172.28.1.7:None
	16:08:23	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.33:49578 172.28.1.7:9269
	16:08:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:46548 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	16:08:23	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.37:51290 172.28.1.7:3306
	16:08:50	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.94:37864 172.28.1.7:389
	16:09:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:57778 172.28.1.7:22
	16:09:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.228:54630 172.28.1.7:8531
	16:09:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.21:30227 172.28.1.7:2152
	16:10:05	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.119.72.191:54358 172.28.1.7:2082
	16:10:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:52470 172.28.1.7:22
	16:10:46	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.87:48824 172.28.1.7:30002
	16:11:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:55734 172.28.1.7:22
	16:11:28	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	UDP	20.55.3.64:44675 172.28.1.7:9160
	16:12:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.176:54201 172.28.1.7:47363
	16:12:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.145:22285 172.28.1.7:47808
	16:12:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:3082 172.28.1.7:1911
	16:12:46	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	UDP	20.168.121.236:49438 172.28.1.7:445
	16:12:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:33092 172.28.1.7:22
	16:12:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.65:37152 172.28.1.7:123
	16:13:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.251:53976 172.28.1.7:9922
	16:13:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:44028 172.28.1.7:22
	16:13:27	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.83.32.170:48055 172.28.1.7:2078
	16:14:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.69:53417 172.28.1.7:5900
	16:14:23	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.154:55187 172.28.1.7:63256
	16:15:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:49188 172.28.1.7:22
	16:15:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:44714 172.28.1.7:22
	16:15:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.146:63639 172.28.1.7:23

	Time	Signature	Protocol	Source / Destination
	16:15:45	ET CINS Active Threat Intelligence Poor Reputation IP group 6 [1:2403305:104040] - Misc Attack	TCP	8.209.96.247:23996 172.28.1.7:37443
	16:15:54	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:16063
	16:17:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:59824 172.28.1.7:22
	16:17:18	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:18028
	16:17:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	65.49.1.140:49993 172.28.1.7:500
	16:17:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:34794 172.28.1.7:22
	16:17:33	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.200:51714 172.28.1.7:49330
	16:17:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:400
	16:18:23	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.105.132.34:53086 172.28.1.7:139
	16:19:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:52874 172.28.1.7:22
	16:19:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:53188 172.28.1.7:22
	16:19:52	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.82.167:24250 172.28.1.7:8443
	16:20:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.5:50273 172.28.1.7:2404
	16:20:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.139:52061 172.28.1.7:9954
	16:20:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.16:26200 172.28.1.7:3403
	16:21:33	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:46310 172.28.1.7:22
	16:21:58	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:46426 172.28.1.7:22
	16:22:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.146:35779 172.28.1.7:47808
	16:22:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.72:49908 172.28.1.7:5938
	16:22:21	ET CINS Active Threat Intelligence Poor Reputation IP group 15 [1:2403314:104040] - Misc Attack	TCP	20.115.90.214:54358 172.28.1.7:179
	16:22:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:12346
	16:23:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.230:44677 172.28.1.7:1167
	16:23:36	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:54042 172.28.1.7:22
	16:23:58	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:37100 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	16:24:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.3:5791 172.28.1.7:8085
	16:25:08	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.61:54387 172.28.1.7:9399
	16:25:40	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:40326 172.28.1.7:22
	16:26:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.190:46670 172.28.1.7:52200
	16:26:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:54510 172.28.1.7:22
	16:26:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.113:43302 172.28.1.7:49670
	16:26:28	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.62.197.113:43302 172.28.1.7:49670
	16:27:40	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:34080 172.28.1.7:25565
	16:27:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:43756 172.28.1.7:22
	16:27:53	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.99:52992 172.28.1.7:48574
	16:28:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:51182 172.28.1.7:3389
	16:28:14	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:38480 172.28.1.7:22
	16:28:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.196:44590 172.28.1.7:2002
	16:28:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:8144 172.28.1.7:22
	16:28:54	ET CINS Active Threat Intelligence Poor Reputation IP group 68 [1:2403367:104040] - Misc Attack	TCP	45.156.129.156:15481 172.28.1.7:8282
	16:29:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:12248
	16:29:35	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.78:38784 172.28.1.7:19000
	16:29:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	64.62.156.103:46362 172.28.1.7:123
	16:29:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:60770 172.28.1.7:22
	16:30:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.206:52522 172.28.1.7:49934
	16:30:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:16404
	16:30:26	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42312 172.28.1.7:22
	16:30:33	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:46884 172.28.1.7:22
	16:30:45	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.176.81:46866 172.28.1.7:7474

	Time	Signature	Protocol	Source / Destination
	16:30:49	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:58126 172.28.1.7:22
	16:31:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.246:56420 172.28.1.7:21
	16:31:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.151:35798 172.28.1.7:6001
	16:31:58	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.47.162:23449 172.28.1.7:50995
	16:31:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:52762 172.28.1.7:22
	16:32:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	66.132.153.155:17395 172.28.1.7:2361
	16:32:31	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53308 172.28.1.7:22
	16:32:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:50132 172.28.1.7:22
	16:32:38	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:29921 172.28.1.7:19
	16:33:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.98:39775 172.28.1.7:445
	16:33:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39068 172.28.1.7:22
	16:33:27	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33904 172.28.1.7:22
	16:33:30	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:47925 172.28.1.7:4145
	16:33:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.251:53514 172.28.1.7:5432
	16:33:40	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	193.163.125.251:53514 172.28.1.7:5432
	16:33:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:28063 172.28.1.7:8728
	16:33:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	193.163.125.209:20264 172.28.1.7:111
	16:34:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:42958 172.28.1.7:22
	16:34:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.187:54629 172.28.1.7:2375
	16:34:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53620 172.28.1.7:22
	16:34:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:59414 172.28.1.7:22
	16:34:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.180:27718 172.28.1.7:790
	16:35:11	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34244 172.28.1.7:22
	16:35:32	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:44480 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	16:35:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:8873
	16:36:02	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	103.196.136.4:47827 172.28.1.7:1433
	16:36:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:43806 172.28.1.7:22
	16:36:45	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:37956 172.28.1.7:22
	16:36:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39900 172.28.1.7:22
	16:37:15	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41864 172.28.1.7:22
	16:37:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.104:42560 172.28.1.7:1200
	16:37:28	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.74.208.138:59444 172.28.1.7:20547
	16:37:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54314 172.28.1.7:22
	16:37:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:41126 172.28.1.7:8094
	16:38:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:34500 172.28.1.7:9197
	16:38:08	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.175:56384 172.28.1.7:9020
	16:38:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:48044 172.28.1.7:22
	16:38:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:29011 172.28.1.7:9000
	16:38:53	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.143:51721 172.28.1.7:47773
	16:38:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43762 172.28.1.7:22
	16:38:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:33330 172.28.1.7:22
	16:39:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53780 172.28.1.7:22
	16:39:46	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38472 172.28.1.7:22
	16:39:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:59825 172.28.1.7:56378
	16:40:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:46276 172.28.1.7:22
	16:40:54	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38226 172.28.1.7:22
	16:41:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:58540 172.28.1.7:22
	16:41:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.138:62241 172.28.1.7:8085

	Time	Signature	Protocol	Source / Destination
	16:41:24	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.77:45350 172.28.1.7:9306
	16:41:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47118 172.28.1.7:22
	16:41:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42174 172.28.1.7:22
	16:41:55	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.117:41026 172.28.1.7:8005
	16:42:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:43014 172.28.1.7:22
	16:42:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.223:54041 172.28.1.7:995
	16:42:39	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:48867 172.28.1.7:6379
	16:42:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56296 172.28.1.7:22
	16:43:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:38250 172.28.1.7:22
	16:43:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56926 172.28.1.7:22
	16:43:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.126:54877 172.28.1.7:161
	16:43:38	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	198.235.24.126:54877 172.28.1.7:161
	16:43:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59730 172.28.1.7:22
	16:44:03	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:48760 172.28.1.7:5001
	16:44:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.80:58456 172.28.1.7:5902
	16:44:53	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.127:54669 172.28.1.7:47453
	16:45:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39266 172.28.1.7:22
	16:45:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:43772 172.28.1.7:22
	16:45:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:60470 172.28.1.7:22
	16:45:39	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56036 172.28.1.7:22
	16:46:01	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36624 172.28.1.7:22
	16:47:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:41628 172.28.1.7:22
	16:47:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46684 172.28.1.7:22
	16:47:42	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42112 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	16:47:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:41832 172.28.1.7:22
	16:47:55	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.140.140.15:52590 172.28.1.7:80
	16:48:07	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38582 172.28.1.7:22
	16:48:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:34571 172.28.1.7:5900
	16:48:38	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.217:50297 172.28.1.7:23975
	16:49:16	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47366 172.28.1.7:22
	16:49:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:46848 172.28.1.7:22
	16:49:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.237:39656 172.28.1.7:7888
	16:49:46	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59708 172.28.1.7:22
	16:50:12	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56458 172.28.1.7:22
	16:50:27	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.239:51535 172.28.1.7:52965
	16:51:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:38410 172.28.1.7:22
	16:51:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.168:52477 172.28.1.7:873
	16:51:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42186 172.28.1.7:22
	16:51:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:54918 172.28.1.7:22
	16:51:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51348 172.28.1.7:22
	16:52:11	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:59454 172.28.1.7:8800
	16:52:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47858 172.28.1.7:22
	16:52:18	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.67:36627 172.28.1.7:33060
	16:52:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.20:55914 172.28.1.7:5060
	16:53:00	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:56683 172.28.1.7:123
	16:53:05	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.8.45:54294 172.28.1.7:135
	16:53:07	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.161.50.108:60023 172.28.1.7:64359
	16:53:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:44338 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	16:53:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38692 172.28.1.7:22
	16:53:40	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:36938 172.28.1.7:22
	16:53:58	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:47704 172.28.1.7:21
	16:53:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47490 172.28.1.7:22
	16:54:24	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45382 172.28.1.7:22
	16:54:48	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.114:52072 172.28.1.7:10477
	16:54:55	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.155.21:49600 172.28.1.7:8800
	16:54:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:8190
	16:55:00	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:56917 172.28.1.7:22225
	16:55:16	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:48712 172.28.1.7:22
	16:55:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57912 172.28.1.7:22
	16:55:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:49210 172.28.1.7:22
	16:56:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38140 172.28.1.7:22
	16:56:13	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.85.161:22226 172.28.1.7:9758
	16:56:29	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55240 172.28.1.7:22
	16:56:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.140:53503 172.28.1.7:1433
	16:56:30	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	198.235.24.140:53503 172.28.1.7:1433
	16:57:03	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.25:53973 172.28.1.7:10997
	16:57:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48244 172.28.1.7:22
	16:57:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8090
	16:57:51	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8090
	16:57:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:54002 172.28.1.7:22
	16:58:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.240:52425 172.28.1.7:30099
	16:58:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37740 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	16:58:34	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45054 172.28.1.7:22
	16:58:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:39240 172.28.1.7:22
	16:58:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.200:55076 172.28.1.7:3306
	16:58:41	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	205.210.31.200:55076 172.28.1.7:3306
	16:58:46	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:3014
	16:59:39	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48610 172.28.1.7:22
	16:59:41	ET CINS Active Threat Intelligence Poor Reputation IP group 5 [1:2403304:104040] - Misc Attack	TCP	4.227.178.194:36980 172.28.1.7:8834
	17:00:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49588 172.28.1.7:22
	17:00:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:46310 172.28.1.7:22
	17:00:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:50084 172.28.1.7:22
	17:00:41	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42526 172.28.1.7:22
	17:01:05	ET CINS Active Threat Intelligence Poor Reputation IP group 84 [1:2403383:104040] - Misc Attack	TCP	49.115.217.27:49472 172.28.1.7:6379
	17:01:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.78:51577 172.28.1.7:23
	17:01:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:54130 172.28.1.7:3389
	17:01:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	190.121.192.214:40818 172.28.1.7:22
	17:01:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54104 172.28.1.7:22
	17:02:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55482 172.28.1.7:22
	17:02:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.109:46154 172.28.1.7:3389
	17:02:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:37176 172.28.1.7:22
	17:02:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.251:54447 172.28.1.7:3389
	17:02:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.252:49216 172.28.1.7:22
	17:02:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:54384 172.28.1.7:22
	17:02:46	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56786 172.28.1.7:22
	17:03:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.187:45362 172.28.1.7:993

	Time	Signature	Protocol	Source / Destination
	17:03:57	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43012 172.28.1.7:22
	17:04:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53956 172.28.1.7:22
	17:04:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:60710 172.28.1.7:22
	17:04:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:43410 172.28.1.7:22
	17:04:43	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.172.70.65:47507 172.28.1.7:8086
	17:04:52	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45204 172.28.1.7:22
	17:04:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.38:56876 172.28.1.7:48158
	17:05:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:12280
	17:06:01	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54364 172.28.1.7:22
	17:06:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.65:55427 172.28.1.7:21
	17:06:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43888 172.28.1.7:22
	17:06:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:32774 172.28.1.7:22
	17:06:50	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:34952 172.28.1.7:22
	17:06:50	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:47697 172.28.1.7:95
	17:06:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:51680 172.28.1.7:5985
	17:06:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:57112 172.28.1.7:22
	17:07:19	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:40965 172.28.1.7:8093
	17:08:03	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:46918 172.28.1.7:8082
	17:08:08	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.154:54940 172.28.1.7:9235
	17:08:09	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60096 172.28.1.7:22
	17:08:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43718 172.28.1.7:22
	17:08:47	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.171:51925 172.28.1.7:9089
	17:08:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	146.190.225.13:42102 172.28.1.7:22
	17:08:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:43094 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	17:09:02	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:46364 172.28.1.7:22
	17:09:54	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	137.184.190.246:26312 172.28.1.7:1433
	17:09:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9324
	17:10:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39260 172.28.1.7:22
	17:10:12	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.170:55973 172.28.1.7:47988
	17:10:39	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46752 172.28.1.7:22
	17:10:51	ET CINS Active Threat Intelligence Poor Reputation IP group 62 [1:2403361:104040] - Misc Attack	TCP	43.224.126.107:24199 172.28.1.7:2222
	17:11:08	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37562 172.28.1.7:22
	17:11:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	64.225.66.85:60470 172.28.1.7:22
	17:12:16	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50460 172.28.1.7:22
	17:12:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.73:52238 172.28.1.7:1801
	17:12:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.232:57539 172.28.1.7:8702
	17:12:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54640 172.28.1.7:22
	17:13:13	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.53:57209 172.28.1.7:49218
	17:13:14	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34416 172.28.1.7:22
	17:13:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.136:38500 172.28.1.7:50000
	17:13:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.124:41380 172.28.1.7:3389
	17:13:53	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.90:42176 172.28.1.7:11211
	17:14:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46506 172.28.1.7:22
	17:14:39	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.3:52029 172.28.1.7:46604
	17:14:57	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45594 172.28.1.7:22
	17:15:19	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:39324 172.28.1.7:22
	17:16:32	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56810 172.28.1.7:22
	17:17:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.12:44490 172.28.1.7:5904

	Time	Signature	Protocol	Source / Destination
	17:17:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45578 172.28.1.7:22
	17:17:25	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:44086 172.28.1.7:22
	17:17:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:8198
	17:18:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12137
	17:18:16	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12137
	17:18:32	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46618 172.28.1.7:22
	17:19:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:32976 172.28.1.7:22
	17:19:29	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:32950 172.28.1.7:22
	17:19:29	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:12263
	17:19:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:234
	17:20:30	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.129:52352 172.28.1.7:51145
	17:20:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52936 172.28.1.7:22
	17:21:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:52470 172.28.1.7:1522
	17:21:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42402 172.28.1.7:22
	17:21:36	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33612 172.28.1.7:22
	17:21:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:17422 172.28.1.7:195
	17:22:09	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	UDP	20.169.107.122:35472 172.28.1.7:50000
	17:22:46	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50830 172.28.1.7:22
	17:22:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.51:34251 172.28.1.7:5555
	17:22:56	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.194.73:50762 172.28.1.7:8081
	17:22:59	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	185.243.5.106:5530 172.28.1.7:5060
	17:22:59	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	185.243.5.106:5530 172.28.1.7:5060
	17:23:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:37654 172.28.1.7:22
	17:23:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34472 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	17:23:34	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.36.190:11441 172.28.1.7:12323
	17:23:42	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.240:49384 172.28.1.7:7080
	17:23:44	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55148 172.28.1.7:22
	17:23:46	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:5915
	17:23:48	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.250.82.45:18438 172.28.1.7:7433
	17:23:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.94:49518 172.28.1.7:22
	17:24:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.152:31062 172.28.1.7:8888
	17:24:54	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34096 172.28.1.7:22
	17:25:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.19:26200 172.28.1.7:7510
	17:25:03	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.56:56544 172.28.1.7:46491
	17:25:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35732 172.28.1.7:22
	17:25:48	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:52630 172.28.1.7:22
	17:26:57	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37274 172.28.1.7:22
	17:26:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.231:36278 172.28.1.7:7557
	17:27:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.78:56729 172.28.1.7:80
	17:27:21	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	184.105.139.110:34368 172.28.1.7:3306
	17:27:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43894 172.28.1.7:22
	17:27:58	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42026 172.28.1.7:22
	17:28:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.222:34595 172.28.1.7:212
	17:28:26	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.222:34595 172.28.1.7:212
	17:28:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.154:48023 172.28.1.7:3389
	17:29:09	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59208 172.28.1.7:22
	17:29:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:55966 172.28.1.7:22
	17:29:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38688 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	17:29:42	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	UDP	45.135.95.25:39941 172.28.1.7:5353
	17:30:05	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54856 172.28.1.7:22
	17:30:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	180.76.227.2:55944 172.28.1.7:22
	17:30:48	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.8:49415 172.28.1.7:17004
	17:31:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40106 172.28.1.7:22
	17:31:39	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	180.76.227.2:36122 172.28.1.7:22
	17:31:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48248 172.28.1.7:22
	17:32:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:36046 172.28.1.7:22
	17:32:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:57086 172.28.1.7:22
	17:32:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.148:53982 172.28.1.7:22522
	17:32:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	180.76.227.2:44532 172.28.1.7:22
	17:33:10	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	101.36.97.80:56445 172.28.1.7:3306
	17:33:15	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.86.165:18761 172.28.1.7:8852
	17:33:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48068 172.28.1.7:22
	17:33:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.150:57559 172.28.1.7:5802
	17:33:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49002 172.28.1.7:22
	17:34:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:51593 172.28.1.7:9022
	17:34:15	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37242 172.28.1.7:22
	17:34:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:60786 172.28.1.7:22
	17:34:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:8859
	17:35:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41322 172.28.1.7:22
	17:35:32	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.83.27.89:38699 172.28.1.7:6379
	17:35:32	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.192.163:12584 172.28.1.7:88
	17:35:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:12305

	Time	Signature	Protocol	Source / Destination
	17:35:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59020 172.28.1.7:22
	17:36:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.247:36524 172.28.1.7:7887
	17:36:13	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.44.141:14622 172.28.1.7:9030
	17:36:21	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:35262 172.28.1.7:22
	17:36:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:43038 172.28.1.7:22
	17:37:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49682 172.28.1.7:22
	17:38:03	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.171.27.68:36730 172.28.1.7:2362
	17:38:33	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:43920 172.28.1.7:22
	17:38:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	66.132.153.150:62253 172.28.1.7:5683
	17:38:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:41130 172.28.1.7:22
	17:39:13	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.81:51763 172.28.1.7:8157
	17:39:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:5544
	17:39:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37530 172.28.1.7:22
	17:39:45	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:36301 172.28.1.7:9600
	17:40:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:29011 172.28.1.7:8888
	17:40:09	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39554 172.28.1.7:22
	17:40:33	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51398 172.28.1.7:22
	17:40:36	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	109.236.61.23:56333 172.28.1.7:161
	17:40:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:45840 172.28.1.7:22
	17:41:02	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	20.102.115.137:51272 172.28.1.7:5984
	17:41:42	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48018 172.28.1.7:22
	17:42:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:23320 172.28.1.7:7071
	17:42:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42210 172.28.1.7:22
	17:42:38	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59746 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	17:42:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:33804 172.28.1.7:22
	17:43:05	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.7.129:34033 172.28.1.7:9043
	17:43:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.218:33091 172.28.1.7:10021
	17:43:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42344 172.28.1.7:22
	17:43:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	118.193.40.35:39252 172.28.1.7:22
	17:44:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41660 172.28.1.7:22
	17:44:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.182:50341 172.28.1.7:45027
	17:44:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:4343
	17:44:42	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:4343
	17:44:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56108 172.28.1.7:22
	17:44:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.6:26200 172.28.1.7:3030
	17:45:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.100:48167 172.28.1.7:50376
	17:45:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:60820 172.28.1.7:22
	17:45:04	ET CINS Active Threat Intelligence Poor Reputation IP group 26 [1:2403325:104040] - Misc Attack	TCP	20.169.48.140:55889 172.28.1.7:50000
	17:45:05	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.249:49384 172.28.1.7:47058
	17:45:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:57143 172.28.1.7:3389
	17:45:57	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55254 172.28.1.7:22
	17:46:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.199:55218 172.28.1.7:3500
	17:46:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49118 172.28.1.7:22
	17:46:51	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34176 172.28.1.7:22
	17:46:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.156:64086 172.28.1.7:18084
	17:46:55	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.169.104.49:59121 172.28.1.7:8081
	17:47:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:53354 172.28.1.7:22
	17:48:03	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35620 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	17:48:04	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.141.145:49084 172.28.1.7:8505
	17:48:58	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.51.16:57586 172.28.1.7:3400
	17:49:05	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:46600 172.28.1.7:22
	17:49:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:40544 172.28.1.7:22
	17:49:08	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.121:55058 172.28.1.7:48693
	17:50:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59906 172.28.1.7:22
	17:50:19	ET CINS Active Threat Intelligence Poor Reputation IP group 60 [1:2403359:104040] - Misc Attack	TCP	40.76.250.51:47931 172.28.1.7:1911
	17:50:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48654 172.28.1.7:22
	17:51:03	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:53466 172.28.1.7:22
	17:51:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:60968 172.28.1.7:22
	17:51:08	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.233:50200 172.28.1.7:9244
	17:51:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:21269
	17:51:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:55210 172.28.1.7:2181
	17:52:11	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33038 172.28.1.7:22
	17:52:25	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:45124 172.28.1.7:31337
	17:52:46	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46750 172.28.1.7:22
	17:53:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:48754 172.28.1.7:22
	17:53:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:50050 172.28.1.7:22
	17:53:13	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.231:49649 172.28.1.7:46966
	17:53:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:3794
	17:54:21	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50658 172.28.1.7:22
	17:54:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.173:42392 172.28.1.7:2455
	17:54:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36674 172.28.1.7:22
	17:55:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:49624 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	17:55:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40630 172.28.1.7:22
	17:55:32	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.45.42:59766 172.28.1.7:8847
	17:55:53	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.152:54668 172.28.1.7:2534
	17:56:28	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60424 172.28.1.7:22
	17:56:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.235:39557 172.28.1.7:1723
	17:57:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.129:2041 172.28.1.7:2096
	17:57:14	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:38350 172.28.1.7:22
	17:57:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.130:40066 172.28.1.7:20256
	17:57:25	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.130:40066 172.28.1.7:20256
	17:57:25	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37532 172.28.1.7:22
	17:58:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43576 172.28.1.7:22
	17:59:03	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49200 172.28.1.7:22
	17:59:26	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:46624 172.28.1.7:22
	17:59:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:43060 172.28.1.7:22
	18:00:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33454 172.28.1.7:22
	18:00:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.68:35777 172.28.1.7:17000
	18:01:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39124 172.28.1.7:22
	18:01:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:35002
	18:01:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:55240 172.28.1.7:22
	18:01:32	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36324 172.28.1.7:22
	18:01:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.219:36332 172.28.1.7:14700
	18:01:48	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.179:49304 172.28.1.7:9919
	18:02:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52958 172.28.1.7:22
	18:03:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55930 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	18:03:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.90:44223 172.28.1.7:57722
	18:03:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:53700 172.28.1.7:22
	18:03:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:57562 172.28.1.7:22
	18:04:02	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:44812 172.28.1.7:8200
	18:04:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39260 172.28.1.7:22
	18:04:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.71:37030 172.28.1.7:50070
	18:05:02	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.120:52296 172.28.1.7:6022
	18:05:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.200:54960 172.28.1.7:26379
	18:05:07	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26366 172.28.1.7:5009
	18:05:08	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.135:49285 172.28.1.7:27170
	18:05:21	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43758 172.28.1.7:22
	18:05:42	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.143.24:29622 172.28.1.7:65004
	18:05:46	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41828 172.28.1.7:22
	18:05:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:46920 172.28.1.7:22
	18:06:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.59:52930 172.28.1.7:1883
	18:06:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.64:59642 172.28.1.7:4369
	18:06:57	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57370 172.28.1.7:22
	18:07:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.37:55770 172.28.1.7:5432
	18:07:22	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	205.210.31.37:55770 172.28.1.7:5432
	18:07:23	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:59202 172.28.1.7:9000
	18:07:28	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34508 172.28.1.7:22
	18:07:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36180 172.28.1.7:22
	18:07:58	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:59988 172.28.1.7:22
	18:08:43	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.46:49973 172.28.1.7:9674

	Time	Signature	Protocol	Source / Destination
	18:09:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51430 172.28.1.7:22
	18:09:25	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:46560 172.28.1.7:8002
	18:09:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52730 172.28.1.7:22
	18:09:57	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.108:60095 172.28.1.7:11211
	18:09:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51300 172.28.1.7:22
	18:10:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:39570 172.28.1.7:22
	18:10:47	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.35:58405 172.28.1.7:3306
	18:11:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35024 172.28.1.7:22
	18:11:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:37363 172.28.1.7:5900
	18:11:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36992 172.28.1.7:22
	18:12:03	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34768 172.28.1.7:22
	18:12:36	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:45876 172.28.1.7:22
	18:12:43	ET CINS Active Threat Intelligence Poor Reputation IP group 84 [1:2403383:104040] - Misc Attack	TCP	48.216.242.54:34959 172.28.1.7:587
	18:13:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42008 172.28.1.7:22
	18:13:36	ET CINS Active Threat Intelligence Poor Reputation IP group 5 [1:2403304:104040] - Misc Attack	TCP	8.130.87.18:51370 172.28.1.7:6379
	18:13:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39394 172.28.1.7:22
	18:13:53	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.219:55592 172.28.1.7:28085
	18:14:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33084 172.28.1.7:22
	18:14:23	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.165:57044 172.28.1.7:21601
	18:14:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:51686 172.28.1.7:22
	18:15:21	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35154 172.28.1.7:22
	18:15:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9459
	18:15:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.192:50478 172.28.1.7:5800
	18:15:49	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58840 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	18:16:02	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.138.21:55665 172.28.1.7:5901
	18:16:14	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:52600 172.28.1.7:22
	18:16:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.65:54795 172.28.1.7:830
	18:16:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:60392 172.28.1.7:22
	18:17:14	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.12.169:33898 172.28.1.7:9200
	18:17:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.107:25718 172.28.1.7:63203
	18:17:26	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54056 172.28.1.7:22
	18:17:36	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:7577 172.28.1.7:22
	18:17:41	ET CINS Active Threat Intelligence Poor Reputation IP group 85 [1:2403384:104040] - Misc Attack	TCP	51.15.92.117:59055 172.28.1.7:18903
	18:17:56	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51462 172.28.1.7:22
	18:18:19	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42412 172.28.1.7:22
	18:18:43	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.23:57195 172.28.1.7:53390
	18:18:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.225:42840 172.28.1.7:50075
	18:18:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:57252 172.28.1.7:3389
	18:18:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:43766 172.28.1.7:22
	18:18:58	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.203:57170 172.28.1.7:30004
	18:19:01	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.88.238:60833 172.28.1.7:8915
	18:19:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.142:52595 172.28.1.7:6588
	18:19:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:8102
	18:19:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42238 172.28.1.7:22
	18:19:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.225:45800 172.28.1.7:9022
	18:20:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40728 172.28.1.7:22
	18:20:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.155:56646 172.28.1.7:61616
	18:20:26	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33426 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	18:20:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:2200
	18:20:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.4:58359 172.28.1.7:20547
	18:21:03	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26391 172.28.1.7:1153
	18:21:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:55220 172.28.1.7:22
	18:21:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.137:49468 172.28.1.7:11194
	18:21:30	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	UDP	64.23.214.73:29669 172.28.1.7:5684
	18:21:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56790 172.28.1.7:22
	18:21:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.149:56445 172.28.1.7:27036
	18:21:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.130:40209 172.28.1.7:4840
	18:21:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	199.45.154.188:10115 172.28.1.7:123
	18:22:07	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49766 172.28.1.7:22
	18:22:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37846 172.28.1.7:22
	18:23:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:57662 172.28.1.7:22
	18:23:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.193:34520 172.28.1.7:61616
	18:23:33	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.193:34520 172.28.1.7:61616
	18:23:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56248 172.28.1.7:22
	18:24:10	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.65.195.44:38041 172.28.1.7:29015
	18:24:15	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48266 172.28.1.7:22
	18:24:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.149:48362 172.28.1.7:135
	18:24:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.176:33883 172.28.1.7:63210
	18:24:38	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36022 172.28.1.7:22
	18:24:48	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.124.175.86:37107 172.28.1.7:541
	18:25:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:33148 172.28.1.7:22
	18:25:18	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.7:52127 172.28.1.7:45425

	Time	Signature	Protocol	Source / Destination
	18:25:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51928 172.28.1.7:22
	18:25:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.230:50240 172.28.1.7:49698
	18:26:16	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42252 172.28.1.7:22
	18:26:34	ET CINS Active Threat Intelligence Poor Reputation IP group 59 [1:2403358:104040] - Misc Attack	TCP	40.76.116.105:56921 172.28.1.7:1028
	18:26:42	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59724 172.28.1.7:22
	18:26:49	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.81.157:38510 172.28.1.7:12153
	18:26:54	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:50111 172.28.1.7:90
	18:27:00	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:30267 172.28.1.7:513
	18:27:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:35566 172.28.1.7:22
	18:27:46	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43792 172.28.1.7:22
	18:27:57	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.123.1:57438 172.28.1.7:8333
	18:28:01	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:55093 172.28.1.7:4000
	18:28:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38642 172.28.1.7:22
	18:28:46	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:57426 172.28.1.7:22
	18:29:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:52530 172.28.1.7:22
	18:29:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.231:45290 172.28.1.7:6002
	18:29:45	ET CINS Active Threat Intelligence Poor Reputation IP group 55 [1:2403354:104040] - Misc Attack	TCP	36.99.41.23:56680 172.28.1.7:6379
	18:29:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:12189
	18:29:56	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49954 172.28.1.7:22
	18:30:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.155:1615 172.28.1.7:61616
	18:30:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43980 172.28.1.7:22
	18:30:33	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.112:50451 172.28.1.7:46658
	18:30:54	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60556 172.28.1.7:22
	18:31:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.179:34980 172.28.1.7:2053

	Time	Signature	Protocol	Source / Destination
	18:31:36	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:37586 172.28.1.7:22
	18:32:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59130 172.28.1.7:22
	18:32:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55630 172.28.1.7:22
	18:32:48	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.151:49918 172.28.1.7:47913
	18:33:00	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42882 172.28.1.7:22
	18:33:08	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:44293 172.28.1.7:5901
	18:33:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.227:47052 172.28.1.7:710
	18:33:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:37124 172.28.1.7:22
	18:34:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58876 172.28.1.7:22
	18:34:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55046 172.28.1.7:22
	18:34:41	ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394) [1:2044008:2] - Attempted Administrator Privilege Gain	UDP	94.72.118.193:59729 172.28.1.7:9034
	18:34:53	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.33:56916 172.28.1.7:55635
	18:35:03	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47100 172.28.1.7:22
	18:35:27	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	185.243.5.171:6410 172.28.1.7:5060
	18:35:27	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	185.243.5.171:6410 172.28.1.7:5060
	18:36:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.149.122:33206 172.28.1.7:22
	18:36:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.147:14708 172.28.1.7:636
	18:36:11	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43826 172.28.1.7:22
	18:36:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43348 172.28.1.7:22
	18:37:11	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37140 172.28.1.7:22
	18:37:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.91:38321 172.28.1.7:110
	18:37:48	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.66:46671 172.28.1.7:62078
	18:37:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.147:47202 172.28.1.7:6004
	18:38:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.140:47456 172.28.1.7:22522

	Time	Signature	Protocol	Source / Destination
	18:38:21	ET CINS Active Threat Intelligence Poor Reputation IP group 31 [1:2403330:104040] - Misc Attack	TCP	20.64.105.236:38338 172.28.1.7:514
	18:38:22	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38634 172.28.1.7:22
	18:38:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:3056
	18:38:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.253:49948 172.28.1.7:40470
	18:38:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40418 172.28.1.7:22
	18:38:57	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:50381 172.28.1.7:27017
	18:39:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33140 172.28.1.7:22
	18:39:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.132:49985 172.28.1.7:49669
	18:40:02	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.244:51624 172.28.1.7:9823
	18:40:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.190:53054 172.28.1.7:49238
	18:40:07	ET CINS Active Threat Intelligence Poor Reputation IP group 83 [1:2403382:104040] - Misc Attack	UDP	47.91.29.207:49974 172.28.1.7:10001
	18:40:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36810 172.28.1.7:22
	18:40:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	66.132.153.144:6453 172.28.1.7:34964
	18:40:56	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38404 172.28.1.7:22
	18:41:20	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60574 172.28.1.7:22
	18:41:22	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.140.212:35948 172.28.1.7:16098
	18:41:54	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	TCP	20.84.153.199:50936 172.28.1.7:992
	18:42:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.122:49757 172.28.1.7:9677
	18:42:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41078 172.28.1.7:22
	18:43:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43534 172.28.1.7:22
	18:43:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.253:58940 172.28.1.7:3313
	18:43:28	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47638 172.28.1.7:22
	18:43:33	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.91:50478 172.28.1.7:48329
	18:44:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:51680 172.28.1.7:8443

	Time	Signature	Protocol	Source / Destination
	18:44:23	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.195.121:60871 172.28.1.7:3351
	18:44:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.13:19243 172.28.1.7:17185
	18:44:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35878 172.28.1.7:22
	18:45:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39840 172.28.1.7:22
	18:45:32	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:39626 172.28.1.7:22
	18:45:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:47473 172.28.1.7:7170
	18:45:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.189:39369 172.28.1.7:1201
	18:45:59	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.138.209:52628 172.28.1.7:7340
	18:46:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.10:35750 172.28.1.7:789
	18:46:43	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53390 172.28.1.7:22
	18:47:15	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60348 172.28.1.7:22
	18:47:37	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54310 172.28.1.7:22
	18:47:56	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:59721 172.28.1.7:808
	18:48:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.132:14405 172.28.1.7:61616
	18:48:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.57:34956 172.28.1.7:5984
	18:48:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:8436
	18:48:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50518 172.28.1.7:22
	18:48:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:36778 172.28.1.7:22
	18:49:00	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.29.49.244:44965 172.28.1.7:1931
	18:49:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47356 172.28.1.7:22
	18:49:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.248:36789 172.28.1.7:8008
	18:49:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.43:14821 172.28.1.7:6467
	18:49:45	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47282 172.28.1.7:22
	18:49:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:22082

	Time	Signature	Protocol	Source / Destination
	18:50:55	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51580 172.28.1.7:22
	18:50:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:54700 172.28.1.7:22
	18:51:05	ET CINS Active Threat Intelligence Poor Reputation IP group 38 [1:2403337:104040] - Misc Attack	TCP	20.84.61.38:43533 172.28.1.7:6379
	18:51:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:60794 172.28.1.7:22
	18:51:26	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	111.30.26.121:46754 172.28.1.7:1433
	18:51:28	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52544 172.28.1.7:22
	18:51:52	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47912 172.28.1.7:22
	18:52:31	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.78:35758 172.28.1.7:4848
	18:52:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:59568 172.28.1.7:22
	18:53:01	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.245.89.178:56149 172.28.1.7:9000
	18:53:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59824 172.28.1.7:22
	18:53:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:43076 172.28.1.7:22
	18:53:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35078 172.28.1.7:22
	18:53:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.241:47062 172.28.1.7:54321
	18:53:59	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60468 172.28.1.7:22
	18:54:38	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.62:56000 172.28.1.7:12086
	18:54:44	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.119:55861 172.28.1.7:11002
	18:54:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.103:37504 172.28.1.7:5805
	18:54:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:45826 172.28.1.7:22
	18:55:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43204 172.28.1.7:22
	18:55:19	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:38299 172.28.1.7:5000
	18:55:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:34424 172.28.1.7:22
	18:55:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46132 172.28.1.7:22
	18:56:04	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42196 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	18:56:34	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.121:51662 172.28.1.7:9296
	18:57:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:43952 172.28.1.7:22
	18:57:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47810 172.28.1.7:22
	18:57:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:58392 172.28.1.7:22
	18:57:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46006 172.28.1.7:22
	18:58:11	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:39786 172.28.1.7:22
	18:58:27	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	20.127.157.56:48835 172.28.1.7:53
	18:58:27	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	UDP	20.127.157.56:48835 172.28.1.7:53
	18:58:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	139.19.117.130:60004 172.28.1.7:22
	18:59:02	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:55970 172.28.1.7:22
	18:59:12	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.81.172:15943 172.28.1.7:5523
	18:59:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40866 172.28.1.7:22
	18:59:23	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.170:44718 172.28.1.7:20000
	18:59:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.170:44718 172.28.1.7:20000
	18:59:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:47714 172.28.1.7:22
	18:59:54	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38188 172.28.1.7:22
	18:59:58	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:51638 172.28.1.7:8085
	19:00:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.250:47649 172.28.1.7:30356
	19:00:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59148 172.28.1.7:22
	19:00:33	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.237.6.226:38894 172.28.1.7:8700
	19:01:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:45558 172.28.1.7:22
	19:01:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.27:2398 172.28.1.7:8008
	19:01:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	164.92.168.97:33488 172.28.1.7:22
	19:01:28	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59394 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:01:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:51512 172.28.1.7:22
	19:02:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.70:58914 172.28.1.7:5202
	19:02:22	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.70:58914 172.28.1.7:5202
	19:02:27	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:49550 172.28.1.7:22
	19:02:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.138:18981 172.28.1.7:5683
	19:02:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.158:28562 172.28.1.7:500
	19:03:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:47656 172.28.1.7:22
	19:03:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35754 172.28.1.7:22
	19:03:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:8156
	19:04:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:39498 172.28.1.7:22
	19:04:03	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56364 172.28.1.7:22
	19:04:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:7348
	19:04:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.186:42118 172.28.1.7:44817
	19:04:28	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45026 172.28.1.7:22
	19:04:42	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:36478 172.28.1.7:30000
	19:04:58	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.25:50952 172.28.1.7:13389
	19:05:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:60784 172.28.1.7:22
	19:05:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60354 172.28.1.7:22
	19:05:52	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:28693 172.28.1.7:9042
	19:06:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:53126 172.28.1.7:22
	19:06:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54084 172.28.1.7:22
	19:06:14	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.124:54062 172.28.1.7:9206
	19:06:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.69:60238 172.28.1.7:5903
	19:06:36	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42138 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:06:48	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:26200 172.28.1.7:12341
	19:07:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:55410 172.28.1.7:22
	19:07:28	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.213:51786 172.28.1.7:46024
	19:07:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58830 172.28.1.7:22
	19:08:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:44494 172.28.1.7:22
	19:08:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.94:57388 172.28.1.7:3389
	19:08:46	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47464 172.28.1.7:22
	19:08:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:29011 172.28.1.7:1400
	19:09:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:48486 172.28.1.7:22
	19:09:46	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40434 172.28.1.7:22
	19:10:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.9:50349 172.28.1.7:12694
	19:10:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.40:50099 172.28.1.7:20257
	19:10:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:40240 172.28.1.7:22
	19:10:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40488 172.28.1.7:22
	19:10:41	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.237.79.198:23091 172.28.1.7:7998
	19:10:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:35234 172.28.1.7:22
	19:11:23	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.31:49628 172.28.1.7:9076
	19:11:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:45816 172.28.1.7:22
	19:11:27	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.168.99.52:44644 172.28.1.7:5601
	19:11:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.65:59650 172.28.1.7:5672
	19:11:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.102:39589 172.28.1.7:1911
	19:11:55	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60812 172.28.1.7:22
	19:11:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:36361 172.28.1.7:22
	19:12:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:47428 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:12:28	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59158 172.28.1.7:22
	19:12:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.96:25984 172.28.1.7:20420
	19:12:37	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.15.196:49423 172.28.1.7:5985
	19:12:48	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	46.101.83.206:33459 172.28.1.7:2375
	19:12:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51536 172.28.1.7:22
	19:13:08	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:39196 172.28.1.7:8090
	19:13:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.58:36152 172.28.1.7:102
	19:13:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.10:58914 172.28.1.7:28017
	19:13:35	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.10:58914 172.28.1.7:28017
	19:13:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:50228 172.28.1.7:22
	19:14:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50892 172.28.1.7:22
	19:14:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:46508 172.28.1.7:22
	19:14:25	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	47.237.112.227:20289 172.28.1.7:53
	19:14:25	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	UDP	47.237.112.227:20289 172.28.1.7:53
	19:14:31	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47836 172.28.1.7:22
	19:14:55	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40796 172.28.1.7:22
	19:15:00	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.64.104.142:57529 172.28.1.7:32400
	19:15:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.156:54961 172.28.1.7:9080
	19:15:40	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:58866 172.28.1.7:22
	19:15:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:9529
	19:16:03	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55726 172.28.1.7:22
	19:16:16	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.82.167:38479 172.28.1.7:18002
	19:16:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:48854 172.28.1.7:22
	19:16:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47690 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:16:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.38:40099 172.28.1.7:1337
	19:16:38	ET CINS Active Threat Intelligence Poor Reputation IP group 6 [1:2403305:104040] - Misc Attack	TCP	8.211.33.23:33255 172.28.1.7:8066
	19:16:42	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.74:56816 172.28.1.7:21341
	19:16:53	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.135:57109 172.28.1.7:9012
	19:17:00	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36122 172.28.1.7:22
	19:17:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:39972 172.28.1.7:22
	19:17:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.94:52864 172.28.1.7:53524
	19:18:06	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:35139 172.28.1.7:995
	19:18:09	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52668 172.28.1.7:22
	19:18:18	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.168:56671 172.28.1.7:46300
	19:18:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:46632 172.28.1.7:22
	19:18:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46598 172.28.1.7:22
	19:19:06	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37206 172.28.1.7:22
	19:19:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:43698 172.28.1.7:22
	19:19:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.74:52928 172.28.1.7:2080
	19:20:17	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55382 172.28.1.7:22
	19:20:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:54864 172.28.1.7:22
	19:20:46	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48850 172.28.1.7:22
	19:20:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.102:56018 172.28.1.7:8560
	19:21:10	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38852 172.28.1.7:22
	19:21:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:3200
	19:21:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:53528 172.28.1.7:22
	19:22:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.132:39539 172.28.1.7:11211
	19:22:02	ET CINS Active Threat Intelligence Poor Reputation IP group 99 [1:2403398:104040] - Misc Attack	TCP	64.62.197.132:39539 172.28.1.7:11211

	Time	Signature	Protocol	Source / Destination
	19:22:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56660 172.28.1.7:22
	19:22:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.24:53268 172.28.1.7:8088
	19:22:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.193:48954 172.28.1.7:5901
	19:22:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:39058 172.28.1.7:22
	19:22:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:2351
	19:22:49	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47598 172.28.1.7:22
	19:23:13	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	UDP	47.74.55.112:35390 172.28.1.7:3671
	19:23:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38828 172.28.1.7:22
	19:23:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:46476 172.28.1.7:22
	19:24:15	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.221.68.122:44963 172.28.1.7:1723
	19:24:21	ET CINS Active Threat Intelligence Poor Reputation IP group 62 [1:2403361:104040] - Misc Attack	TCP	42.63.70.211:40654 172.28.1.7:2222
	19:24:26	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57254 172.28.1.7:22
	19:24:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:55698 172.28.1.7:22
	19:24:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.34:39466 172.28.1.7:102
	19:24:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:40911 172.28.1.7:60002
	19:24:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50724 172.28.1.7:22
	19:25:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.176:51877 172.28.1.7:54528
	19:25:06	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	167.99.151.109:59746 172.28.1.7:1521
	19:25:22	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40142 172.28.1.7:22
	19:26:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:51824 172.28.1.7:22
	19:26:31	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58022 172.28.1.7:22
	19:26:53	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:55150 172.28.1.7:22
	19:27:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52144 172.28.1.7:22
	19:27:27	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41724 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:28:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:53574 172.28.1.7:22
	19:28:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34914 172.28.1.7:22
	19:29:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33292 172.28.1.7:22
	19:29:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:46254 172.28.1.7:22
	19:29:16	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.107:52954 172.28.1.7:59189
	19:29:31	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51928 172.28.1.7:22
	19:29:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.224:50224 172.28.1.7:5907
	19:30:29	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:57832 172.28.1.7:22
	19:30:42	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49006 172.28.1.7:22
	19:31:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:47358 172.28.1.7:22
	19:31:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.215:51215 172.28.1.7:943
	19:31:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46806 172.28.1.7:22
	19:31:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:43149 172.28.1.7:3389
	19:31:37	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38384 172.28.1.7:22
	19:31:48	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.71:49948 172.28.1.7:54300
	19:31:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.113:37650 172.28.1.7:33060
	19:31:56	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.62.197.113:37650 172.28.1.7:33060
	19:32:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.52:56779 172.28.1.7:30006
	19:32:30	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.46:35328 172.28.1.7:6645
	19:32:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.173:54722 172.28.1.7:1000
	19:32:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:57918 172.28.1.7:22
	19:32:45	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	TCP	47.254.215.105:43181 172.28.1.7:18001
	19:32:49	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53192 172.28.1.7:22
	19:32:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:9245

	Time	Signature	Protocol	Source / Destination
	19:33:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:55024 172.28.1.7:22
	19:33:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.88:53217 172.28.1.7:88
	19:33:22	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45072 172.28.1.7:22
	19:33:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:21285
	19:33:43	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59052 172.28.1.7:22
	19:34:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.223:50966 172.28.1.7:995
	19:34:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:56963 172.28.1.7:5900
	19:34:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:58204 172.28.1.7:22
	19:34:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43514 172.28.1.7:22
	19:35:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:41160 172.28.1.7:22
	19:35:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35568 172.28.1.7:22
	19:35:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:49352 172.28.1.7:22
	19:36:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:23320 172.28.1.7:8085
	19:36:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12310
	19:36:11	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.87:58914 172.28.1.7:12310
	19:36:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.102:50531 172.28.1.7:50995
	19:36:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60330 172.28.1.7:22
	19:36:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:49498 172.28.1.7:22
	19:37:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.231:43748 172.28.1.7:8883
	19:37:28	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:52132 172.28.1.7:22
	19:37:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53782 172.28.1.7:22
	19:37:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.19:49678 172.28.1.7:9042
	19:37:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.67:54674 172.28.1.7:8888
	19:37:43	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.135:51777 172.28.1.7:45852

	Time	Signature	Protocol	Source / Destination
	19:37:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.198:57348 172.28.1.7:502
	19:37:51	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.198:57348 172.28.1.7:502
	19:37:54	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40932 172.28.1.7:22
	19:38:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9372
	19:38:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.36:43414 172.28.1.7:44818
	19:38:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.87:55952 172.28.1.7:5353
	19:39:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54234 172.28.1.7:22
	19:39:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:44350 172.28.1.7:22
	19:39:33	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:53356 172.28.1.7:22
	19:39:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45784 172.28.1.7:22
	19:39:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.86:58148 172.28.1.7:2000
	19:40:01	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33030 172.28.1.7:22
	19:40:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.175:37615 172.28.1.7:5222
	19:40:30	ET CINS Active Threat Intelligence Poor Reputation IP group 100 [1:2403399:104040] - Misc Attack	TCP	64.62.197.175:37615 172.28.1.7:5222
	19:40:53	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.63:56539 172.28.1.7:9517
	19:41:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.156.123:54842 172.28.1.7:636
	19:41:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.218:50512 172.28.1.7:873
	19:41:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49690 172.28.1.7:22
	19:41:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:46112 172.28.1.7:22
	19:41:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:49386 172.28.1.7:22
	19:41:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.217:50311 172.28.1.7:6568
	19:41:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.104:52924 172.28.1.7:63256
	19:42:06	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.81.157:43841 172.28.1.7:83
	19:42:12	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34116 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:42:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.67:56724 172.28.1.7:502
	19:42:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.161:51630 172.28.1.7:993
	19:42:46	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	2.59.22.234:26366 172.28.1.7:5009
	19:43:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.246:56997 172.28.1.7:37777
	19:43:10	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:29011 172.28.1.7:8060
	19:43:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46326 172.28.1.7:22
	19:43:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:34682 172.28.1.7:22
	19:43:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40342 172.28.1.7:22
	19:43:53	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.189:49480 172.28.1.7:46494
	19:43:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:43680 172.28.1.7:22
	19:44:10	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60136 172.28.1.7:22
	19:44:56	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.95:41356 172.28.1.7:2003
	19:45:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:1457
	19:45:10	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.189:49303 172.28.1.7:8443
	19:45:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54460 172.28.1.7:22
	19:45:33	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:48172 172.28.1.7:22
	19:45:52	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48302 172.28.1.7:22
	19:46:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:45164 172.28.1.7:22
	19:46:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:39482 172.28.1.7:22
	19:46:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	65.49.1.138:40329 172.28.1.7:5803
	19:46:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.11:59491 172.28.1.7:6467
	19:46:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.50:56280 172.28.1.7:50002
	19:47:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.163:52929 172.28.1.7:3052
	19:47:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34160 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:47:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:50762 172.28.1.7:22
	19:47:53	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.78:56088 172.28.1.7:54043
	19:47:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57384 172.28.1.7:22
	19:48:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:40756 172.28.1.7:22
	19:48:23	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:50256 172.28.1.7:22
	19:48:33	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.56:55482 172.28.1.7:47434
	19:48:44	ET CINS Active Threat Intelligence Poor Reputation IP group 32 [1:2403331:104040] - Misc Attack	TCP	20.65.136.87:59726 172.28.1.7:8445
	19:48:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:42987 172.28.1.7:3389
	19:49:19	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:60676 172.28.1.7:49152
	19:49:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46176 172.28.1.7:22
	19:49:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:60504 172.28.1.7:22
	19:49:53	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.210:54222 172.28.1.7:8450
	19:50:06	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41976 172.28.1.7:22
	19:50:10	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	195.24.237.37:44614 172.28.1.7:3306
	19:50:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:52036 172.28.1.7:22
	19:50:27	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33034 172.28.1.7:22
	19:50:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.42:52982 172.28.1.7:990
	19:51:01	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.33:53199 172.28.1.7:14875
	19:51:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:40184 172.28.1.7:50022
	19:51:32	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60538 172.28.1.7:22
	19:51:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.89:54425 172.28.1.7:1911
	19:51:52	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.127.170.79:49480 172.28.1.7:1414
	19:51:58	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:57706 172.28.1.7:22
	19:52:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40928 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:52:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:42410 172.28.1.7:22
	19:52:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38812 172.28.1.7:22
	19:53:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45698 172.28.1.7:22
	19:53:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.110:51498 172.28.1.7:8080
	19:54:02	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	159.65.199.120:35980 172.28.1.7:22
	19:54:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:45462 172.28.1.7:22
	19:54:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47058 172.28.1.7:22
	19:54:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:35980 172.28.1.7:22
	19:54:38	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41856 172.28.1.7:22
	19:54:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:42915 172.28.1.7:81
	19:54:53	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.105.215:59108 172.28.1.7:5984
	19:55:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:2195
	19:55:33	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.218:49305 172.28.1.7:12266
	19:55:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49966 172.28.1.7:22
	19:56:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:37180 172.28.1.7:44322
	19:56:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:46602 172.28.1.7:22
	19:56:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51586 172.28.1.7:22
	19:56:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:36714 172.28.1.7:22
	19:56:43	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45546 172.28.1.7:22
	19:57:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.101:56752 172.28.1.7:4911
	19:57:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:44569 172.28.1.7:3389
	19:57:54	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55338 172.28.1.7:22
	19:58:03	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:60684 172.28.1.7:9443
	19:58:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:56740 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	19:58:26	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55978 172.28.1.7:22
	19:58:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:50654 172.28.1.7:22
	19:58:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:53264 172.28.1.7:22
	20:00:01	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56550 172.28.1.7:22
	20:00:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50244 172.28.1.7:22
	20:00:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:44130 172.28.1.7:22
	20:00:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:45762 172.28.1.7:22
	20:00:53	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45046 172.28.1.7:22
	20:02:06	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52926 172.28.1.7:22
	20:02:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.180:9106 172.28.1.7:7443
	20:02:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50616 172.28.1.7:22
	20:02:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:43456 172.28.1.7:22
	20:02:49	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:52494 172.28.1.7:22
	20:02:58	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40412 172.28.1.7:22
	20:03:13	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	45.251.22.32:60636 172.28.1.7:1433
	20:03:13	ET CINS Active Threat Intelligence Poor Reputation IP group 70 [1:2403369:104040] - Misc Attack	TCP	45.251.22.32:60636 172.28.1.7:1433
	20:03:18	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.229:53678 172.28.1.7:2
	20:04:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37156 172.28.1.7:22
	20:04:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60660 172.28.1.7:22
	20:04:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:44492 172.28.1.7:22
	20:04:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:37130 172.28.1.7:22
	20:05:04	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51106 172.28.1.7:22
	20:05:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.140:49214 172.28.1.7:636
	20:05:30	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.66:36384 172.28.1.7:16993

	Time	Signature	Protocol	Source / Destination
	20:06:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.79:56254 172.28.1.7:52200
	20:06:15	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51264 172.28.1.7:22
	20:06:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:6274 172.28.1.7:22
	20:06:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48012 172.28.1.7:22
	20:06:52	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.29.49.134:48202 172.28.1.7:1583
	20:06:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:43764 172.28.1.7:22
	20:07:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.198:55167 172.28.1.7:4018
	20:07:03	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.188:54710 172.28.1.7:49353
	20:07:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:38632 172.28.1.7:22
	20:07:10	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42676 172.28.1.7:22
	20:07:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	195.184.76.3:12987 172.28.1.7:7777
	20:07:38	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.65:51399 172.28.1.7:47170
	20:07:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:29011 172.28.1.7:4040
	20:08:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55766 172.28.1.7:22
	20:08:30	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.111:49441 172.28.1.7:2343
	20:08:32	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.248.225:48534 172.28.1.7:30019
	20:08:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:18025
	20:08:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58438 172.28.1.7:22
	20:09:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:47812 172.28.1.7:22
	20:09:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:51914 172.28.1.7:22
	20:09:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60650 172.28.1.7:22
	20:09:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.249:52542 172.28.1.7:2380
	20:10:26	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51080 172.28.1.7:22
	20:10:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.189:3847 172.28.1.7:20546

	Time	Signature	Protocol	Source / Destination
	20:10:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52678 172.28.1.7:22
	20:11:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:51436 172.28.1.7:22
	20:11:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	159.65.199.120:42514 172.28.1.7:22
	20:11:20	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:46306 172.28.1.7:22
	20:11:32	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	159.65.199.120:48402 172.28.1.7:22
	20:12:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42092 172.28.1.7:22
	20:13:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38150 172.28.1.7:22
	20:13:03	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.180:55161 172.28.1.7:49982
	20:13:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.225:53247 172.28.1.7:8448
	20:13:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:6020
	20:13:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:55194 172.28.1.7:22
	20:13:25	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60762 172.28.1.7:22
	20:13:27	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:54591 172.28.1.7:33335
	20:13:33	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	UDP	45.135.95.25:57671 172.28.1.7:1900
	20:13:39	ET CINS Active Threat Intelligence Poor Reputation IP group 29 [1:2403328:104040] - Misc Attack	TCP	20.51.245.30:33777 172.28.1.7:6666
	20:13:48	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.23:52827 172.28.1.7:46509
	20:13:56	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:12577
	20:14:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33796 172.28.1.7:22
	20:15:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59724 172.28.1.7:22
	20:15:29	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:52756 172.28.1.7:22
	20:15:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:50778 172.28.1.7:22
	20:15:36	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	117.159.248.29:55339 172.28.1.7:1433
	20:16:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56822 172.28.1.7:22
	20:16:42	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:44251 172.28.1.7:5959

	Time	Signature	Protocol	Source / Destination
	20:17:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53706 172.28.1.7:22
	20:17:34	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47912 172.28.1.7:22
	20:17:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:45630 172.28.1.7:22
	20:18:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57918 172.28.1.7:22
	20:19:16	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59320 172.28.1.7:22
	20:19:40	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56000 172.28.1.7:22
	20:19:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.213:54403 172.28.1.7:5000
	20:19:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:42500 172.28.1.7:22
	20:20:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.168:54872 172.28.1.7:6379
	20:20:03	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.5:55313 172.28.1.7:24172
	20:20:12	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:32997 172.28.1.7:8005
	20:20:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.184:27376 172.28.1.7:2077
	20:20:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60796 172.28.1.7:22
	20:21:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60032 172.28.1.7:22
	20:22:04	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:32986 172.28.1.7:22
	20:22:17	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:12581
	20:22:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.64:55157 172.28.1.7:500
	20:22:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.252:50103 172.28.1.7:8899
	20:22:55	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56764 172.28.1.7:22
	20:23:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51888 172.28.1.7:22
	20:23:52	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40224 172.28.1.7:22
	20:23:52	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	135.237.123.203:37579 172.28.1.7:111
	20:23:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.225:50087 172.28.1.7:20249
	20:24:02	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:42298 172.28.1.7:8080

	Time	Signature	Protocol	Source / Destination
	20:24:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:46434 172.28.1.7:22
	20:24:40	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	118.193.46.136:59336 172.28.1.7:3306
	20:24:56	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	51.158.61.186:61001 172.28.1.7:80
	20:25:05	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.221.68.159:44368 172.28.1.7:8080
	20:25:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58412 172.28.1.7:22
	20:25:24	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:43829 172.28.1.7:2077
	20:25:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49558 172.28.1.7:22
	20:25:58	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.149:54730 172.28.1.7:17500
	20:25:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.150:30591 172.28.1.7:102
	20:26:01	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36788 172.28.1.7:22
	20:26:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:50312 172.28.1.7:22
	20:27:03	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.30:51695 172.28.1.7:50501
	20:27:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48690 172.28.1.7:22
	20:27:12	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:45690 172.28.1.7:8389
	20:27:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:646
	20:27:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39592 172.28.1.7:22
	20:28:06	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56190 172.28.1.7:22
	20:28:21	ET CINS Active Threat Intelligence Poor Reputation IP group 73 [1:2403372:104040] - Misc Attack	TCP	45.82.76.75:40914 172.28.1.7:1400
	20:28:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:33160 172.28.1.7:22
	20:28:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.79:52202 172.28.1.7:9443
	20:28:42	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.96:40921 172.28.1.7:2052
	20:29:16	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41256 172.28.1.7:22
	20:29:49	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:32874 172.28.1.7:22
	20:30:11	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.65.195.51:35351 172.28.1.7:513

	Time	Signature	Protocol	Source / Destination
	20:30:14	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:48882 172.28.1.7:22
	20:30:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:39048 172.28.1.7:22
	20:30:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.75:50988 172.28.1.7:9092
	20:31:18	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.106:52313 172.28.1.7:8022
	20:31:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:35138 172.28.1.7:22
	20:31:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56152 172.28.1.7:22
	20:32:01	ET CINS Active Threat Intelligence Poor Reputation IP group 75 [1:2403374:104040] - Misc Attack	TCP	46.161.50.108:60023 172.28.1.7:11211
	20:32:05	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:24858 172.28.1.7:666
	20:32:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.88:54520 172.28.1.7:2483
	20:32:19	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42150 172.28.1.7:22
	20:32:40	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:52178 172.28.1.7:22
	20:32:46	ET CINS Active Threat Intelligence Poor Reputation IP group 89 [1:2403388:104040] - Misc Attack	TCP	54.227.48.48:34326 172.28.1.7:8080
	20:33:26	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:33261 172.28.1.7:8092
	20:33:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57658 172.28.1.7:22
	20:33:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:3548
	20:33:52	ET CINS Active Threat Intelligence Poor Reputation IP group 4 [1:2403303:104040] - Misc Attack	TCP	3.90.204.214:28644 172.28.1.7:80
	20:33:55	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:50306 172.28.1.7:22
	20:33:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.210:57038 172.28.1.7:1521
	20:33:55	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	147.185.132.210:57038 172.28.1.7:1521
	20:34:08	ET CINS Active Threat Intelligence Poor Reputation IP group 88 [1:2403387:104040] - Misc Attack	TCP	54.163.221.179:12818 172.28.1.7:7443
	20:34:11	ET CINS Active Threat Intelligence Poor Reputation IP group 4 [1:2403303:104040] - Misc Attack	TCP	3.86.147.57:28200 172.28.1.7:56001
	20:34:20	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.204.204.49:31594 172.28.1.7:22
	20:34:35	ET CINS Active Threat Intelligence Poor Reputation IP group 88 [1:2403387:104040] - Misc Attack	TCP	54.159.138.145:26738 172.28.1.7:21
	20:34:43	ET CINS Active Threat Intelligence Poor Reputation IP group 88 [1:2403387:104040] - Misc Attack	TCP	54.172.106.146:58634 172.28.1.7:3389

	Time	Signature	Protocol	Source / Destination
	20:34:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:57430 172.28.1.7:22
	20:34:58	ET CINS Active Threat Intelligence Poor Reputation IP group 90 [1:2403389:104040] - Misc Attack	TCP	54.91.199.32:13046 172.28.1.7:8443
	20:35:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:4433
	20:35:01	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:4433
	20:35:08	ET CINS Active Threat Intelligence Poor Reputation IP group 10 [1:2403309:104040] - Misc Attack	TCP	13.222.30.221:65014 172.28.1.7:50050
	20:35:08	ET CINS Active Threat Intelligence Poor Reputation IP group 88 [1:2403387:104040] - Misc Attack	TCP	54.161.140.158:29160 172.28.1.7:9200
	20:35:11	ET CINS Active Threat Intelligence Poor Reputation IP group 4 [1:2403303:104040] - Misc Attack	TCP	3.88.226.53:22004 172.28.1.7:9200
	20:35:13	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.83.134.175:35638 172.28.1.7:8443
	20:35:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.249:56164 172.28.1.7:995
	20:35:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52772 172.28.1.7:22
	20:36:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.214:56047 172.28.1.7:9601
	20:36:07	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45340 172.28.1.7:22
	20:36:32	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:32984 172.28.1.7:22
	20:36:35	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5306 172.28.1.7:5060
	20:36:35	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5306 172.28.1.7:5060
	20:36:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:20624 172.28.1.7:44818
	20:36:51	ET CINS Active Threat Intelligence Poor Reputation IP group 10 [1:2403309:104040] - Misc Attack	TCP	13.217.228.89:56694 172.28.1.7:9200
	20:36:56	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:59672 172.28.1.7:22
	20:36:57	ET CINS Active Threat Intelligence Poor Reputation IP group 88 [1:2403387:104040] - Misc Attack	TCP	54.166.212.56:54072 172.28.1.7:443
	20:36:57	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.104.9:53936 172.28.1.7:3011
	20:36:58	ET CINS Active Threat Intelligence Poor Reputation IP group 38 [1:2403337:104040] - Misc Attack	TCP	23.22.168.204:15846 172.28.1.7:13443
	20:36:58	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.82.192.40:13286 172.28.1.7:12443
	20:37:04	ET CINS Active Threat Intelligence Poor Reputation IP group 41 [1:2403340:104040] - Misc Attack	TCP	34.201.46.79:44990 172.28.1.7:8443
	20:37:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:18438 172.28.1.7:2002

	Time	Signature	Protocol	Source / Destination
	20:37:19	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:44667 172.28.1.7:9200
	20:37:27	ET CINS Active Threat Intelligence Poor Reputation IP group 92 [1:2403391:104040] - Misc Attack	TCP	58.59.246.91:57668 172.28.1.7:2000
	20:37:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47450 172.28.1.7:22
	20:37:46	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	UDP	20.83.165.36:46117 172.28.1.7:7474
	20:37:58	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.174:53561 172.28.1.7:53311
	20:38:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:56586 172.28.1.7:7
	20:38:10	ET CINS Active Threat Intelligence Poor Reputation IP group 30 [1:2403329:104040] - Misc Attack	TCP	20.64.104.70:38090 172.28.1.7:7002
	20:38:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37458 172.28.1.7:22
	20:38:28	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.206.38.162:16964 172.28.1.7:1244
	20:38:30	ET CINS Active Threat Intelligence Poor Reputation IP group 19 [1:2403318:104040] - Misc Attack	TCP	20.163.15.225:54389 172.28.1.7:443
	20:38:31	ET CINS Active Threat Intelligence Poor Reputation IP group 90 [1:2403389:104040] - Misc Attack	TCP	54.89.240.189:20418 172.28.1.7:10443
	20:38:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:53030 172.28.1.7:22
	20:38:47	ET CINS Active Threat Intelligence Poor Reputation IP group 89 [1:2403388:104040] - Misc Attack	TCP	54.234.188.99:63714 172.28.1.7:11443
	20:38:48	ET CINS Active Threat Intelligence Poor Reputation IP group 90 [1:2403389:104040] - Misc Attack	TCP	54.91.50.100:50298 172.28.1.7:1245
	20:38:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	199.45.154.186:44820 172.28.1.7:4070
	20:38:54	ET SCAN HID VertX and Edge door controllers discover [1:2025822:2] - Attempted Information Leak	UDP	199.45.154.186:44820 172.28.1.7:4070
	20:38:58	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.177:52674 172.28.1.7:8017
	20:39:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:50666 172.28.1.7:22
	20:39:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.178:55179 172.28.1.7:4506
	20:39:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:46058 172.28.1.7:3389
	20:39:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38856 172.28.1.7:22
	20:40:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.14:50227 172.28.1.7:50994
	20:40:17	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55516 172.28.1.7:22
	20:40:43	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:43264 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	20:40:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.99:53988 172.28.1.7:138
	20:41:09	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.125.66:43340 172.28.1.7:8091
	20:41:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:42152 172.28.1.7:22
	20:41:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.156:14115 172.28.1.7:8081
	20:41:41	ET CINS Active Threat Intelligence Poor Reputation IP group 90 [1:2403389:104040] - Misc Attack	TCP	54.242.127.31:26858 172.28.1.7:8443
	20:41:42	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.206.123.19:40458 172.28.1.7:3000
	20:41:46	ET CINS Active Threat Intelligence Poor Reputation IP group 10 [1:2403309:104040] - Misc Attack	TCP	13.221.220.141:47112 172.28.1.7:9443
	20:41:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56354 172.28.1.7:22
	20:41:55	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.205.154.226:34982 172.28.1.7:7547
	20:42:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.107:13987 172.28.1.7:8565
	20:42:24	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49922 172.28.1.7:22
	20:42:48	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.48:51721 172.28.1.7:51067
	20:42:48	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37688 172.28.1.7:22
	20:43:13	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:56797 172.28.1.7:8729
	20:43:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:42536 172.28.1.7:22
	20:43:27	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.38.129:57399 172.28.1.7:9200
	20:44:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52734 172.28.1.7:22
	20:44:59	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34376 172.28.1.7:22
	20:45:30	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	128.199.50.29:36436 172.28.1.7:22
	20:46:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44878 172.28.1.7:22
	20:46:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.133:54459 172.28.1.7:17184
	20:46:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36824 172.28.1.7:22
	20:46:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.250:55469 172.28.1.7:53
	20:46:53	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	205.210.31.250:55469 172.28.1.7:53

	Time	Signature	Protocol	Source / Destination
	20:46:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.52:51494 172.28.1.7:5903
	20:46:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51606 172.28.1.7:22
	20:47:14	GPL DNS named version attempt [1:2101616:9] - Attempted Information Leak	UDP	205.210.31.65:56070 172.28.1.7:53
	20:47:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.65:56070 172.28.1.7:53
	20:48:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41998 172.28.1.7:22
	20:48:18	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.89:53876 172.28.1.7:44444
	20:48:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38760 172.28.1.7:22
	20:49:04	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60476 172.28.1.7:22
	20:49:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:26200 172.28.1.7:4602
	20:49:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.180:55813 172.28.1.7:5905
	20:50:00	ET CINS Active Threat Intelligence Poor Reputation IP group 38 [1:2403337:104040] - Misc Attack	TCP	20.98.164.209:43088 172.28.1.7:443
	20:50:18	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33516 172.28.1.7:22
	20:50:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.62:51078 172.28.1.7:8190
	20:50:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.32:56445 172.28.1.7:34567
	20:50:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55496 172.28.1.7:22
	20:50:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:29011 172.28.1.7:8010
	20:51:03	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.135:51104 172.28.1.7:19983
	20:51:14	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:44448 172.28.1.7:22
	20:51:35	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:34133 172.28.1.7:88
	20:52:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.218:34459 172.28.1.7:4224
	20:52:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.135:24289 172.28.1.7:6007
	20:52:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59548 172.28.1.7:22
	20:52:38	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.193:56277 172.28.1.7:45842
	20:52:56	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50578 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	20:53:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37502 172.28.1.7:22
	20:53:22	ET SCAN HID VertX and Edge door controllers discover [1:2025822:2] - Attempted Information Leak	UDP	143.198.225.197:20365 172.28.1.7:4070
	20:54:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:27153 172.28.1.7:992
	20:54:28	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54756 172.28.1.7:22
	20:54:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.74:54909 172.28.1.7:5632
	20:54:44	GPL POLICY PCAnywhere server response [1:2100566:5] - Misc activity	UDP	205.210.31.74:54909 172.28.1.7:5632
	20:55:13	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.253:50151 172.28.1.7:22462
	20:55:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36970 172.28.1.7:22
	20:55:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.84:56650 172.28.1.7:4016
	20:56:09	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:12544
	20:56:32	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46226 172.28.1.7:22
	20:56:35	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:8556
	20:57:03	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36594 172.28.1.7:22
	20:57:26	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:52422 172.28.1.7:22
	20:58:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.115:56104 172.28.1.7:9870
	20:58:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.104:57270 172.28.1.7:10443
	20:58:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9435
	20:58:38	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39810 172.28.1.7:22
	20:59:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60350 172.28.1.7:22
	20:59:35	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:48176 172.28.1.7:22
	20:59:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:45204 172.28.1.7:22
	21:00:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.244:52878 172.28.1.7:17185
	21:00:28	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.161:57183 172.28.1.7:8009
	21:00:47	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43932 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:00:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.220:43884 172.28.1.7:6172
	21:01:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39944 172.28.1.7:22
	21:01:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:34807 172.28.1.7:22
	21:01:41	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59266 172.28.1.7:22
	21:01:47	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.10:58914 172.28.1.7:5601
	21:01:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.10:58914 172.28.1.7:5601
	21:01:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:55090 172.28.1.7:22
	21:02:28	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	TCP	20.169.105.38:41656 172.28.1.7:8443
	21:02:35	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.121.45:53260 172.28.1.7:111
	21:02:49	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45452 172.28.1.7:22
	21:03:13	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.211.52.18:60846 172.28.1.7:8015
	21:03:35	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.98.14:34916 172.28.1.7:8081
	21:03:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55452 172.28.1.7:22
	21:04:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:51556 172.28.1.7:22
	21:04:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.78:55082 172.28.1.7:50805
	21:04:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:36222 172.28.1.7:22
	21:04:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	167.94.138.141:4737 172.28.1.7:5093
	21:04:56	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37666 172.28.1.7:22
	21:05:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56596 172.28.1.7:22
	21:05:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.192:53992 172.28.1.7:401
	21:05:53	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:46004 172.28.1.7:22
	21:06:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:34124 172.28.1.7:22
	21:06:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	147.185.132.109:56742 172.28.1.7:5351
	21:06:50	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:36916 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:07:01	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34624 172.28.1.7:22
	21:07:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.39:50899 172.28.1.7:1521
	21:07:19	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	205.210.31.39:50899 172.28.1.7:1521
	21:07:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56260 172.28.1.7:22
	21:07:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.192:49467 172.28.1.7:4020
	21:07:59	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47110 172.28.1.7:22
	21:08:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:36648 172.28.1.7:22
	21:08:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.159:50912 172.28.1.7:9595
	21:09:11	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47952 172.28.1.7:22
	21:09:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:40542 172.28.1.7:22
	21:09:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:44569 172.28.1.7:3393
	21:09:42	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44416 172.28.1.7:22
	21:09:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.174:53005 172.28.1.7:10250
	21:10:05	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34548 172.28.1.7:22
	21:10:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:49268 172.28.1.7:22
	21:10:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.78:51038 172.28.1.7:20
	21:10:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.201:55303 172.28.1.7:5632
	21:11:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50500 172.28.1.7:22
	21:11:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45382 172.28.1.7:22
	21:11:51	ET SCAN Suspicious inbound to MSSQL port 1433 [1:2010935:3] - Potentially Bad Traffic	TCP	61.149.12.198:54071 172.28.1.7:1433
	21:11:51	ET CINS Active Threat Intelligence Poor Reputation IP group 95 [1:2403394:104040] - Misc Attack	TCP	61.149.12.198:54071 172.28.1.7:1433
	21:11:55	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.21:26200 172.28.1.7:8076
	21:12:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34370 172.28.1.7:22
	21:12:15	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:23183 172.28.1.7:25001

	Time	Signature	Protocol	Source / Destination
	21:12:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:51676 172.28.1.7:22
	21:12:23	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.168:51204 172.28.1.7:49210
	21:12:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:38072 172.28.1.7:22
	21:12:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:7050
	21:13:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.139:56420 172.28.1.7:26000
	21:13:21	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59846 172.28.1.7:22
	21:13:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:58219 172.28.1.7:5900
	21:13:52	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56602 172.28.1.7:22
	21:14:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47372 172.28.1.7:22
	21:14:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:58800 172.28.1.7:22
	21:14:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.227:50321 172.28.1.7:2001
	21:15:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:59622 172.28.1.7:22
	21:15:06	ET CINS Active Threat Intelligence Poor Reputation IP group 7 [1:2403306:104040] - Misc Attack	TCP	8.211.46.83:27417 172.28.1.7:8148
	21:15:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38194 172.28.1.7:22
	21:15:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.243:52794 172.28.1.7:139
	21:15:56	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.240:49843 172.28.1.7:993
	21:15:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60060 172.28.1.7:22
	21:16:22	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:50474 172.28.1.7:22
	21:16:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	163.179.63.235:55382 172.28.1.7:22
	21:16:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:54134 172.28.1.7:22
	21:16:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.252:54819 172.28.1.7:44344
	21:17:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.224:55901 172.28.1.7:3388
	21:17:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:47998 172.28.1.7:22
	21:17:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40530 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:18:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60532 172.28.1.7:22
	21:18:07	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.4:57084 172.28.1.7:15812
	21:18:27	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:49918 172.28.1.7:22
	21:18:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:54236 172.28.1.7:22
	21:18:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:44760 172.28.1.7:22
	21:19:01	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.237.116.254:59403 172.28.1.7:12538
	21:19:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39948 172.28.1.7:22
	21:19:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:58002 172.28.1.7:22
	21:20:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.101:54433 172.28.1.7:1443
	21:20:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60012 172.28.1.7:22
	21:20:31	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:50888 172.28.1.7:22
	21:20:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:38450 172.28.1.7:22
	21:20:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:42589 172.28.1.7:22
	21:21:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36788 172.28.1.7:22
	21:21:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.208:50022 172.28.1.7:51401
	21:22:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55462 172.28.1.7:22
	21:22:15	ET CINS Active Threat Intelligence Poor Reputation IP group 81 [1:2403380:104040] - Misc Attack	UDP	47.254.248.116:54113 172.28.1.7:64738
	21:22:37	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:43024 172.28.1.7:22
	21:22:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:55780 172.28.1.7:22
	21:22:42	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.228:51566 172.28.1.7:2083
	21:22:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:59762 172.28.1.7:22
	21:22:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:52050 172.28.1.7:22
	21:22:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.235:49497 172.28.1.7:93
	21:23:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:3160

	Time	Signature	Protocol	Source / Destination
	21:23:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.177:46845 172.28.1.7:50000
	21:23:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56616 172.28.1.7:22
	21:23:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.18:56174 172.28.1.7:5443
	21:23:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.106:28649 172.28.1.7:3721
	21:24:14	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:29011 172.28.1.7:5901
	21:24:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.155:52728 172.28.1.7:30005
	21:24:46	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:35942 172.28.1.7:22
	21:24:55	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:44077 172.28.1.7:22
	21:25:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:59776 172.28.1.7:22
	21:25:02	ET CINS Active Threat Intelligence Poor Reputation IP group 77 [1:2403376:104040] - Misc Attack	TCP	47.237.76.193:41334 172.28.1.7:12369
	21:25:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:54818 172.28.1.7:22
	21:25:18	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.103:53935 172.28.1.7:49762
	21:25:36	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:47456 172.28.1.7:8003
	21:25:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45002 172.28.1.7:22
	21:26:22	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36510 172.28.1.7:22
	21:26:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.224:44438 172.28.1.7:7547
	21:26:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:53902 172.28.1.7:22
	21:26:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:50113 172.28.1.7:22
	21:27:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:49416 172.28.1.7:22
	21:27:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:62080
	21:28:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45372 172.28.1.7:22
	21:28:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:56828 172.28.1.7:22
	21:28:33	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.143:55937 172.28.1.7:52110
	21:28:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43446 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:28:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36698 172.28.1.7:22
	21:29:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:56723 172.28.1.7:22
	21:29:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:37560 172.28.1.7:22
	21:29:23	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.67:56146 172.28.1.7:29403
	21:29:23	GPL RPC portmap listing UDP 111 [1:2101280:10] - Decode of an RPC Query	UDP	147.182.225.86:14903 172.28.1.7:111
	21:29:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:9076
	21:30:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59122 172.28.1.7:22
	21:30:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51726 172.28.1.7:22
	21:30:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:45284 172.28.1.7:22
	21:31:02	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37324 172.28.1.7:22
	21:31:07	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	62.60.131.129:58455 172.28.1.7:9000
	21:31:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	62.60.131.129:58455 172.28.1.7:9000
	21:31:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:59547 172.28.1.7:22
	21:31:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:58492 172.28.1.7:22
	21:31:20	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:56262 172.28.1.7:5222
	21:31:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.164:52117 172.28.1.7:987
	21:32:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53000 172.28.1.7:22
	21:32:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44538 172.28.1.7:22
	21:32:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:40860 172.28.1.7:22
	21:33:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.226:56414 172.28.1.7:9587
	21:33:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:35302 172.28.1.7:22
	21:33:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.184:51096 172.28.1.7:8883
	21:33:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:35174 172.28.1.7:22
	21:33:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:47362 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:34:02	ET CINS Active Threat Intelligence Poor Reputation IP group 58 [1:2403357:104040] - Misc Attack	TCP	40.124.174.73:43807 172.28.1.7:102
	21:34:06	ET CINS Active Threat Intelligence Poor Reputation IP group 33 [1:2403332:104040] - Misc Attack	TCP	20.65.193.129:42181 172.28.1.7:27017
	21:34:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52690 172.28.1.7:22
	21:34:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.12:26200 172.28.1.7:16072
	21:34:48	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.192:53875 172.28.1.7:8777
	21:34:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45420 172.28.1.7:22
	21:34:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:33672 172.28.1.7:22
	21:34:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.176:48847 172.28.1.7:9999
	21:34:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.119:52044 172.28.1.7:25827
	21:35:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.146:42411 172.28.1.7:5000
	21:35:08	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.157:51700 172.28.1.7:46639
	21:35:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36176 172.28.1.7:22
	21:35:25	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.96:35684 172.28.1.7:15
	21:35:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:49068 172.28.1.7:22
	21:35:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.209:49659 172.28.1.7:1234
	21:35:30	ET CINS Active Threat Intelligence Poor Reputation IP group 74 [1:2403373:104040] - Misc Attack	TCP	45.82.76.98:35680 172.28.1.7:3542
	21:35:33	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:54172 172.28.1.7:22
	21:35:43	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.154:53650 172.28.1.7:60731
	21:36:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56490 172.28.1.7:22
	21:36:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47428 172.28.1.7:22
	21:37:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.101:50332 172.28.1.7:9594
	21:37:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:56562 172.28.1.7:22
	21:37:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.255:54094 172.28.1.7:10010
	21:37:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:54444 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:37:39	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:51105 172.28.1.7:10001
	21:37:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:47641 172.28.1.7:22
	21:37:48	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:45456 172.28.1.7:8091
	21:38:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.234:40105 172.28.1.7:5556
	21:38:30	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50360 172.28.1.7:22
	21:38:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42440 172.28.1.7:22
	21:39:26	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34146 172.28.1.7:22
	21:39:28	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:60646 172.28.1.7:22
	21:39:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:50764 172.28.1.7:22
	21:39:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:54016 172.28.1.7:22
	21:39:48	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.10:53747 172.28.1.7:46205
	21:39:58	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.125:49781 172.28.1.7:48404
	21:40:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:48813 172.28.1.7:3389
	21:40:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53666 172.28.1.7:22
	21:40:50	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.127.156.244:57485 172.28.1.7:4332
	21:41:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.68:53983 172.28.1.7:1025
	21:41:08	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51350 172.28.1.7:22
	21:41:13	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.247:49772 172.28.1.7:47500
	21:41:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:59474 172.28.1.7:22
	21:41:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:41861 172.28.1.7:22
	21:41:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:60634 172.28.1.7:22
	21:42:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.10:22335 172.28.1.7:7777
	21:42:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42570 172.28.1.7:22
	21:43:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.69:54603 172.28.1.7:5061

	Time	Signature	Protocol	Source / Destination
	21:43:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43132 172.28.1.7:22
	21:43:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:59692 172.28.1.7:22
	21:43:36	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34532 172.28.1.7:22
	21:43:50	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.236.42.116:41072 172.28.1.7:8767
	21:43:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:49277 172.28.1.7:22
	21:44:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	198.235.24.247:52230 172.28.1.7:137
	21:44:05	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	24.199.126.56:26200 172.28.1.7:8852
	21:44:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:48540 172.28.1.7:22
	21:44:47	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50098 172.28.1.7:22
	21:45:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56622 172.28.1.7:22
	21:45:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:50890 172.28.1.7:22
	21:45:43	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60430 172.28.1.7:22
	21:45:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.235:56052 172.28.1.7:2084
	21:46:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:49045 172.28.1.7:22
	21:46:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.223:52465 172.28.1.7:8887
	21:46:41	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.108:33875 172.28.1.7:9000
	21:46:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:51554 172.28.1.7:22
	21:46:54	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54560 172.28.1.7:22
	21:47:05	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.38:51116 172.28.1.7:8531
	21:47:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36074 172.28.1.7:22
	21:47:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:43904 172.28.1.7:22
	21:47:52	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:59710 172.28.1.7:22
	21:48:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:53985 172.28.1.7:22
	21:48:31	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.73:56432 172.28.1.7:8080

	Time	Signature	Protocol	Source / Destination
	21:49:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43426 172.28.1.7:22
	21:49:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:43726 172.28.1.7:22
	21:49:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44524 172.28.1.7:22
	21:49:38	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.34:50988 172.28.1.7:52005
	21:49:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:58134 172.28.1.7:22
	21:49:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:9885
	21:49:58	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:43768 172.28.1.7:22
	21:50:21	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.184:49108 172.28.1.7:4242
	21:50:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:57667 172.28.1.7:22
	21:50:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:314
	21:51:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48644 172.28.1.7:22
	21:51:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:39812 172.28.1.7:22
	21:51:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:44484 172.28.1.7:22
	21:52:11	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51296 172.28.1.7:22
	21:52:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:48194 172.28.1.7:22
	21:52:23	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.5:51034 172.28.1.7:9029
	21:53:16	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37090 172.28.1.7:22
	21:53:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:53554 172.28.1.7:22
	21:53:47	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44754 172.28.1.7:22
	21:53:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:38958 172.28.1.7:22
	21:53:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.25:26810 172.28.1.7:5060
	21:53:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.248:47109 172.28.1.7:2244
	21:54:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41456 172.28.1.7:22
	21:54:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:54502 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:54:28	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.183:53215 172.28.1.7:18017
	21:54:45	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	20.83.32.182:44031 172.28.1.7:161
	21:54:45	ET CINS Active Threat Intelligence Poor Reputation IP group 37 [1:2403336:104040] - Misc Attack	UDP	20.83.32.182:44031 172.28.1.7:161
	21:55:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45810 172.28.1.7:22
	21:55:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:44468 172.28.1.7:22
	21:55:42	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:56254 172.28.1.7:5002
	21:55:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52572 172.28.1.7:22
	21:55:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:60036 172.28.1.7:22
	21:56:17	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:49076 172.28.1.7:22
	21:56:18	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	20.65.194.88:35832 172.28.1.7:3306
	21:56:18	ET CINS Active Threat Intelligence Poor Reputation IP group 35 [1:2403334:104040] - Misc Attack	TCP	20.65.194.88:35832 172.28.1.7:3306
	21:56:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:46183 172.28.1.7:22
	21:56:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.203:52513 172.28.1.7:2096
	21:56:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:4183 172.28.1.7:22
	21:57:15	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:34714 172.28.1.7:5431
	21:57:16	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:8622
	21:57:20	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:39322 172.28.1.7:22
	21:57:31	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52678 172.28.1.7:22
	21:57:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.243:55390 172.28.1.7:3333
	21:57:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43554 172.28.1.7:22
	21:58:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:38602 172.28.1.7:22
	21:58:22	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:58858 172.28.1.7:22
	21:58:34	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	UDP	20.29.56.247:37336 172.28.1.7:161
	21:58:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:53737 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	21:59:22	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:57870 172.28.1.7:22
	21:59:24	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.120.173:49874 172.28.1.7:11211
	21:59:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54480 172.28.1.7:22
	22:00:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50636 172.28.1.7:22
	22:00:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:50998 172.28.1.7:22
	22:00:31	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45168 172.28.1.7:22
	22:00:44	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:44638 172.28.1.7:22
	22:00:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:26200 172.28.1.7:9204
	22:00:49	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.62.106:56176 172.28.1.7:40000
	22:01:04	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:26200 172.28.1.7:8916
	22:01:27	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:34564 172.28.1.7:22
	22:01:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.227:51158 172.28.1.7:3929
	22:01:43	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60298 172.28.1.7:22
	22:02:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.200:51729 172.28.1.7:143
	22:02:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51230 172.28.1.7:22
	22:02:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:55684 172.28.1.7:22
	22:02:36	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38118 172.28.1.7:22
	22:02:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	91.196.152.147:24200 172.28.1.7:636
	22:02:44	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:59913 172.28.1.7:8089
	22:02:57	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:46581 172.28.1.7:22
	22:03:19	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.207:56241 172.28.1.7:3000
	22:03:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:52224 172.28.1.7:22
	22:03:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58250 172.28.1.7:22
	22:03:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:23320 172.28.1.7:5986

	Time	Signature	Protocol	Source / Destination
	22:04:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52484 172.28.1.7:22
	22:04:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:43484 172.28.1.7:22
	22:04:43	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45380 172.28.1.7:22
	22:05:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:51744 172.28.1.7:22
	22:05:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.96:51935 172.28.1.7:9983
	22:05:38	ET CINS Active Threat Intelligence Poor Reputation IP group 25 [1:2403324:104040] - Misc Attack	UDP	20.169.107.128:47793 172.28.1.7:8081
	22:05:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:60990 172.28.1.7:22
	22:05:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48284 172.28.1.7:22
	22:06:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:44574 172.28.1.7:22
	22:06:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46674 172.28.1.7:22
	22:06:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41500 172.28.1.7:22
	22:07:17	ET CINS Active Threat Intelligence Poor Reputation IP group 67 [1:2403366:104040] - Misc Attack	TCP	45.156.128.53:42374 172.28.1.7:10000
	22:07:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:48133 172.28.1.7:22
	22:07:19	ET CINS Active Threat Intelligence Poor Reputation IP group 85 [1:2403384:104040] - Misc Attack	TCP	51.15.220.227:52836 172.28.1.7:6375
	22:07:48	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.99:53189 172.28.1.7:3358
	22:07:53	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:36314 172.28.1.7:22
	22:07:58	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46346 172.28.1.7:22
	22:07:58	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.160:53509 172.28.1.7:45882
	22:08:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.165:52180 172.28.1.7:111
	22:08:28	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:36990 172.28.1.7:22
	22:08:55	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36274 172.28.1.7:22
	22:09:26	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:41818 172.28.1.7:22
	22:09:36	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5263 172.28.1.7:5060
	22:09:36	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5263 172.28.1.7:5060

	Time	Signature	Protocol	Source / Destination
	22:09:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.53:53557 172.28.1.7:83
	22:09:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:44569 172.28.1.7:3399
	22:09:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.208:56606 172.28.1.7:11211
	22:09:58	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:33116 172.28.1.7:22
	22:10:01	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40576 172.28.1.7:22
	22:10:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.74:49994 172.28.1.7:8282
	22:10:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44736 172.28.1.7:22
	22:10:38	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:59256 172.28.1.7:22
	22:10:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.29:55746 172.28.1.7:21515
	22:10:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42860 172.28.1.7:22
	22:11:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:55440 172.28.1.7:22
	22:12:02	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:53500 172.28.1.7:22
	22:12:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36210 172.28.1.7:22
	22:12:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.121:50058 172.28.1.7:49952
	22:12:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.253:49465 172.28.1.7:49452
	22:12:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43558 172.28.1.7:22
	22:12:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:39170 172.28.1.7:22
	22:12:47	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.185:22265 172.28.1.7:1961
	22:13:02	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42690 172.28.1.7:22
	22:13:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.54:55610 172.28.1.7:4022
	22:13:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:51729 172.28.1.7:22
	22:13:58	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:44686 172.28.1.7:7000
	22:14:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:40136 172.28.1.7:22
	22:14:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36272 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	22:14:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38542 172.28.1.7:22
	22:14:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:59584 172.28.1.7:22
	22:14:51	ET CINS Active Threat Intelligence Poor Reputation IP group 27 [1:2403326:104040] - Misc Attack	TCP	20.29.22.204:35305 172.28.1.7:18245
	22:15:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:28693 172.28.1.7:70
	22:15:08	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34846 172.28.1.7:22
	22:15:13	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.231:54955 172.28.1.7:110
	22:15:59	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:50774 172.28.1.7:22
	22:16:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:56612 172.28.1.7:22
	22:16:20	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46180 172.28.1.7:22
	22:16:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:52658 172.28.1.7:22
	22:16:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:48350 172.28.1.7:22
	22:17:14	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55758 172.28.1.7:22
	22:17:16	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:56367 172.28.1.7:5900
	22:17:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8008
	22:17:32	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.99:58914 172.28.1.7:8008
	22:17:38	ET CINS Active Threat Intelligence Poor Reputation IP group 20 [1:2403319:104040] - Misc Attack	TCP	20.163.33.220:52848 172.28.1.7:2323
	22:18:09	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:44260 172.28.1.7:22
	22:18:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:47981 172.28.1.7:22
	22:18:15	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.59.96:42238 172.28.1.7:30011
	22:18:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53428 172.28.1.7:22
	22:18:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2080
	22:18:33	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.142.154.98:58914 172.28.1.7:2080
	22:18:41	ET CINS Active Threat Intelligence Poor Reputation IP group 6 [1:2403305:104040] - Misc Attack	TCP	8.209.96.38:11519 172.28.1.7:8014
	22:18:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.89:52452 172.28.1.7:2161

	Time	Signature	Protocol	Source / Destination
	22:18:55	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58536 172.28.1.7:22
	22:19:01	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.8.46:42485 172.28.1.7:20201
	22:19:01	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.214.73:20217 172.28.1.7:8333
	22:19:05	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	157.245.75.204:54690 172.28.1.7:22
	22:19:21	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56732 172.28.1.7:22
	22:19:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.57:53705 172.28.1.7:3443
	22:20:05	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.217.194.148:42378 172.28.1.7:444
	22:20:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.233:52929 172.28.1.7:443
	22:20:14	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:53728 172.28.1.7:22
	22:20:23	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:46492 172.28.1.7:22
	22:20:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46036 172.28.1.7:22
	22:20:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:32812 172.28.1.7:22
	22:21:01	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.9.231:21020 172.28.1.7:8175
	22:21:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.148:14387 172.28.1.7:7547
	22:21:16	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:44680 172.28.1.7:55555
	22:21:26	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40856 172.28.1.7:22
	22:22:15	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:40844 172.28.1.7:22
	22:22:30	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.208.236:39754 172.28.1.7:631
	22:22:33	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:59960 172.28.1.7:22
	22:22:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55298 172.28.1.7:22
	22:22:43	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.74:52468 172.28.1.7:48935
	22:22:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.70:52171 172.28.1.7:82
	22:23:03	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.92.56:29849 172.28.1.7:12192
	22:23:04	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:55662 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	22:23:28	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56296 172.28.1.7:22
	22:24:18	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:51968 172.28.1.7:3389
	22:24:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:43650 172.28.1.7:22
	22:24:24	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.79:54201 172.28.1.7:5901
	22:24:35	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:48652 172.28.1.7:22
	22:24:36	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37322 172.28.1.7:22
	22:24:48	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.146:51036 172.28.1.7:46625
	22:24:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:23320 172.28.1.7:9002
	22:25:07	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40244 172.28.1.7:22
	22:25:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.223:53412 172.28.1.7:6099
	22:25:38	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47142 172.28.1.7:22
	22:26:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:42436 172.28.1.7:22
	22:26:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:55774 172.28.1.7:22
	22:26:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34200 172.28.1.7:22
	22:27:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.59:49509 172.28.1.7:88
	22:27:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:19222 172.28.1.7:1025
	22:27:22	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44136 172.28.1.7:22
	22:27:45	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41564 172.28.1.7:22
	22:27:52	ET CINS Active Threat Intelligence Poor Reputation IP group 90 [1:2403389:104040] - Misc Attack	TCP	57.151.105.130:52598 172.28.1.7:11743
	22:28:50	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:49029 172.28.1.7:22
	22:28:55	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60850 172.28.1.7:22
	22:29:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:32962 172.28.1.7:22
	22:29:13	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.115.242:15468 172.28.1.7:7704
	22:29:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.49:49784 172.28.1.7:2160

	Time	Signature	Protocol	Source / Destination
	22:29:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41912 172.28.1.7:22
	22:29:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.204:53473 172.28.1.7:5902
	22:29:45	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.38.35.154:52283 172.28.1.7:5902
	22:29:50	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:47630 172.28.1.7:22
	22:29:54	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.80:52263 172.28.1.7:2002
	22:30:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:8147
	22:30:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.239:53137 172.28.1.7:1521
	22:30:12	ET SCAN Suspicious inbound to Oracle SQL port 1521 [1:2010936:3] - Potentially Bad Traffic	TCP	193.163.125.239:53137 172.28.1.7:1521
	22:30:39	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	TCP	23.95.186.189:51601 172.28.1.7:7789
	22:30:55	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.223.104.85:58613 172.28.1.7:30003
	22:31:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56930 172.28.1.7:22
	22:31:00	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:40716 172.28.1.7:22
	22:31:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:38158 172.28.1.7:22
	22:31:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.221:49311 172.28.1.7:50998
	22:31:57	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:46244 172.28.1.7:22
	22:31:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.187:26861 172.28.1.7:22822
	22:32:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.227:55256 172.28.1.7:28000
	22:33:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:43552 172.28.1.7:22
	22:33:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50228 172.28.1.7:22
	22:33:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	218.23.170.184:56092 172.28.1.7:22
	22:33:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.244:44021 172.28.1.7:15672
	22:33:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.90:56098 172.28.1.7:8081
	22:33:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57784 172.28.1.7:22
	22:34:00	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:35820 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	22:35:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:55532 172.28.1.7:22
	22:35:11	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33558 172.28.1.7:22
	22:35:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38844 172.28.1.7:22
	22:35:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.211:49725 172.28.1.7:7547
	22:36:04	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:58258 172.28.1.7:22
	22:36:22	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.60.95:32742 172.28.1.7:2105
	22:36:36	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:29011 172.28.1.7:9191
	22:36:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	64.62.197.67:40213 172.28.1.7:1111
	22:37:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58724 172.28.1.7:22
	22:37:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:44064 172.28.1.7:22
	22:37:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:58576 172.28.1.7:22
	22:38:09	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54672 172.28.1.7:22
	22:39:02	ET CINS Active Threat Intelligence Poor Reputation IP group 23 [1:2403322:104040] - Misc Attack	TCP	20.168.6.85:42603 172.28.1.7:2375
	22:39:18	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60268 172.28.1.7:22
	22:39:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:34336 172.28.1.7:22
	22:40:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60334 172.28.1.7:22
	22:41:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41412 172.28.1.7:22
	22:41:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:40406 172.28.1.7:22
	22:41:56	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:49906 172.28.1.7:22
	22:42:22	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55862 172.28.1.7:22
	22:42:36	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:58602 172.28.1.7:10002
	22:43:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38446 172.28.1.7:22
	22:43:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.149:44982 172.28.1.7:18245
	22:44:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48246 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	22:44:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:55252 172.28.1.7:22
	22:44:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.147:18224 172.28.1.7:4433
	22:44:26	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55022 172.28.1.7:22
	22:44:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.145:46834 172.28.1.7:8008
	22:45:13	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.211.112:49747 172.28.1.7:9996
	22:45:19	ET CINS Active Threat Intelligence Poor Reputation IP group 65 [1:2403364:104040] - Misc Attack	TCP	45.135.95.25:56241 172.28.1.7:5269
	22:45:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41434 172.28.1.7:22
	22:45:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.222:54483 172.28.1.7:51005
	22:45:49	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:54736 172.28.1.7:3389
	22:46:07	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57688 172.28.1.7:22
	22:46:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:60344 172.28.1.7:22
	22:46:23	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.226:44302 172.28.1.7:587
	22:46:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60614 172.28.1.7:22
	22:46:43	GPL SNMP public access udp [1:2101411:13] - Attempted Information Leak	UDP	165.154.179.204:32959 172.28.1.7:161
	22:47:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.30:51687 172.28.1.7:8094
	22:47:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39684 172.28.1.7:22
	22:47:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.145:64920 172.28.1.7:389
	22:48:10	ET CINS Active Threat Intelligence Poor Reputation IP group 24 [1:2403323:104040] - Misc Attack	UDP	20.169.104.60:55457 172.28.1.7:9433
	22:48:18	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:35718 172.28.1.7:22
	22:48:34	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	207.90.244.21:8584 172.28.1.7:3391
	22:48:37	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:40026 172.28.1.7:22
	22:48:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.79:55773 172.28.1.7:88
	22:49:29	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.46:41611 172.28.1.7:6443
	22:49:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:8026

	Time	Signature	Protocol	Source / Destination
	22:49:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59768 172.28.1.7:22
	22:50:18	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36936 172.28.1.7:22
	22:50:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:42658 172.28.1.7:22
	22:50:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54304 172.28.1.7:22
	22:50:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.24:26200 172.28.1.7:9289
	22:51:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.10:26200 172.28.1.7:5433
	22:51:51	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40644 172.28.1.7:22
	22:51:58	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.67:50476 172.28.1.7:46997
	22:52:10	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:32350 172.28.1.7:22
	22:52:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44224 172.28.1.7:22
	22:52:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:41788 172.28.1.7:22
	22:52:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:58418 172.28.1.7:22
	22:52:52	ET CINS Active Threat Intelligence Poor Reputation IP group 82 [1:2403381:104040] - Misc Attack	TCP	47.74.63.114:57910 172.28.1.7:5500
	22:53:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9017
	22:53:07	ET CINS Active Threat Intelligence Poor Reputation IP group 80 [1:2403379:104040] - Misc Attack	TCP	47.251.86.165:57275 172.28.1.7:8131
	22:53:13	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.122.207:43465 172.28.1.7:9091
	22:53:52	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50592 172.28.1.7:22
	22:54:23	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40818 172.28.1.7:22
	22:54:48	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:56548 172.28.1.7:22
	22:54:53	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60152 172.28.1.7:22
	22:55:03	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.111:51270 172.28.1.7:81
	22:55:26	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.80.105.50:52300 172.28.1.7:8192
	22:55:51	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.20:26200 172.28.1.7:12352
	22:56:02	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50524 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	22:56:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.242:50150 172.28.1.7:5906
	22:56:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47528 172.28.1.7:22
	22:56:58	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33656 172.28.1.7:22
	22:57:07	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:55308 172.28.1.7:22
	22:57:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.203:54340 172.28.1.7:12345
	22:58:07	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53990 172.28.1.7:22
	22:58:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.3:26200 172.28.1.7:16400
	22:58:39	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46992 172.28.1.7:22
	22:59:03	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:58202 172.28.1.7:22
	22:59:19	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	178.128.247.39:35768 172.28.1.7:22
	22:59:48	ET CINS Active Threat Intelligence Poor Reputation IP group 48 [1:2403347:104040] - Misc Attack	TCP	35.203.210.99:55094 172.28.1.7:59522
	22:59:59	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.104:52172 172.28.1.7:9002
	23:00:00	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.132:37364 172.28.1.7:771
	23:00:11	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50538 172.28.1.7:22
	23:00:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	199.45.154.180:60282 172.28.1.7:10259
	23:00:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46566 172.28.1.7:22
	23:01:08	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55352 172.28.1.7:22
	23:02:08	ET CINS Active Threat Intelligence Poor Reputation IP group 43 [1:2403342:104040] - Misc Attack	TCP	35.203.210.128:50899 172.28.1.7:47198
	23:02:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:60700 172.28.1.7:22
	23:02:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	205.210.31.178:53095 172.28.1.7:5060
	23:02:43	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.76:49437 172.28.1.7:45249
	23:02:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59900 172.28.1.7:22
	23:02:50	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.25:26200 172.28.1.7:8168
	23:03:01	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.143:56785 172.28.1.7:46338

	Time	Signature	Protocol	Source / Destination
	23:03:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.26:29011 172.28.1.7:37215
	23:03:14	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:58024 172.28.1.7:22
	23:03:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.144:56392 172.28.1.7:40000
	23:04:22	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54538 172.28.1.7:22
	23:04:41	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	65.60.34.138:5066 172.28.1.7:5060
	23:04:41	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	65.60.34.138:5066 172.28.1.7:5060
	23:04:43	ET CINS Active Threat Intelligence Poor Reputation IP group 45 [1:2403344:104040] - Misc Attack	TCP	35.203.210.221:50513 172.28.1.7:9221
	23:04:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:46670 172.28.1.7:22
	23:05:13	ET CINS Active Threat Intelligence Poor Reputation IP group 34 [1:2403333:104040] - Misc Attack	TCP	20.65.194.27:49765 172.28.1.7:27019
	23:05:21	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:39222 172.28.1.7:22
	23:05:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.17:26200 172.28.1.7:12237
	23:05:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.47:51424 172.28.1.7:80
	23:05:40	ET CINS Active Threat Intelligence Poor Reputation IP group 79 [1:2403378:104040] - Misc Attack	TCP	47.251.85.121:50999 172.28.1.7:8249
	23:06:24	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	TCP	20.127.170.152:35517 172.28.1.7:5061
	23:06:28	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.153:55011 172.28.1.7:46896
	23:06:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33700 172.28.1.7:22
	23:06:52	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.190.163.148:60901 172.28.1.7:9500
	23:07:00	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59560 172.28.1.7:22
	23:07:24	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45984 172.28.1.7:22
	23:08:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.147:5942 172.28.1.7:833
	23:08:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43242 172.28.1.7:22
	23:08:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.83:52868 172.28.1.7:9998
	23:08:37	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	93.152.230.178:48772 172.28.1.7:22
	23:08:44	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.243:40406 172.28.1.7:1090

	Time	Signature	Protocol	Source / Destination
	23:08:52	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.225.74.178:26200 172.28.1.7:21304
	23:09:33	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54562 172.28.1.7:22
	23:09:49	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	UDP	52.188.189.7:34830 172.28.1.7:123
	23:10:37	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:42524 172.28.1.7:22
	23:11:08	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33666 172.28.1.7:22
	23:11:23	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.188.189.6:47600 172.28.1.7:9030
	23:11:34	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:56900 172.28.1.7:22
	23:11:35	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:52476 172.28.1.7:22
	23:12:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.232:42808 172.28.1.7:1611
	23:12:33	ET CINS Active Threat Intelligence Poor Reputation IP group 6 [1:2403305:104040] - Misc Attack	TCP	8.211.39.215:12397 172.28.1.7:8291
	23:12:45	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:54344 172.28.1.7:22
	23:12:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.146:65248 172.28.1.7:53282
	23:13:13	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.39:56396 172.28.1.7:45846
	23:13:17	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50330 172.28.1.7:22
	23:13:41	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:44800 172.28.1.7:22
	23:13:41	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:37984 172.28.1.7:22
	23:14:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	66.132.153.156:51102 172.28.1.7:61616
	23:14:36	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.246:36917 172.28.1.7:20108
	23:14:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39114 172.28.1.7:22
	23:15:21	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33738 172.28.1.7:22
	23:15:45	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:51100 172.28.1.7:22
	23:15:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:49156 172.28.1.7:22
	23:16:04	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.242:42194 172.28.1.7:9300
	23:16:22	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	TCP	64.23.161.101:18438 172.28.1.7:50100

	Time	Signature	Protocol	Source / Destination
	23:16:38	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.23:56317 172.28.1.7:46073
	23:16:55	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:48654 172.28.1.7:22
	23:17:08	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.145:50980 172.28.1.7:49979
	23:17:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:39868 172.28.1.7:22
	23:17:28	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.139:55293 172.28.1.7:50037
	23:17:39	ET CINS Active Threat Intelligence Poor Reputation IP group 28 [1:2403327:104040] - Misc Attack	TCP	20.29.57.212:50751 172.28.1.7:9000
	23:17:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:58790 172.28.1.7:22
	23:17:52	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:55618 172.28.1.7:22
	23:18:02	ET CINS Active Threat Intelligence Poor Reputation IP group 16 [1:2403315:104040] - Misc Attack	UDP	20.119.99.184:53116 172.28.1.7:5632
	23:18:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.6:26200 172.28.1.7:16003
	23:18:30	ET CINS Active Threat Intelligence Poor Reputation IP group 39 [1:2403338:104040] - Misc Attack	UDP	24.199.126.56:19986 172.28.1.7:5008
	23:18:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.13:18438 172.28.1.7:30002
	23:19:03	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41618 172.28.1.7:22
	23:19:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56482 172.28.1.7:22
	23:19:38	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.18:57226 172.28.1.7:53208
	23:19:47	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:48164 172.28.1.7:22
	23:19:58	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36384 172.28.1.7:22
	23:20:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.246:50879 172.28.1.7:3493
	23:21:07	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47954 172.28.1.7:22
	23:21:52	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:58756 172.28.1.7:22
	23:22:08	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:60830 172.28.1.7:22
	23:22:20	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.2:26200 172.28.1.7:452
	23:22:58	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.224:50744 172.28.1.7:8009
	23:23:10	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.108:53216 172.28.1.7:389

	Time	Signature	Protocol	Source / Destination
	23:23:13	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47926 172.28.1.7:22
	23:23:28	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.155:56896 172.28.1.7:47984
	23:23:28	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.230:49197 172.28.1.7:9255
	23:23:50	ET CINS Active Threat Intelligence Poor Reputation IP group 8 [1:2403307:104040] - Misc Attack	TCP	8.219.248.225:13972 172.28.1.7:12575
	23:23:56	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	62.3.58.23:5060 172.28.1.7:5060
	23:23:56	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	62.3.58.23:5060 172.28.1.7:5060
	23:24:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:36696 172.28.1.7:22
	23:24:03	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.212:55592 172.28.1.7:9048
	23:24:11	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:50658 172.28.1.7:22
	23:25:03	ET SCAN Sipvicious Scan [1:2008578:4] - Attempted Information Leak	UDP	62.210.6.159:5320 172.28.1.7:5060
	23:25:03	ET SCAN Sipvicious User-Agent Detected (friendly-scanner) [1:2011716:3] - Attempted Information Leak	UDP	62.210.6.159:5320 172.28.1.7:5060
	23:25:03	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	UDP	62.210.6.159:5320 172.28.1.7:5060
	23:25:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47490 172.28.1.7:22
	23:25:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.222:33820 172.28.1.7:2007
	23:25:43	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36450 172.28.1.7:22
	23:26:10	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:49012 172.28.1.7:22
	23:26:13	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:58560 172.28.1.7:22
	23:26:23	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.47:57303 172.28.1.7:49241
	23:27:22	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45752 172.28.1.7:22
	23:27:40	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.101:61625 172.28.1.7:32309
	23:27:53	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41622 172.28.1.7:22
	23:28:02	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.23:26200 172.28.1.7:16002
	23:28:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.29:56430 172.28.1.7:51009
	23:28:16	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:51552 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	23:28:24	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:34820 172.28.1.7:22
	23:28:39	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.245:50648 172.28.1.7:2147
	23:28:55	ET CINS Active Threat Intelligence Poor Reputation IP group 47 [1:2403346:104040] - Misc Attack	TCP	35.203.210.58:55655 172.28.1.7:13228
	23:29:21	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.188.81.67:42472 172.28.1.7:7474
	23:29:27	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:33208 172.28.1.7:22
	23:29:45	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.126:54088 172.28.1.7:1144
	23:30:08	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.46:41507 172.28.1.7:5900
	23:30:13	ET CINS Active Threat Intelligence Poor Reputation IP group 98 [1:2403397:104040] - Misc Attack	UDP	64.23.214.73:1143 172.28.1.7:5683
	23:30:17	ET SCAN Suspicious inbound to PostgreSQL port 5432 [1:2010939:3] - Potentially Bad Traffic	TCP	52.14.58.0:57471 172.28.1.7:5432
	23:30:17	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.14.58.0:57471 172.28.1.7:5432
	23:30:20	ET CINS Active Threat Intelligence Poor Reputation IP group 11 [1:2403310:104040] - Misc Attack	TCP	13.89.125.25:32806 172.28.1.7:953
	23:30:24	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:52992 172.28.1.7:22
	23:30:30	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.180.156.198:51985 172.28.1.7:49152
	23:30:30	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.81:54827 172.28.1.7:8530
	23:30:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:54340 172.28.1.7:22
	23:31:18	ET CINS Active Threat Intelligence Poor Reputation IP group 51 [1:2403350:104040] - Misc Attack	TCP	35.203.211.49:53341 172.28.1.7:48839
	23:31:25	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36656 172.28.1.7:22
	23:31:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.18:26200 172.28.1.7:5557
	23:31:32	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.247:55863 172.28.1.7:593
	23:31:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40650 172.28.1.7:22
	23:32:11	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.122:53155 172.28.1.7:57955
	23:32:24	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36538 172.28.1.7:22
	23:32:28	ET CINS Active Threat Intelligence Poor Reputation IP group 68 [1:2403367:104040] - Misc Attack	TCP	45.156.129.118:31954 172.28.1.7:9443
	23:32:43	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:50902 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	23:32:47	ET CINS Active Threat Intelligence Poor Reputation IP group 78 [1:2403377:104040] - Misc Attack	TCP	47.250.143.163:49203 172.28.1.7:10019
	23:32:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:35988 172.28.1.7:22
	23:32:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	205.210.31.232:54063 172.28.1.7:6002
	23:32:58	ET CINS Active Threat Intelligence Poor Reputation IP group 49 [1:2403348:104040] - Misc Attack	TCP	35.203.211.180:53732 172.28.1.7:28500
	23:33:06	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.32:55498 172.28.1.7:9408
	23:33:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.40:50570 172.28.1.7:22
	23:33:19	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.143.152.247:42012 172.28.1.7:2000
	23:33:34	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:43898 172.28.1.7:22
	23:34:06	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:51116 172.28.1.7:22
	23:34:14	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.236:57609 172.28.1.7:50092
	23:34:24	ET CINS Active Threat Intelligence Poor Reputation IP group 21 [1:2403320:104040] - Misc Attack	TCP	20.168.0.45:53105 172.28.1.7:1900
	23:34:29	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.58:54587 172.28.1.7:38080
	23:34:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:44614 172.28.1.7:22
	23:34:41	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.188:52566 172.28.1.7:46114
	23:34:46	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:58936 172.28.1.7:22
	23:35:01	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.140.212:37670 172.28.1.7:10014
	23:35:40	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50430 172.28.1.7:22
	23:36:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:47804 172.28.1.7:22
	23:36:31	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:37268 172.28.1.7:22
	23:36:36	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:41848 172.28.1.7:22
	23:36:36	ET CINS Active Threat Intelligence Poor Reputation IP group 96 [1:2403395:104040] - Misc Attack	TCP	64.226.86.7:16592 172.28.1.7:11211
	23:36:39	ET CINS Active Threat Intelligence Poor Reputation IP group 17 [1:2403316:104040] - Misc Attack	TCP	20.14.73.54:47033 172.28.1.7:5094
	23:37:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:51668 172.28.1.7:22
	23:37:27	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.158:1078 172.28.1.7:4841

	Time	Signature	Protocol	Source / Destination
	23:37:47	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50080 172.28.1.7:22
	23:37:53	ET CINS Active Threat Intelligence Poor Reputation IP group 50 [1:2403349:104040] - Misc Attack	TCP	35.203.211.224:51968 172.28.1.7:46248
	23:38:13	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.47:53845 172.28.1.7:46155
	23:38:18	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:56480 172.28.1.7:22
	23:38:40	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:57416 172.28.1.7:22
	23:39:06	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:47798 172.28.1.7:22
	23:39:48	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.159:56484 172.28.1.7:64227
	23:39:48	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37756 172.28.1.7:22
	23:40:08	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:54474 172.28.1.7:22
	23:40:12	ET CINS Active Threat Intelligence Poor Reputation IP group 9 [1:2403308:104040] - Misc Attack	TCP	8.221.141.145:13822 172.28.1.7:2052
	23:40:24	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37888 172.28.1.7:22
	23:40:47	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:44566 172.28.1.7:22
	23:41:11	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:55782 172.28.1.7:22
	23:41:35	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.19:26200 172.28.1.7:12172
	23:41:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.96:51110 172.28.1.7:4567
	23:41:43	ET CINS Active Threat Intelligence Poor Reputation IP group 46 [1:2403345:104040] - Misc Attack	TCP	35.203.210.252:52343 172.28.1.7:50013
	23:41:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44926 172.28.1.7:22
	23:42:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53846 172.28.1.7:22
	23:42:52	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	UDP	193.163.125.212:22996 172.28.1.7:4500
	23:42:54	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:36416 172.28.1.7:22
	23:43:21	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:40230 172.28.1.7:22
	23:43:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:38838 172.28.1.7:22
	23:43:58	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	117.146.110.78:41117 172.28.1.7:3306
	23:43:59	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40312 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	23:44:33	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40920 172.28.1.7:22
	23:45:01	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:34392 172.28.1.7:22
	23:45:11	ET CINS Active Threat Intelligence Poor Reputation IP group 13 [1:2403312:104040] - Misc Attack	TCP	18.117.57.162:33670 172.28.1.7:8180
	23:45:32	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:43924 172.28.1.7:22
	23:45:52	ET CINS Active Threat Intelligence Poor Reputation IP group 22 [1:2403321:104040] - Misc Attack	TCP	20.168.124.152:48597 172.28.1.7:2181
	23:46:10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:38050 172.28.1.7:22
	23:46:44	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57222 172.28.1.7:22
	23:47:03	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:55860 172.28.1.7:22
	23:47:07	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.22:26200 172.28.1.7:9922
	23:47:07	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:38928 172.28.1.7:22
	23:47:39	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	84.242.54.23:1890 172.28.1.7:22
	23:47:42	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:48460 172.28.1.7:22
	23:47:48	ET CINS Active Threat Intelligence Poor Reputation IP group 87 [1:2403386:104040] - Misc Attack	TCP	52.180.136.250:48023 172.28.1.7:8009
	23:48:19	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:53852 172.28.1.7:22
	23:48:33	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.56:49886 172.28.1.7:5555
	23:48:50	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:41586 172.28.1.7:22
	23:48:53	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.27:26200 172.28.1.7:3580
	23:48:57	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.205:53923 172.28.1.7:9997
	23:49:03	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.136.67.107:55546 172.28.1.7:888
	23:49:12	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:42348 172.28.1.7:22
	23:49:54	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:35700 172.28.1.7:22
	23:50:12	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	207.90.244.5:26200 172.28.1.7:7084
	23:50:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:53270 172.28.1.7:22
	23:50:21	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:50578 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	23:50:22	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.237.115.193:52471 172.28.1.7:12207
	23:50:24	ET CINS Active Threat Intelligence Poor Reputation IP group 76 [1:2403375:104040] - Misc Attack	TCP	47.236.242.199:40290 172.28.1.7:8000
	23:50:45	ET CINS Active Threat Intelligence Poor Reputation IP group 86 [1:2403385:104040] - Misc Attack	TCP	52.15.85.154:34521 172.28.1.7:8181
	23:50:52	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:37900 172.28.1.7:22
	23:51:05	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.172:52677 172.28.1.7:80
	23:51:18	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:44858 172.28.1.7:22
	23:51:48	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	167.94.138.154:3588 172.28.1.7:2053
	23:52:01	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:46824 172.28.1.7:22
	23:52:29	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:45746 172.28.1.7:22
	23:52:58	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.152:52649 172.28.1.7:49480
	23:53:22	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.231:47562 172.28.1.7:31932
	23:53:28	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	198.235.24.64:51301 172.28.1.7:47001
	23:53:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:56664 172.28.1.7:22
	23:53:37	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:56086 172.28.1.7:22
	23:54:12	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:36908 172.28.1.7:22
	23:54:13	ET CINS Active Threat Intelligence Poor Reputation IP group 14 [1:2403313:104040] - Misc Attack	TCP	18.221.137.47:58446 172.28.1.7:9080
	23:54:15	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.24:53878 172.28.1.7:1717
	23:54:35	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:57304 172.28.1.7:22
	23:55:05	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:40098 172.28.1.7:22
	23:55:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.22:50864 172.28.1.7:4786
	23:55:30	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:45606 172.28.1.7:22
	23:56:17	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:54580 172.28.1.7:22
	23:56:42	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:36842 172.28.1.7:22
	23:56:51	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	206.189.3.149:43868 172.28.1.7:22

	Time	Signature	Protocol	Source / Destination
	23:57:03	ET CINS Active Threat Intelligence Poor Reputation IP group 44 [1:2403343:104040] - Misc Attack	TCP	35.203.210.164:56621 172.28.1.7:50582
	23:57:09	ET CINS Active Threat Intelligence Poor Reputation IP group 36 [1:2403335:104040] - Misc Attack	TCP	20.80.105.157:48500 172.28.1.7:10024
	23:57:38	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.38:44569 172.28.1.7:3392
	23:57:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:54694 172.28.1.7:22
	23:58:02	ET CINS Active Threat Intelligence Poor Reputation IP group 3 [1:2403302:104040] - Misc Attack	TCP	3.148.147.222:44234 172.28.1.7:110
	23:58:25	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	147.185.132.118:55183 172.28.1.7:2078
	23:58:25	ET INFO SSH-2.0-Go version string Observed in Network Traffic [1:2038967:1] - Misc activity	TCP	167.172.36.39:33344 172.28.1.7:22
	23:58:26	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	193.163.125.229:56398 172.28.1.7:21272
	23:58:41	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:44976 172.28.1.7:22
	23:58:46	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.130:57723 172.28.1.7:3389
	23:58:58	ET CINS Active Threat Intelligence Poor Reputation IP group 52 [1:2403351:104040] - Misc Attack	TCP	35.203.211.56:53619 172.28.1.7:20222
	23:59:11	ET SCAN Suspicious inbound to mySQL port 3306 [1:2010937:3] - Potentially Bad Traffic	TCP	176.32.195.85:60023 172.28.1.7:3306
	23:59:14	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [1:2006546:9] - Attempted Administrator Privilege Gain	TCP	181.78.211.242:59480 172.28.1.7:22
	23:59:39	ET SCAN Potential SSH Scan [1:2001219:20] - Attempted Information Leak	TCP	181.78.211.242:33100 172.28.1.7:22
	23:59:43	ET DROP Dshield Block Listed Source group 1 [1:2402000:7537] - Misc Attack	TCP	78.128.114.170:41958 172.28.1.7:9144