Malware Research and Coordination Facility Project

Monthly Trend Report

FEBRUARY 2020

CyberSecurity MALAYSIA

Powered by:

LebahNET.MY
CyberSecurity Honeynet Project

Disclaimer
This document is for informational purposes only. Every effort has been made to make this document as complete as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. CyberSecurity Malaysia, an agency under the Ministry of Communications and Multimedia Malaysia shall has neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.
The logos and names of organizations and products mentioned herein are the trademarks of their respective owners. Use of the logos and names do not imply any affiliation with or endorsement by the respective organizations.

Executive Summary

All malwares that are successfully captured under the Malware Research and Coordination Facility Project have high severity impact to the systems and networks affecting a total of 3630 devices. It involves data unavailability, data breaches, and backdoor activities. The list of captured malware consists of WannaCry, Occamy, Small, Eqtonex, Linux.XorDdos, Zombieboy and Tiggre.

The main threat is the WannaCry malware with 1732 malwares captured. This is followed by Small with 736 malwares captured; Tiggre with 655 malwares captured; Zombieboy with 230 malwares captured; Occamy with 96 malwares captured; Eqtonex with 93 malwares captured; and finally, the Linux.XorDdos and with 88 malwares being captured.

Introduction

A malware is a malicious software which is intended to cause harm to the users' system or network. Each malware has different capabilities that can cause changes / damages to the targeted system or network such as the ability to spread itself in the network and remain undetectable. This kind of software can bring down the machine's performance to a complete stop which may cause destructions. A computer can be infected and is no longer usable, rendering the data inside it unavailable – these are some of the damage scenarios inflicted by malwares. Malware usages can be traced back to the time when the Internet is still at its infant stage.

About the Project

The Malware Research and Coordination Facility Project (the Project) is initiated by CyberSecurity Malaysia, which is also the Permanent Secretariat of the OIC-CERT. The participating agencies / organisations subscribing to this Project, mainly members of the OIC-CERT and APCERT, share malware data that allow collective malware threat analysis to be done.

Such analysis from the Project data provides early detection of malware, assist to provide awareness to the public, and for the cyber security personnel to act accordingly based on the shared information.

WannaCry Tiggre

Occamy Linux.XorDdos Zombieboy

Eqtonex Small

OIC-CERT : Organization of the Islamic Cooperation – Computer Emergency Response Team
APCERT : Asia Pacific Computer Emergency Response Team

Attack Type

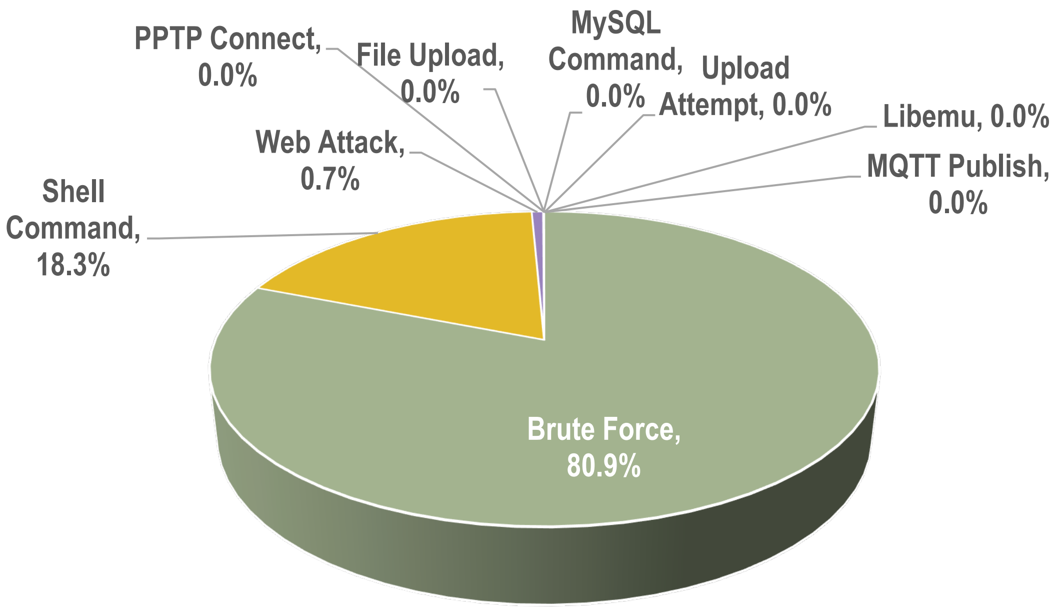

Figure 1 Attack Types

Figure 1 above illustrates the statistics of attack types recorded in February 2020. Based on Figure 1, Brute Force recorded the highest attack with 80.9%, followed by Shell Command attack with 18.3% and Web Attack with 0.7%.

Table 1 Attack Types

ATTACK TYPE	TOTAL
Brute Force	13,799,762
Shell Command	3,128,770
Web Attack	112,418
MySQL Command	5,473
File Upload	4,320
Upload Attempt	280
Libemu	182
PPTP Connect	11
MQTT Publish	2

Targeted Services

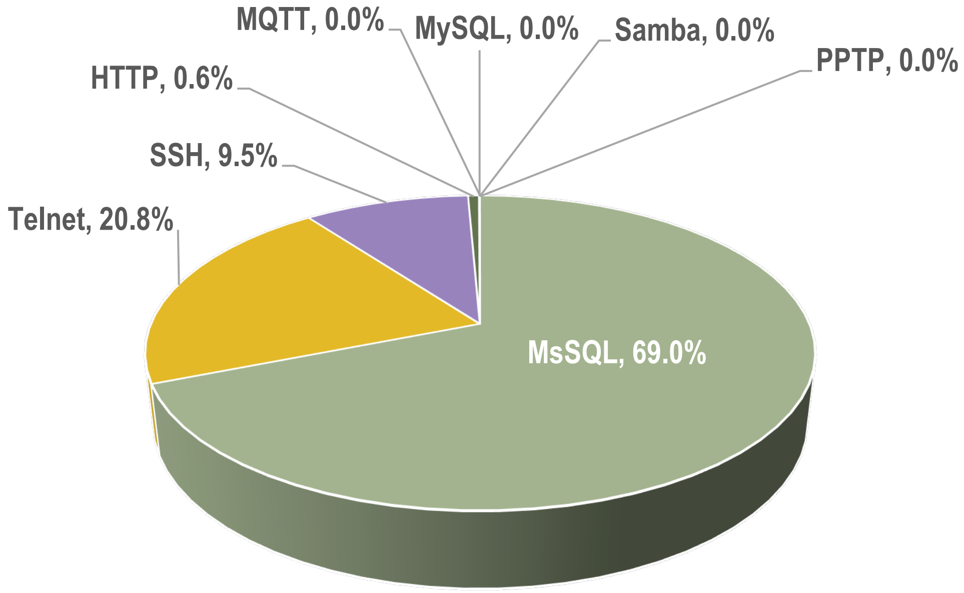

Figure 2 Targeted Services

In Figure 2, eight (8) targeted services data are recorded during in February 2020. From Table 2 on the right, MsSQL became the main target with 12,361,700 or 69.0% closely followed by Telnet (20.8%) and SSH (9.5%). MQTT is at bottom with only 2 attacks logged.

Table 2 Targeted Services

TARGETED SERVICES	TOTAL
MsSQL	12,361,700
Telnet	3,727,612
SSH	1,705,626
HTTP	112,418
MySQL	6,229
Samba	4,047
PPTP	11
MQTT	2

Top Malware Detected

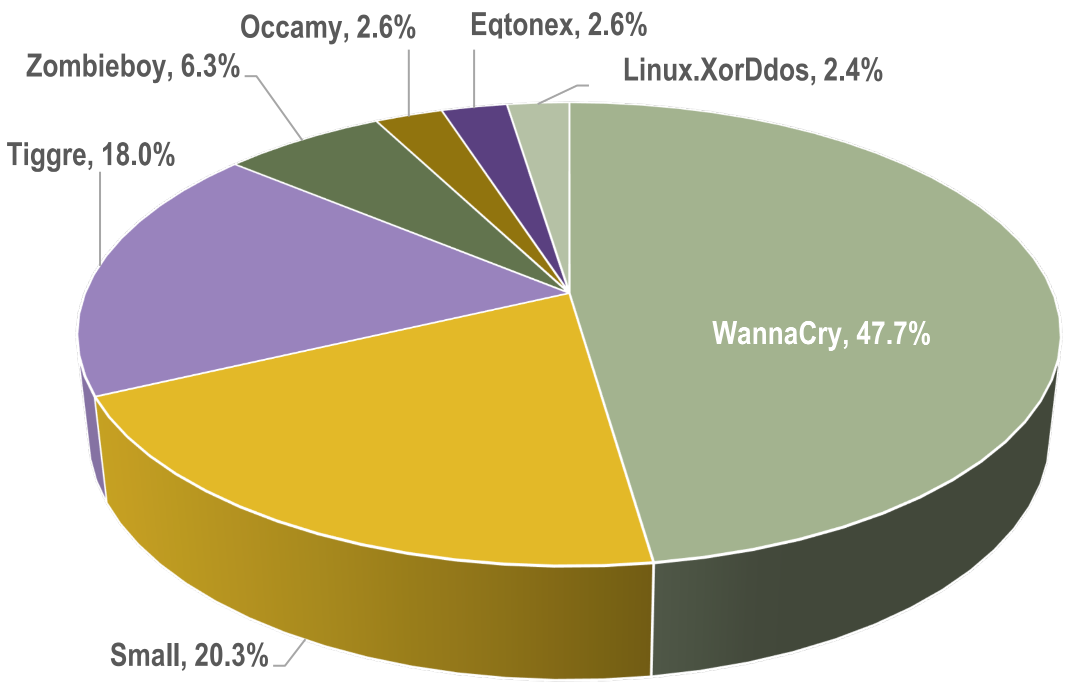

Figure 3 Detected Malwares

Table 3 Malwares Counts

MALWARE TYPE	MALWARE NAME	SEVERITY	EVENT COUNT
Ransomware	WannaCry	High	1732
Trojan Downloader	Small	High	736
	Occamy	High	96
	Eqtonex	High	93
	Linux.XorDdos	High	88
Cryptocurrency Mining	Tiggre	High	655
	Zombieboy	High	230

Table 3 shows the summary of malwares detected classified by the malware type. This report list the IP and Hash identified in the Project relating to the identified malwares for the information of the technical teams in mitigating such malwares. Ransomware has the highest detection with total of 1732 detections. The ransomware captured is WannaCry having a total of 334 unique hashes. This month, trojan downloader malware become second impact to the detection count with 1013 detections; Small (736 detections, 7 unique hashes), Occamy (96 detections, 5 unique hashes), Eqtonex (93 detections, 10 unique hashes) and Linux.XorDdos (88 detections, 11 unique hashes) . The lowest detection count is the cryptocurrency mining malware type with 885 detection count by the sensors; Tiggre (655 detections, 1 unique hash) and Zombieboy (230 detections, 6 unique hashes) . The list of malware hashes is shown in *Appendix 1 – List of MD5 Malware Hashes.*

a. WannaCry – Severity: High

WannaCry is a ransomware that contains a malicious worm component. It spreads by using Eternal Blue exploit in the Windows SMBv1 protocol which allows remote code execution if an attacker sends specially crafted messages [1]. It has the capability to remotely compromised systems, encrypt files and infect other hosts. However, any systems that have been patched using the MS17-010 security update are not vulnerable to the exploits used by this malware [2].

IP

1.0.194.56
1.1.236.203
1.2.178.197
1.6.120.155
1.22.152.42
1.22.158.46
1.47.171.121
1.52.96.181
1.53.3.93
1.53.8.40
1.53.170.4
1.55.48.126
1.55.94.43
1.55.142.199
1.55.142.228
1.161.102.229
1.165.0.209
1.169.24.223
1.170.71.37
1.175.1.123
1.175.130.149
1.179.192.69
1.179.234.215
1.192.32.46
2.50.15.138
2.61.122.31
2.61.191.158
2.75.107.240
2.133.129.254
2.134.171.86
2.136.46.104
2.183.156.174
2.185.215.33
2.187.248.252
2.228.39.100
2.228.162.254
5.35.53.198
5.56.133.161
5.59.147.116
5.101.20.78
5.107.221.139
5.113.205.137
5.142.160.79
5.160.175.202
5.190.57.21
5.200.87.60
5.204.83.62
5.210.215.66
5.232.6.141
12.176.40.155
12.226.240.170
14.0.19.6
14.0.19.160
14.98.44.182
14.98.66.130
14.98.72.30
14.98.215.26
14.98.233.18
14.139.62.117
14.139.122.139
14.142.118.68
14.143.53.14
14.143.207.214
14.143.251.38
14.160.23.226
14.160.184.194
14.161.29.150
14.162.6.45
14.162.18.180
14.162.34.254
14.162.121.31
14.162.144.140
14.162.165.173
14.162.216.81
14.162.217.150
14.163.14.210
14.163.91.115
14.163.249.116
14.164.230.171
14.166.115.109
14.167.140.184
14.169.64.222
14.170.155.23
14.171.30.79
14.171.114.20
14.171.163.5
14.171.219.204
14.174.79.54
14.174.193.174
14.175.8.84
14.175.62.111
14.175.154.89
14.176.124.254
14.176.151.226
14.177.97.124
14.177.145.136
14.181.21.78
14.181.52.176
14.181.86.152
14.182.92.179
14.183.169.46
14.184.44.148
14.184.108.212
14.185.99.51
14.186.84.88
14.186.235.103
14.187.35.189
14.187.171.58
14.188.42.1
14.188.50.27
14.188.242.49
14.190.144.169
14.190.152.179
14.190.233.142
14.207.198.34
14.226.54.35
14.226.86.178
14.227.32.71
14.228.34.89
14.228.40.79
14.228.146.139
14.228.253.202
14.231.17.146
14.231.47.144
14.231.121.4
14.231.140.44
14.231.188.196
14.231.210.102
14.231.246.94
14.232.161.132
14.233.82.158
14.233.145.61
14.234.17.85
14.234.56.239
14.234.221.198
14.235.14.177
14.235.29.135
14.235.136.39
14.235.251.227
14.236.150.50
14.238.2.178
14.238.14.50
14.241.67.247
14.241.67.250
14.241.75.55
14.242.147.165
14.242.170.233
14.244.56.192
14.244.74.252
14.245.45.169
14.245.64.111
14.246.105.226
14.247.40.117
14.247.59.59
14.247.96.255
14.248.23.128
14.248.77.83
14.248.141.187
14.250.233.8
14.251.168.87
14.251.217.4
14.251.246.188
14.252.114.118
14.252.125.101
14.252.251.92
14.254.46.161
14.255.107.177
27.2.128.27
27.2.193.26
27.2.209.78
27.3.8.28
27.64.52.104
27.66.192.29
27.66.202.243
27.67.32.222
27.69.203.11
27.72.21.140
27.72.31.43
27.72.72.48
27.72.91.118
27.72.95.32
27.72.100.83
27.72.104.173
27.72.145.222
27.72.149.230
27.73.211.82
27.74.58.125
27.74.133.142
27.74.244.66
27.74.254.101
27.76.68.15
27.100.42.3
27.106.44.142
27.111.38.166
27.116.17.114
27.123.2.18
27.123.249.110
27.123.251.69
27.123.251.74
27.123.251.116
31.13.63.222
31.145.150.194
31.154.74.226
31.176.159.110
31.193.125.236
36.37.94.197
36.37.126.98
36.65.100.84
36.65.120.73
36.65.137.222
36.65.234.7
36.67.6.71
36.67.214.90
36.68.5.115
36.68.104.136
36.68.187.39
36.68.237.148
36.69.138.209
36.69.197.47
36.69.217.83
36.69.240.90
36.71.153.40
36.71.233.67
36.71.234.165
36.71.235.108
36.71.239.44
36.71.239.238
36.72.2.210
36.72.28.42
36.72.43.19
36.72.218.188
36.72.220.229
36.73.34.103
36.75.33.206
36.75.140.236
36.75.141.0
36.75.141.36
36.75.141.242
36.75.142.33
36.75.203.10
36.75.219.45
36.76.244.127
36.80.119.230
36.82.6.176
36.82.43.139
36.82.96.143
36.82.189.26
36.84.10.150
36.84.244.2
36.85.219.142
36.89.207.250
36.89.229.183
36.90.2.134
36.90.40.196
36.90.80.180
36.90.99.95
36.91.37.13
36.91.42.35
36.92.26.162
36.92.118.169
36.224.244.170
36.225.71.72
36.225.132.57
36.231.72.147
36.232.22.173
36.235.130.31
37.54.246.42
37.57.91.206
37.79.9.81
37.122.3.125
37.131.224.158
37.147.217.167
37.182.196.137
37.193.149.35
37.208.97.231
38.99.5.194
41.0.69.212
41.33.69.243
41.33.129.154
41.33.211.194
41.34.228.188
41.39.225.68
41.44.169.145
41.76.172.20
41.86.237.83
41.90.122.21
41.191.227.142
41.201.8.10
41.206.15.18
41.212.122.153
41.242.18.1
42.112.108.13
42.112.234.223
42.113.84.37
42.113.84.113
42.113.112.13
42.113.247.255
42.114.39.179
42.114.202.106
42.114.206.35
42.115.207.129
42.118.38.137
42.118.114.5
42.119.200.216
42.245.203.130
43.225.23.18
43.228.130.66
43.230.196.66
43.230.196.71
43.231.254.220
43.240.6.234
43.240.102.18
43.240.103.180
43.242.210.138
43.254.220.180
45.64.122.66
45.112.127.155
45.114.79.152
45.126.146.162
45.249.79.10
45.252.245.245
46.41.82.178
46.42.27.83
46.48.216.190
46.72.187.110
46.100.53.152
47.206.62.218
49.34.117.38
49.36.52.64
49.36.140.205
49.37.14.88
49.49.233.24
49.144.204.117
49.145.197.13
49.145.201.57
49.145.203.183
49.145.229.249
49.145.236.189
49.146.32.249
49.146.37.98
49.146.39.154
49.146.54.2
49.149.64.207
49.149.66.146
49.149.74.20
49.149.77.84
49.149.104.21
49.149.108.236
49.149.109.79
49.151.25.39
49.205.166.166
49.206.11.143
49.206.208.121
49.206.213.169
49.207.71.111
49.207.76.71
49.207.132.225
49.207.144.231
49.230.68.0
49.231.13.190
49.231.145.167
49.231.222.4
49.231.222.9
49.248.3.10
51.39.204.227
58.69.150.148
58.91.105.74
58.186.105.95
58.187.66.20
59.46.65.246
59.55.98.64
59.90.156.203
59.91.78.83
59.91.186.42
59.96.168.5
59.97.100.244
59.99.202.139
59.120.197.109
59.125.207.109
60.172.4.133
60.172.42.175
60.251.51.100
61.0.123.109
61.0.137.134
61.2.64.80
61.7.147.137
61.8.71.20
61.12.89.234
61.16.130.22
61.47.81.74

a. WannaCry (cont’d)

IP

61.91.111.26
61.94.143.7
61.108.45.196
61.145.151.150
61.216.35.247
61.227.88.70
61.244.46.34
62.78.80.36
62.105.155.250
62.182.26.142
62.215.51.3
62.248.49.14
63.141.244.186
66.96.237.254
69.160.2.184
69.162.98.71
69.162.98.83
70.63.66.99
71.41.155.238
72.164.246.194
77.29.195.148
77.89.156.4
77.93.60.33
77.222.106.76
77.232.51.202
77.232.51.218
77.233.11.86
77.240.177.218
78.36.229.202
78.107.206.121
78.175.53.71
78.189.87.126
78.189.221.50
78.190.186.120
79.33.115.212
79.60.56.218
79.99.110.98
79.133.68.139
79.134.212.242
80.67.220.20
80.68.0.89
80.80.194.42
80.154.141.111
80.191.51.178
80.191.174.37
80.240.253.242
80.250.221.54
80.254.123.36
81.30.215.93
81.213.199.131
82.61.145.160
82.77.63.42
82.80.37.162
82.81.169.209
82.127.16.223
82.166.181.43
82.204.178.188
82.207.27.154
83.96.6.210
83.102.147.28
83.146.113.7
83.169.203.66
83.221.202.187
83.221.211.251
83.239.91.250
85.18.124.166
85.21.53.203
85.30.254.43
85.62.37.246
85.95.179.146
85.103.116.210
85.105.57.34
85.143.112.35
85.154.145.195
85.173.245.112
85.174.45.245
85.174.227.185
85.185.42.99
85.185.95.130
85.235.49.211
85.237.46.251
86.123.65.20
87.117.59.113
87.140.117.162
87.226.169.222
87.226.213.74
88.84.202.11
88.87.140.110
88.147.6.33
88.206.11.125
88.228.2.22
88.243.161.13
88.247.40.19
88.247.219.155
88.248.98.146
88.250.89.150
89.42.77.169
89.109.35.233
89.148.240.53
89.190.234.150
89.207.93.137
89.218.91.170
90.151.84.243
90.154.35.106
90.163.187.8
90.188.163.135
90.189.113.86
91.106.87.34
91.121.91.24
91.122.193.147
91.138.234.26
91.185.21.41
91.205.239.5
91.206.55.84
91.215.204.170
91.218.160.14
91.219.164.69
91.225.163.76
91.226.210.84
91.228.118.1
91.231.128.38
91.234.89.216
92.42.160.34
92.45.61.74
92.46.109.226
92.46.215.58
92.49.164.31
92.51.75.246
92.113.36.21
92.222.193.128
92.241.122.248
93.35.229.55
93.81.213.57
93.81.218.177
93.174.229.21
93.191.17.238
94.25.8.218
94.25.171.9
94.25.173.198
94.25.233.16
94.25.234.254
94.53.95.35
94.74.132.250
94.75.103.54
94.101.189.178
94.141.178.42
94.143.40.235
94.153.137.98
94.158.158.143
94.159.62.134
95.9.113.73
95.13.104.82
95.30.123.215
95.31.156.231
95.38.123.192
95.53.129.22
95.106.93.38
95.107.0.61
95.134.187.239
95.161.151.2
95.188.95.214
95.189.104.78
98.101.100.92
101.50.78.218
101.50.124.229
101.51.146.247
101.51.155.73
101.51.180.188
101.99.13.197
101.108.63.250
101.108.198.178
101.108.235.144
101.109.11.32
101.109.49.129
101.109.242.42
103.4.92.85
103.7.130.226
103.8.125.194
103.13.99.100
103.14.196.77
103.19.59.34
103.19.81.29
103.26.56.2
103.26.97.245
103.30.222.150
103.37.80.198
103.37.181.3
103.38.15.8
103.38.15.162
103.49.189.8
103.52.228.89
103.66.199.34
103.69.91.89
103.70.38.220
103.72.142.9
103.72.179.9
103.74.111.72
103.74.111.107
103.74.121.31
103.76.14.61
103.76.82.180
103.80.210.112
103.80.211.187
103.81.13.252
103.81.114.106
103.81.115.3
103.81.115.66
103.81.115.69
103.85.11.221
103.86.195.76
103.95.8.170
103.101.233.21
103.207.0.150
103.213.228.174
103.216.236.236
103.218.231.193
103.227.98.195
103.230.152.101
103.230.155.26
103.231.32.34
103.232.245.226
103.233.48.31
103.238.15.53
103.238.69.241
103.239.204.41
103.240.79.250
103.241.46.143
103.242.56.63
103.243.185.24
103.244.245.254
103.248.31.50
103.249.81.86
103.249.240.62
103.250.136.174
103.250.199.70
103.251.226.54
105.112.97.100
105.112.120.45
105.112.122.32
105.227.168.233
105.247.26.242
106.5.173.75
106.51.4.130
106.51.5.165
106.51.74.162
106.51.76.35
106.51.127.115
106.51.137.107
106.77.80.92
106.105.176.80
106.200.36.255
106.215.83.22
109.62.236.184
109.75.249.107
109.105.184.201
109.230.73.170
109.252.123.44
109.252.247.234
110.77.232.29
110.137.167.14
110.138.150.148
110.139.13.143
110.139.91.158
110.139.97.195
110.164.77.46
110.170.33.34
111.68.101.170
111.93.13.4
111.252.161.198
112.78.133.253
112.78.177.11
112.133.248.105
112.133.251.173
112.134.144.207
112.197.0.92
112.197.43.157
112.207.46.185
112.208.145.196
112.208.177.226
113.22.10.240
113.22.11.232
113.22.86.128
113.22.236.141
113.23.49.55
113.53.185.198
113.91.144.187
113.160.96.93
113.160.106.69
113.160.166.9
113.160.182.13
113.160.205.222
113.160.227.125
113.160.228.229
113.160.235.240
113.161.37.15
113.161.70.67
113.161.128.96
113.161.162.185
113.161.194.18
113.161.198.16
113.162.19.120
113.162.32.44
113.162.55.179
113.162.162.78
113.167.45.240
113.168.72.154
113.168.220.220
113.168.255.67
113.174.178.136
113.176.7.142
113.176.25.127
113.176.43.150
113.176.84.232
113.179.21.115
113.182.4.164
113.183.43.28
113.183.206.237
113.184.48.133
113.184.78.230
113.184.139.76
113.185.79.54
113.190.103.109
113.190.109.91
113.190.141.199
113.190.149.132
113.190.193.151
113.190.231.244
113.190.253.76
114.7.120.94
114.7.146.131
114.29.236.125
114.36.249.17
114.41.8.218
114.47.26.161
114.79.152.106
115.42.211.146
115.72.210.26
115.74.210.81
115.78.8.188
115.78.15.25
115.78.230.159
115.79.47.123
115.79.75.242
115.79.141.10
115.79.201.196
115.84.72.214
115.84.105.110
115.84.253.226
115.127.5.9
115.150.175.219
115.165.200.165
115.171.222.198
115.186.149.66
116.9.122.44
116.12.200.194
116.58.227.77
116.96.177.227
116.97.45.90
116.97.212.42
116.97.243.142
116.98.37.192
116.101.122.205
116.103.209.28
116.104.182.211
116.105.227.93
116.111.92.112
117.1.118.250
117.1.242.138
117.2.123.165
117.2.147.236
117.2.167.233
117.4.1.39
117.4.32.63
117.4.115.62
117.4.120.126
117.6.87.232
117.6.131.81
117.6.160.117
117.7.108.123
117.7.214.95
117.55.242.131
117.58.241.233
117.58.243.242
117.97.132.31
117.201.15.148
117.203.220.181
117.207.208.53
117.211.167.49
117.215.213.208
117.216.142.114
117.221.69.34
117.232.78.209
117.247.71.240
117.247.83.240
117.247.119.73
117.247.137.73
117.247.177.16
117.247.191.92
117.247.232.146
117.247.233.115
117.254.141.8
118.68.71.145
118.69.35.240
118.69.36.26
118.69.62.81
118.69.66.174
118.69.67.248
118.69.68.155
118.70.8.46
118.70.12.171
118.70.20.148
118.70.42.107
118.70.67.172
118.70.80.170
118.70.91.40
118.70.124.109
118.70.125.91
118.70.131.201
118.70.182.219
118.70.187.84
118.71.96.128
118.71.128.5
118.71.152.247
118.71.153.133
118.71.153.205
118.96.43.239
118.96.203.60
118.96.236.55
118.97.98.204
118.97.115.66
118.97.166.154
118.160.6.66
118.167.194.122
118.168.106.96
118.169.184.181
118.173.104.142
118.173.126.64
118.173.179.213
118.173.181.164
118.173.202.167
118.174.15.242
118.174.183.124
119.93.131.171
119.95.74.53
119.160.216.227
119.235.52.220
120.28.192.151
120.29.78.126
120.77.242.199
120.188.37.171
121.15.0.221
121.34.49.169
121.78.147.220
121.122.95.186
121.201.67.128
121.244.153.82
122.53.183.69
122.54.134.242
122.55.63.133
122.100.153.46
122.117.10.66
122.154.18.2
122.154.33.214
122.154.139.129
122.160.84.31
122.162.185.100
122.162.199.21
122.170.99.171

a. WannaCry (cont'd)

IP

122.176.25.87
122.176.122.8
122.225.48.252
122.225.74.118
122.227.16.242
122.248.108.32
123.16.13.148
123.16.15.45
123.16.79.36
123.16.131.90
123.16.252.50
123.17.123.248
123.18.38.7
123.18.206.22
123.19.35.196
123.19.74.143
123.19.186.121
123.19.212.70
123.19.243.124
123.20.21.221
123.20.33.23
123.20.161.29
123.21.16.163
123.22.148.35
123.24.89.216
123.24.224.58
123.24.243.131
123.25.85.103
123.25.116.123
123.25.241.81
123.26.56.253
123.26.171.189
123.176.34.155
123.231.122.37
124.105.87.101
124.109.56.87

124.123.79.235
125.17.139.220
125.19.48.66
125.24.48.146
125.24.144.59
125.24.171.24
125.24.172.228
125.25.54.64
125.72.101.58
125.160.13.6
125.160.114.12
125.160.114.62
125.161.105.221
125.161.107.75
125.161.129.6
125.161.131.179
125.161.137.183
125.162.46.249
125.162.90.43
125.162.179.158
125.162.209.172
125.162.241.130
125.162.253.253
125.163.20.157
125.163.58.70
125.163.238.209
125.165.46.235
125.165.114.73
125.165.193.197
125.165.234.204
125.209.71.250
125.213.136.210
125.214.49.110
125.214.59.128
125.224.73.28
125.230.8.24

128.68.225.206
128.69.66.218
128.74.216.211
131.72.222.165
131.107.147.197
131.107.159.183
131.107.159.199
131.161.3.194
131.228.32.67
131.228.56.116
131.228.56.122
131.228.56.123
132.157.66.83
134.204.119.62
134.236.3.255
136.232.8.106
136.232.176.66
137.175.30.127
138.185.96.16
138.186.225.4
139.5.159.167
139.60.187.102
139.255.26.242
139.255.37.250
139.255.49.18
139.255.74.106
140.213.2.129
140.213.47.160
143.202.252.124
144.2.246.194
148.243.54.129
150.107.5.211
150.129.131.178
151.22.13.44
154.65.34.39
154.121.51.165

154.197.17.170
154.236.162.171
156.19.42.139
156.204.143.233
156.222.235.114
156.223.225.14
157.39.193.81
157.39.218.164
157.48.71.166
157.51.181.12
158.140.185.63
158.181.184.215
159.192.73.136
159.192.98.149
159.192.99.86
159.192.133.210
159.192.136.25
159.192.180.239
159.192.227.201
161.246.145.39
162.216.143.136
164.77.201.218
165.225.106.61
165.225.106.206
167.60.100.33
167.249.51.1
167.250.30.58
167.250.232.9
168.90.91.171
168.121.137.189
168.187.19.26
168.195.98.250
168.228.103.255
169.255.74.10
170.80.71.114
170.233.34.73

170.238.254.254
171.4.30.225
171.4.216.44
171.4.228.143
171.4.232.240
171.4.236.74
171.5.246.176
171.6.247.183
171.7.247.127
171.224.110.100
171.224.177.156
171.224.178.175
171.224.178.249
171.224.180.139
171.224.181.55
171.224.181.205
171.224.181.253
171.227.205.253
171.229.152.59
171.229.217.137
171.231.34.154
171.231.95.235
171.231.218.35
171.234.239.82
171.237.77.75
171.237.130.116
171.241.100.176
171.243.151.20
171.243.181.206
171.244.185.75
171.246.190.155
171.246.243.71
171.249.60.163
171.250.21.230
171.251.194.61
171.251.238.115

171.252.210.194
171.255.67.216
173.95.33.171
174.108.180.250
175.29.177.38
175.176.186.154
176.32.185.242
176.50.118.234
176.59.32.29
176.59.137.80
176.109.76.37
176.110.126.140
176.110.246.54
176.114.188.168
176.115.196.74
176.118.52.158
176.236.77.187
177.10.193.106
177.23.63.35
177.38.140.93
177.38.243.154
177.42.37.44
177.45.0.211
177.46.129.21
177.52.19.205
177.76.229.172
177.92.3.130
177.92.5.130
177.92.22.10
177.92.43.193
177.93.243.20
177.94.208.54
177.101.162.221
177.107.192.6
177.136.103.172
177.149.159.92

177.152.132.206
177.154.75.7
177.159.98.42
177.185.94.3
177.191.98.167
177.206.231.2
177.220.128.114
178.17.176.61
178.22.199.221
178.34.154.51
178.44.251.158
178.141.205.238
178.150.12.53
178.150.173.68
178.158.11.18
178.173.144.69
178.176.171.181
178.176.173.6
178.185.14.195
178.188.179.58
178.207.15.78
178.208.158.230
178.214.255.32
178.214.255.186
178.238.17.26
178.238.17.69
179.6.201.243
179.127.65.233
179.183.237.50
179.190.116.58
179.228.4.172
179.236.176.173
179.252.115.38
179.255.9.254
180.129.68.39
180.183.28.71

180.183.62.67
180.183.192.132
180.183.193.195
180.183.231.132
180.183.235.120
180.183.245.217
180.190.179.114
180.211.159.90
180.217.167.18
180.232.102.226
180.241.7.234
180.242.154.99
180.243.248.181
180.244.21.154
180.244.191.0
180.244.233.238
180.244.244.52
180.245.253.63
180.246.90.251
180.246.148.238
180.246.240.62
180.248.95.91
180.248.121.233
180.248.123.199
180.249.116.156
180.249.200.18
180.250.102.226
180.250.187.115
180.251.193.185
180.254.140.243
181.39.51.18
181.41.102.196
181.48.13.10
181.48.247.222
181.57.205.82
181.112.155.196

181.114.110.5
181.129.177.226
181.143.11.98
181.143.170.108
181.192.204.64
181.224.228.114
182.16.168.67
182.23.82.202
182.30.17.66
182.50.112.72
182.52.30.75
182.52.104.95
182.52.215.140
182.53.52.47
182.53.149.15
182.53.192.47
182.53.196.73
182.53.207.45
182.56.160.216
182.56.236.65
182.61.165.204
182.71.173.126
182.72.89.142
182.72.122.122
182.73.121.90
182.73.180.5
182.74.3.190
182.74.43.212
182.75.24.234
182.75.226.250
182.76.26.90
182.76.171.10
182.77.125.59
182.105.247.194
182.107.185.97
182.111.53.148

182.156.249.250
182.160.2.209
182.160.117.170
182.186.89.244
182.253.11.234
182.253.62.122
182.253.75.241
182.253.174.108
182.253.251.212
183.62.57.249
183.80.93.144
183.80.220.7
183.80.236.195
183.81.4.181
183.81.97.37
183.81.121.68
183.82.2.131
183.82.5.68
183.82.17.10
183.82.97.122
183.82.108.131
183.82.108.157
183.82.114.28
183.82.116.79
183.82.120.66
183.82.120.188
183.82.124.145
183.83.36.107
183.83.71.176
183.83.75.95
183.83.89.115
183.83.129.42
183.83.164.45
183.83.236.206
183.87.61.226
183.87.154.5

183.88.44.76
183.88.121.209
183.88.237.225
183.89.72.148
183.89.76.196
183.91.4.116
184.22.78.119
184.22.162.45
184.82.26.170
184.82.26.235
185.15.62.32
185.19.78.18
185.39.206.2
185.41.20.130
185.44.230.23
185.70.130.156
185.97.93.13
185.97.93.14
185.98.225.217
185.107.253.80
185.120.249.203
185.148.84.131
186.37.82.180
186.88.131.75
186.88.228.195
186.89.123.75
186.92.128.83
186.93.54.212
186.93.131.247
186.96.72.218
186.96.109.146
186.117.128.82
186.149.238.12
186.154.234.165
186.177.31.62
186.178.10.91

186.200.33.2
186.208.221.5
186.213.21.181
186.216.192.154
186.226.71.179
186.238.15.218
186.248.68.8
186.251.18.154
187.16.4.216
187.16.108.34
187.17.145.231
187.28.155.214
187.29.170.218
187.33.69.226
187.33.235.74
187.35.182.34
187.49.85.62
187.49.85.90
187.75.227.199
187.84.95.166
187.86.132.227
187.86.218.0
187.92.246.98
187.95.114.77
187.95.114.113
187.95.123.82
187.114.10.27
187.120.3.10
187.135.75.8
187.188.161.124
187.189.87.222
187.189.243.225
187.189.247.188
187.218.54.228
187.237.123.210
187.250.31.125

188.0.134.154
188.50.244.65
188.138.251.61
188.163.12.139
188.163.41.31
188.170.53.74
188.170.78.163
188.170.189.28
188.170.196.3
188.246.185.130
189.1.163.70
189.1.166.66
189.15.70.167
189.26.101.204
189.47.168.151
189.47.215.72
189.69.26.130
189.78.150.208
189.84.169.245
189.87.130.202
189.109.203.222
189.113.72.100
189.126.193.82
189.145.132.77
189.176.133.171
189.203.131.87
189.204.192.113
189.210.93.229
189.211.188.47
189.224.143.52
189.234.70.33
189.254.96.50
189.254.171.158
190.0.40.22
190.7.215.5
190.14.247.226

a. WannaCry (cont'd)

IP

190.24.8.82
190.37.101.123
190.38.206.145
190.60.91.212
190.72.188.37
190.82.94.205
190.86.203.10
190.93.197.249
190.94.247.75
190.129.12.139
190.129.15.224
190.129.95.194
190.145.177.2
190.148.157.31
190.153.50.162
190.184.203.162
190.186.21.185
190.186.158.114
190.187.67.2
190.187.87.162
190.187.120.210
190.196.71.2
190.196.147.180
190.196.182.149
190.204.156.55
190.207.106.195
190.212.7.104
190.215.57.118
190.217.31.4
190.237.41.211
190.242.60.208
190.248.17.182
191.30.137.101
191.54.103.195
191.55.188.166
191.98.73.25
191.209.88.13
191.240.157.93
191.241.242.92
191.242.190.40
191.249.54.34
191.249.180.176
191.254.115.51
192.41.24.33
192.82.65.72
192.99.4.62
192.162.112.139
192.243.220.101
193.31.205.209
193.108.216.91
193.151.24.138
193.169.4.21
193.194.79.229
193.200.33.251
193.227.16.25
194.78.58.50
194.135.123.66
194.135.209.146
194.209.157.121
195.9.91.250
195.9.117.30
195.25.27.104
195.58.61.27
195.87.86.170
195.96.87.210
195.161.162.254
195.175.84.174
195.206.55.154
195.230.151.230
195.239.225.98
196.25.35.242
196.30.113.194
196.34.35.90
196.41.72.1
196.41.72.3
196.41.72.5
196.184.62.66
196.188.1.41
196.188.65.156
196.189.45.32
196.189.185.241
196.189.185.248
196.204.195.56
196.221.202.68
196.221.228.27
197.37.88.39
197.44.142.131
197.51.60.81
197.135.34.216
197.156.73.170
197.156.93.28
197.210.28.132
197.210.47.122
197.210.226.116
197.230.42.158
197.232.26.137
197.248.50.18
200.12.130.151
200.27.145.196
200.32.10.210
200.37.200.157
200.37.232.129
200.42.20.164
200.44.228.141
200.48.158.74
200.56.125.90
200.58.76.85
200.84.188.31
200.85.80.95
200.105.245.122
200.107.136.193
200.109.199.61
200.132.7.10
200.142.108.110
200.150.87.60
200.150.124.226
200.160.116.25
200.178.114.203
200.181.30.58
200.185.17.254
200.185.51.133
200.187.173.40
200.195.8.18
200.195.147.202
200.195.171.125
200.225.212.1
200.231.37.70
200.250.55.145
200.252.105.194
201.31.190.66
201.55.53.77
201.64.22.66
201.64.81.158
201.111.87.102
201.130.203.130
201.131.97.7
201.140.123.178
201.140.236.236
201.144.64.70
201.144.200.38
201.163.149.123
201.163.176.4
201.174.12.195
201.209.181.167
201.217.212.98
201.218.223.234
201.236.149.102
201.247.149.53
201.248.7.78
201.249.163.106
202.9.40.92
202.28.63.66
202.28.64.247
202.28.64.248
202.51.117.211
202.53.90.227
202.53.94.108
202.62.65.140
202.62.72.98
202.62.84.213
202.62.86.50
202.71.25.158
202.79.36.151
202.83.28.134
202.90.136.10
202.91.71.18
202.129.39.206
202.129.211.52
202.131.108.4
202.138.244.99
202.152.33.66
202.163.104.237
202.165.46.2
202.166.205.141
203.63.46.142
203.78.114.100
203.81.71.101
203.88.147.244
203.90.82.34
203.94.92.29
203.101.174.14
203.130.242.210
203.150.151.185
203.154.65.167
203.177.60.237
203.177.251.222
203.210.84.117
206.180.107.22
208.122.73.127
209.45.67.228
209.91.204.142
209.141.6.210
210.206.53.82
210.212.213.50
211.75.220.225
211.181.237.97
211.205.95.37
212.12.19.188
212.35.105.96
212.55.98.30
212.98.186.249
212.156.51.134
212.156.147.42
212.171.12.182
212.178.129.115
212.253.93.10
213.27.227.26
213.55.96.14
213.154.15.66
213.171.43.155
216.75.225.203
216.161.207.176
217.15.150.213
217.22.171.251
217.23.37.83
217.76.194.70
217.86.235.141
217.169.208.70
217.219.163.77
218.88.187.70
218.161.75.235
219.85.158.95
220.129.116.211
220.191.239.6
220.225.164.134
222.124.196.205
222.212.88.75
222.212.135.248
222.252.20.83
222.252.30.30
222.252.30.190
222.252.95.126
222.254.82.56
223.30.41.146
223.204.225.120
223.205.75.132
223.205.244.175
223.206.208.194
223.206.246.151
223.229.150.40
223.237.52.23

Hash

ae12bb54af31227017feffd9598a6f5e
996c2b2ca30180129c69352a3a3515e4
414a3594e4a822cfb97a4326e185f620
0ab2aeda90221832167e5127332dd702
a55b9addb2447db1882a3ae995a70151
cd99e5e4f44621978faf8df0e01d2d2b
cf4f46336abeec03630297f846d17482
e9d1ba0ee54fcdf37cf458cd3209c9f3
6e72ad805b4322612b9c9c7673a45635
a4d49eaf60a8e333708469606ad9e1a4
ef894d1c6dd120fad5a885bc737d6338
a48ca7b40ab2a6ebdd94dbd52164c6cf
9ba5379aa41d707a4331d27a004baec1
8e6bfea06cb00553ee29b3822b349bd6
bdcaf7ef34cd9b02932e5ee2297e4893
6633a19602561d359e76a67a008d62e8
33d373e264dc7fdb0bcdbd8e075a6319
879d69d4c18d6947f9ea5e545ac16d01
aa718a028875637e1c6eb648706340b6
fcdecb1304a1fc6d574e8337eaf4cdaf
62186bebffffcfafb1c70a8ff03fa317
3553aeb71299e94c2549f1b34f6c1a43
095d83ee1494554d00b726cfddee494c
2de98404eb4ac4a525ed1884f4ea445b
7c7262d9e49a40a52d0040942810456c
a2151cd48a3186290411217caf1016df
ab5b987b02bed407d4833ba83a0878b8
8bd8a9c3871c32f8dfbac7711a75dc52
8fa0e5dd92185799b73cbfab3da3e919
c16edec919fc35cb39097f84f1b87455
e49594ffa18e330c8692d88dc8e73752
e5840a9753ed8f90fbd7264c8db27c4b
8b7137adb7aac5cbf55b039babb612bc
5d19193a153ab77f7d3a5807fbf03767
50b93e08b91de26b5487abe79afe1d4a
59b5090fad3d62f05572470f0c79c9a4
2f76b88b420003516f90062940ef7881
0ab9a60a55cb40fc338e8f4988feee2f
30e3f8ebb578da4247b6bf7e43beda36
4f53357da304a79b6cb55fd8de9a094c
54dd9593fb858bb8b1a77fe5e9238ae2
5ffdc8b7825f72a04d5c97b6a4d80e7e
d58fef5143d515816faeeeacc1627286
d3891f56ad175f9af1d21f3072f73ccb
daf7e72c18545d74aa1cdcdd6b306dc7
c475b82f1e0b421e051622f034b1d5e3
c0d149a7828c3ad6046da2d897bcff0c
c5ff03fe7bb4384a1814c3fe7fe84119
caf082a135af8d966e8dc7fb9f619bba
8da3345636b0f9b8c0acc811f5a26c61
aa7d98d151002e997fdbf6f2dbe7b8ba
a135677250b0007496c39cb5c876954d
a1fb001af7f76d36d0ee85b3c6453ca7
af76bbae1d51d04f1113bc225f979820
8d340ce819b42f0c5a27753dd7170ff9
951b218fab52434aa7d4624c03dd3415
95ff0a735ffc1b048110d8d21924da66
98df58e71b5202e49ba6f9e6e43ef6ef
c024bd7b3e360bed37d815bdf106acdb
da5eee93accd46fe8755b93a19ada407
ed03cfcc81546aee052e5d3360abda8d
6313dc47b8f44c9a808c0577ca7f4fcc
6e1dfefa794474d92b9e4412aea69f77
890d5aa0d18a6fca571cf710269c714c
6567e663303386b7152d5fcab1f06cac
729a5152f496cd96b653cca40a14eba4
78eae7fce7c9388446dc27ff213fe28b
398c9ce412840482219a86730d9853f1
3c63f9be8f7752de7f002ed0c3bdfddf
44bc540ed22c83517ff5068ba58da383

a. WannaCry (cont’d)

Hash

```
033f9150e241e7accecb60d849481871
0064e2641d419d2c68f9beb18246a297
2b4d3c993bc777de8d10ac080e3e5c00
2c003aef97036420170c481b10fc8da5
1a8996bae6e4cde7e6e8322e787506d1
f14afcac1094f1a6dfd84da5162a55c7
f9ca5dc4c240d66aaf08b2853d1535ba
fb1d03437dea96371c7c7d91e234c4d0
fc1e617b1ff659f1826868baedc9c258
fcb6b0f95853dfda72d5535a424b3a29
2118ffc9aa1c4f3f2c209293d0b12c42
2259ebf3658c2dd6ab1e53e3c23fad4d
22bc832a16559912d53fbe83cab1a17b
2ce0cc8415ef608a6c97e7848e29ba8e
1844584ed70abd0c48cf3c4d68e9e15f
2f92bf0bb72ed014b515e338c5bf0d59
017f63d0be693e53bc5b8edd426cfbd1
01d87121a4a589930d580a88e4df3640
4c8168df8d268aa5b6d1b02145b20379
3695f6d3175e85e25ea3cc65ab3801cf
5265fc3146b7e3922c79ef463aaecd16
6a139899acde9af3c79c024bee1a800b
6b0ac3a36170aa066c86caec90aea67b
7823636f9ce01306178c1ee7772ad831
63c573c0e2eb59009ef97da2ecf73f0e
4fbfa754204df11c5d7d4d76bb4b777f
5a579e20d6fe26579648c3961ef179ca
5a9e809ef287470a50cef41df8897b62
ec53e27425a44def7eb3f950ed0cb6d0
ed979ce49b3373765a91b15c1c37c00b
e66a0f43a8a5220d362645a13569ebca
e6a999cd5df18b0962b89e1a9c1ebfaf
e14e4f339bb5dc690862e91cc6341137
d5cf687cd06c000d9421413c18972c75
dfac55e674f9d62589cd531ffe25fcac
dce06798d1f588e14a50dd741ff7e8c1
c2b8b099bb55f52e094d22266b6d7b34
cc435ef3d7e00bcb2720743f17705323
c96b8c08aa8c7177a82b22d898eb1d79
d31d25eedd79f744b8a3d58888fd668b
ce223b231f2862124386c585e9b95ca1
cebb64bfd042804239424fed482aa986
951806fed26ede01685f03413607fe18
978fcc48a006c05c94e626ccb2ddfe53
9792cbeaa00a9e7f3a58b5827441e71d
98abe26199f28ab4e2b42e85f975b9e4
997e58102bf42ef2aade109867968160
99cd95db92c4e4cb4b882eb034e75cab
843ae62b27d29e88a4a5389dbf501ddd
b294e857dbc07134be8c0624b94e6b69
b794a273d022fc0c10d783afd6e1493b
9df37b7f669ad8290c382975e961b600
9ecca08445521f486fe9bff458817b2f
9f0f848cc5f6daecccddf8ca0bed1f10
9f61d37c99f647a1b0b3d0a431e4db24
9fe0b783f824bdac40dc63586086224e
a1192132123bfd5c9f3b916ee332fe8f
9e1b0a51e149acfa5937bf52bd9e3b9e
a143dc870869cc275ef35dbf733e046d
a3115fd8e1717b46a08dd2100b625e6d
a5e5710ba3eb92ff1010bba4642517a7
a725bf924d21fc981dd173fa66bca35f
a73c89e52851553a63963fd0f790c789
a821b8ced79eeff440a64b3d87e984c6
a917c331735c46c1aec3e23fba88e7a0
b7c30ca8a05951ed1c76ae4a62749f6a
b9de290ef3ec191950f0550cf6d14a6f
bb1cf62b506c0848a878a1526efa1357
bc4756aae7540d6073d9f440da474481
bd675a31ff5ea593c51e9bad87917784
b37d1c7a3260e50826b3cbd6ceb203e2
b46b61f29402626a483f28f99644b8b7
b6d1f1d400b26f78039216850f50dc88
b72ba971ee250f3f493008a638040fad
b016a2d5e8963fb6bb1f810502e1562f
b075ffe9788c0befe9ba892d0844bfd0
b0a5f29fc283d06db2109d62bd0aa9df
b153ea5ba3e0e4e285e2394be2af3784
aa884946d64a8967cdc994872990a299
abf42da16e0971ff966687c6e7d21987
ad7134b925745229f56b8fbff4a4e84c
8c74951768866866ed126be277e09d87
8ce48814e2d2289caa614f87856cb5f1
8e6635b3dcb090c8478fc392ca94722e
8e909510d1a1ac5ace42ed5e1afaea33
8f6a66a53beb129cd07a8520e1326041
967d46d8baa5152f7f366571b39225dd
96b11451d63b36111ba78a37532e97f3
901decc503049bc0108dc9cd5eb94ffc
9155183e0b2031ba0c7159f76840ffed
94b1b4ca313dc3ae348fa5a79b36ad34
9a142dcdc57eac7225800aa114f1fdb5
9a1768e5531d0852278b95e4d0137977
9aa3637857d84aa040c097ba0be6b900
9aa42e3fba9d860fd23c3dc54cf65d0b
9aae6412b2dfc9ed503e6c7123e95579
9b26bb265141692a7b81cef74fa9bf8a
9baf8ffbe84fdb05ad355f75d4ac73e4
9cabb6302630ba5b43b166575f157db4
9cc600b0c21a0ee60257aa9d5aaf0b44
ceeea870bf5ecffb612cc284e14ffb2b
d251dc6ccf4c3a88b7c6a97abb64e2a5
cab74b35aa582da53c621a442ec5ee33
cacbe198c83c1e1420c2f0bde401585d
c688aaf68c68b2570d10258d7e435de4
c69d230d92302dafb9f6f3a93113ec0e
c71854ceb8c814bd85c0663c72c1a5a5
c72e5e053e21231065d266fd3eaa708a
c75e04ce201b41356cb3befe228a23df
c881745e136cd982aee1cb9edffb0020
c2c4612c2138df47a52a526fbae3ab92
c3d8b9d5bb048eebca994cdce641f885
c04e6ce0dafa8fd0c005f90f997083d1
c4fca61333b642e21c2b1ba417c0100d
c0f043df3a5f47dc6bde71922417df86
c1045e165824a769408792e176290035
c14432e2751479323db1fe1f185e5c6c
be6da1c267fc762b8e26a57e3026abef
be9bdee97e6142aeb032bda086b983f7
bf137d87e79f68177dd1eb0b780a35e4
bff0aa6595e3fc250a32ada5ca1c0cfe
bff63cefd43b6a881ffc1e61dd0215ac
de5d77be7e096b08f8eb25cabe59d16c
de5e5585f3e65d16cc19af7b2daf3090
dee385512069d92fa4f4c84eed132415
e07b1006b251db11368b60f57e13cb0e
e12d0c0ba668e1592c5de9390f3005dc
dbd4a6eb6f597b3f53e66e5284d05e23
d8730841f4ace471fdd23544cc27b1d5
d8eedc656348729aea8571c5640d9b87
da2506e63930938a41ad2bf44d59697b
dab719e743b33b9b4f47a49a6a21d966
d52f3678521d2330610811723f1c2891
d540f05b1d45787a0bf809f115855134
e2f6cd5e295645e69b6f1e5e0fc56964
e4cc9844574dec633d8adc474215159c
e5551e9a1ef43d37bfe254e39afeab4a
e6cc34d3d80b6941ac7fbd8bbb1ddbc5
ef308fb6f974a766ab59bb68b1864aa1
f0b0714d21283cbb8429edae07962291
f0e4df1d50065af086a85c17103c57f1
ed39402aa43bebf9dc6839dcb9cecf03
5ab41fee92e06daffa1276902b90f7c2
51724a2aa578961ed6784b711c164b58
51f74846b7f7ea38ea74758c2cdf5adf
552e88c8f7678d685b0498dd6c50245d
56319a9877f62b75bafe89300d324090
56fd3342b2996306982bcbb578115e33
5778216a90f804958862d66af3ceeb87
5818d137c6c7324aa05a01c8c3cfe9d9
58686fd92b0cf4183e84c2017b37d46e
58a20a3827a0e27c337fce30efacce7b
6442441eb52236bbf78d67820f833fe9
654ae4e4c97fb243a71a15532e3287f0
6350f8da991da9ee85c63e15cce88fbb
675ca172a6c351db3f43d328c7347097
678323b12f8ae74c7bf406efced5f476
68e889e597051dc2bba55f53c69d5c73
61371b4c0b9e0250d5b3273f58780df4
614cbd6036e337f710caa34c66ba5a69
6207b75cae51b6f73891a014863845b4
5dbb17f0ac41162154e1690d25483e68
5eca730845d10f71d767d5a3f3119b15
6293f4978ec83cf7c6ad8f9baef25743
62af43d2b728f200f8d576f095fc85cd
8b9d53fad84c0d7972484bbd8f258127
89e18532ea2245deb8af6585708e7d74
8a4f6a3629fe6ad3ae8b0e7101d252d8
8af6e4ce4bffac0b4807851250709943
8b31308f2bf97e940dab49334d2d2011
7cf21cdad3e9afe55c93277c8a6bdf05
7dccf1d3a50c9d76557d0fbb68cdfc22
7f6c952f2cdd24fe828f30f0d2433d72
7f7fc6a29e4b39b530e6ace0ae8d7bdc
804748534449ce9b2b081831567b806f
809456dd1cbe82ab1a13473bfb638ba4
8110273cddd766bda4aab40e443427e0
827e7a475c522b2c6d81fa99154dcb8f
8337e6b54b5a982f20228ed33adefa9f
83544683ea936a82697a465bdf6093e1
```

a. WannaCry (cont’d)

Hash

837b7a7a2f4b984cfda9a83199f767b0
83a1896164025997d76a7dd94393db3e
6b17566ae9ed0fae76f1fd0b9a9029ef
6b5a9da099c8dd5b63a63c01c0256210
6cb21deaca071ac4d8c3a6f9cdc17f58
711a166b88ac297cc530b8140119841d
791af1c17458398c52f4aa53770dea37
79762e653db25e4af8d1233059005745
79e1e07fce2b0436cfb643ee8465dbbe
7a60943b74e7d36a2b1b922f07432a83
733c67a5a392b66b8b8259169ef240f7
74b16d9cf7d09b4878401401a481223b
75c75db2124405f06a8351465d7892c3
76b47e0829177757b39cf3c3672049dd
36d7c42d5490b82267a617b1d6bd5c96
36e5f7f493f155a87baedf34c2705b6a
372a3f6e2b9752a2035c673b6dd7fe32
37984af86c5d8c00c8456c1292771c72
37a3ca268f5d7379fcb5268296336771
38ab7916fc2ba54ec6ade58a137556b2
3116ac3731d2d5688452074d7fb5a6c9
3151485a025cb17bc3732533209a9f79
345ea68ae2052193e6a5c34806801550
347cc5676fceecc0598a4d62c2c36b7e
3ce7baba17fcf32f7310e9ab435b9511
3d71c399da5b2f7bd4208c740231979a
3e1f1ab7eb22b54d451f764377d869ab
3e655040fe787d7ec833fa019fc3a5a6
3f3d6691012cff45f5fbf67a0c65a6fb
3b34cfe3ec07b73d508edda28e3ffffe
3be07dbcc9dcf772a64bebf30bc8d1c0
3c3591eb1df1f5f60cc846685303fb58
4dcb93a3f82760112c1ac9cebc3f44ff
358ebe06d58df0203a6067d0575e9d7e
42708471bba43fab8c0834de27a7a3a4
429e6c88db4d5fc81669f5987abf110d
42cc3dc485724f134451fb157eb77213
430599e85618bd750b5bbfb21cb5f857
4306b68e3ca2d7ed71364acb8a6939c3
44ade454a487822f1c9d75aa7d8df907
4535d83ee1b6cc87b19eb788f0961422
45735a816370f26b06e053656ca7315d
46590d5fc431f79c2abfc7783c21f409
47bc7c8f1ac38746f74e543a4c421d75
499482e2c2069f814dc9e1e9a16952d5
49e38bc384b99902d6dca4754c63edee
4a4de629b32cfbe6b19f12bddc3ebef3
4adc61cc12645a3318edbcfee460a3e5
4b2d8f066eb5a0438f855201d1a1b3b9
4bb7874325d95b3f1fcb57ac10bdba45
4c50e407de345c5544d27fa28315519a
00c9e54f5c2c31cf4bc2bb0a178712ec
081967adb6eaab608a891f96f520d5e3
08bcd0b071a5ea741d60269654223c37
09900abd691ab580d9ddf0b20c8671ce
0a3a089906fcbd25904c8c8d7464ffda
0b57fe54929b51600497598c03408806
0c8caa346454bb05990d4fe63465da26
1367ff38c61bd7deff3837c4f24ca4ef
15a0cf8350ef9bd4222d203dbe437977
15b30b0a2e52a673af3137e586ef2d64
1815f0196e040bc3eaf33915bd783c3f
30bca04ec262394f907bc24f1c403f25
2f2356b9514e121a978e83571642db0d
1906fb2a0a7504b7681b9cd53f09b653
1a400481251fac98bc574c0aed7beca8
24b6839687dba863ac1e9c19c1a6284a
28ec18a041331d264e3836ddcc25f022
1af0aeb8c8fafd1f46cc5ba04bd64994
1ba63cac44899c36555f2ecc792e81f9
1cf9f30d114f6ec60778e47b7059f99b
20f22ed774bb74a36bb7701cf74e2be0
fce216145469021d65b5cd206ef6a016
fd7c451d538bde5e7f4c44f9adcd9f20
feae26f17da20dcf2f3b92c1e1384b0c
fecedeedc700847c52753f372c6b6357
fa0776d8538fcff32441a3715f5671d1
fa59ff8aaa60b1c40ee893c6ddf1ded4
fada11e2b67669f57cf1bab8734f86a4
fb04dd5a154182887cae35c3834719af
f2b799946df7a339075e94b7243cdfb2
f3ffc458ba9943d13842677eaf1d3b5a
f4467cf9b7f5c536f0766ac2851b53b7
f72f081b765a58da02a1d6d3069965b2

Reference

[1] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[2] https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

b. Small – Severity: High

Win32/Small is a generic detection for files that perform various malicious actions on an affected computer. Malicious files detected as variants of Win32/Small can have virtually any purpose, however, they are often used to download and execute arbitrary files (including additional malware) of an attacker's choice to an affected computer [3].

IP

1.53.184.92
1.54.196.249
14.162.165.48
14.162.166.42
14.164.8.147
14.169.204.114
14.190.118.48
14.227.196.191
14.229.94.187
14.230.143.232
14.230.183.27
14.233.221.168
14.245.45.245
14.249.34.70
14.254.202.224
23.141.128.248
27.50.18.130
27.66.118.25
27.72.46.64
27.72.91.252
31.29.215.136
31.167.153.141
36.66.243.2
36.68.53.23
36.68.76.246
36.68.239.5
36.72.216.197
36.73.34.0
36.77.25.250
36.77.180.162
36.80.190.59
36.81.4.112
36.84.38.92
36.84.186.32
36.84.227.146
36.89.92.61
36.90.184.126
36.91.66.173
36.91.157.193
37.224.40.29
42.112.170.145
42.112.181.10
42.113.154.44
42.114.31.16
42.114.234.18
42.117.236.229
45.79.186.48
46.2.241.16
49.49.237.134
49.144.163.162
49.204.229.245
49.228.137.219
50.116.42.99
51.255.140.235
51.255.219.220
51.255.219.221
51.255.219.222
51.255.219.223
58.65.179.226
59.144.126.39
64.225.2.125
64.227.1.133
64.227.5.161
77.89.235.14
78.167.195.77
82.140.212.114
83.102.217.45
83.239.13.130
85.105.222.101
85.154.58.188
88.230.172.181
91.213.8.47
93.91.112.19
95.181.132.140
101.51.227.18
103.3.69.66
103.41.132.187
103.43.129.98
103.48.20.138
103.72.223.119
103.73.68.71
103.83.178.230
103.94.168.62
103.216.217.188
103.235.171.8
104.128.54.37
104.200.19.19
104.248.56.20
106.193.35.49
110.49.105.114
110.139.25.143
111.73.45.90
112.78.149.179
113.20.100.203
113.22.10.148
113.23.99.72
113.53.91.139
113.161.13.233
113.163.189.34
113.175.166.7
114.142.175.52
114.143.182.230
115.75.212.128
115.124.77.253
115.186.155.238
116.206.40.23
116.206.148.82
117.0.142.155
117.6.229.162
117.102.85.170
117.220.197.154
118.71.251.244
118.175.153.172
120.29.158.14
120.188.77.178
122.51.246.185
122.226.117.52
122.226.117.77
123.16.242.214
123.24.136.139
125.25.24.94
125.26.97.205
125.63.70.211
125.161.107.81
125.161.128.50
125.161.138.244
125.165.31.132
125.167.40.6
134.209.38.216
134.209.47.171
134.209.167.34
134.209.167.167
138.68.225.132
138.94.39.131
138.197.109.180
138.197.207.67
138.197.211.42
139.198.126.118
142.93.63.161
142.93.123.164
142.93.123.230
142.93.254.154
144.91.127.139
156.226.33.138
157.245.123.87
157.245.127.27
159.65.34.127
159.65.74.50
159.89.53.250
159.89.134.121
159.89.151.4
159.89.157.46
162.243.172.247
165.22.33.84
165.22.34.233
165.22.38.97
165.22.41.91
165.227.5.254
165.227.63.163
165.227.101.90
165.227.116.13
165.227.121.100
165.227.123.30
165.227.124.83
165.227.185.101
167.71.98.82
167.99.156.42
167.99.158.56
167.99.173.42
167.172.29.221
167.172.224.131
167.172.225.20
167.172.228.117
171.7.247.114
171.224.172.191
171.224.178.238
171.224.179.211
171.233.17.187
171.236.48.67
171.253.131.193
173.230.148.156
173.248.225.80
177.23.16.164
178.128.0.42
178.128.15.68
178.128.178.207
178.128.189.45
178.151.158.61
178.159.227.142
178.251.106.109
180.148.215.138
180.244.33.153
180.247.203.240
180.248.22.42
180.249.182.227
181.49.30.109
182.23.59.216
182.253.190.12
183.134.20.30
184.22.27.180
186.67.104.83
186.88.196.251
186.93.195.189
186.94.79.135
187.202.175.130
188.127.37.18
190.39.49.236
190.39.147.193
190.73.6.246
190.74.230.228
190.75.38.132
190.97.246.3
190.141.228.83
190.201.128.148
190.201.148.31
190.202.18.78
190.203.27.232
190.206.62.17
190.206.122.44
193.242.178.234
196.1.184.6
196.62.185.95
197.45.169.157
197.51.33.82
197.51.85.44
197.51.184.18
198.199.120.162
198.211.112.108
200.92.226.50
200.93.67.209
200.109.237.11
201.114.204.192
201.243.4.30
201.248.120.93
202.53.71.42
202.141.231.194
202.142.163.227
202.162.194.182
202.162.195.65
206.189.71.181
206.189.72.55
206.189.73.152
206.189.177.191
206.189.179.184
206.189.185.39
206.189.218.52
208.104.79.93
210.210.137.130
223.165.5.1
223.205.228.9

Hash

685bc2af410d86a742b59b96d116a7d9
474ecb2fac7ef6f1b798d81d8a3ba5a2
b3812008522d080fcbdec1adc499df2b
235e9af4c6f5b5de7d30d0589bbcff14
0129086ae5fa2269d1037ff0ac0fca48
0cad216d1be79f216e76bb561bb0f67f
64f62894e7b8f7574cb8ccea414d768f

Reference

[3] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Small&threatId=

c. Occamy – Severity: High

This Trojan Spy arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites[4].

IP

31.10.15.12
37.57.208.166
37.147.94.19
58.218.66.175
58.218.66.180
58.218.213.76
94.143.149.202
103.57.121.14
109.169.65.141
109.169.65.215
114.80.116.184
138.122.5.218
181.19.118.58
188.163.83.93
190.201.129.241
201.208.30.219
201.242.61.152
201.242.88.4
222.186.3.21

Hash

9e19876ac649ec0cd226fd2240b09a07
ce1db9113237975df9965eff3d0c8754
8831cfc4b15416f07eb34d944641e179
72a300f8574f78906277b84a8c332532
7f51d4359d732b0a2b035d08ef10798a

Reference

[4] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_trickload.wil

d. Linux.XorDdos – Severity: High

Linux.Xorddos is a trojan horse that opens a back door on the compromised computer. It can also download potentially malicious files [5].

IP

23.228.109.180
23.228.112.164
23.228.200.67
104.253.78.252
107.179.34.4
157.52.228.135
172.82.191.119
192.200.197.98

Hash

42ba80053b0e744346236592b01949d0
55a111f4625348cffd6d910e49f5dbdc
2004f9f08f281f8d4ea7c913573dd6cc
28b4c1d34913014f2ea43298db493216
232e172f7a005dd12d4aad55e0c4a331
3e34bff8e13cf6068f4a30218b55b549
bcf80d78a918b22179c51cc68d671840
79a7792955c2e7137c68bec4803ce65b
8c8da16a2b9e7c318a9544ff032bddbe
b9cb431c103bd716493a7b70133012de
c663827b1cf068ff2e2b1a731bbf2826

Reference

[5] https://www.symantec.com/security-center/writeup/2015-010823-3741-99

e. Eqtonex – Severity: High

This Trojan may arrive bundled with malware packages as a malware component. It arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. It requires its main component to successfully perform its intended routine [6].

IP

2.187.97.160
5.52.1.156
5.199.221.174
14.232.80.215
31.135.182.75
36.70.238.12
36.73.63.70
36.75.64.119
36.75.66.195
36.77.55.181
36.78.155.225
36.82.97.42
36.85.42.154
36.90.166.46
36.255.45.199
37.190.61.174
37.208.97.231
41.46.132.78
45.251.34.77
46.99.184.59
46.201.245.101
46.242.61.54
59.93.86.176
59.94.166.99
61.1.212.230
62.76.6.70
77.238.101.162
84.246.229.135
87.238.233.25
94.101.241.203
95.29.180.238
103.230.155.82
103.249.80.122
103.249.81.86
104.209.104.97
110.138.246.55
110.139.53.86
113.160.178.146
114.7.165.186
116.58.233.29
116.58.251.30
117.192.182.113
117.193.77.254
117.202.79.48
117.215.129.9
117.222.165.39
117.239.148.35
117.241.195.88
119.42.77.81
120.188.83.12
122.160.66.248
125.160.65.88
125.164.244.191
125.166.116.234
125.167.48.215
128.70.169.83
153.174.36.237
158.140.167.18
171.236.210.69
176.222.157.188
177.221.59.163
179.191.239.12
180.241.2.83
180.242.154.133
180.246.148.177
182.73.11.98
182.253.186.83
183.83.247.32
185.17.18.48
186.167.35.166
187.95.114.113
189.15.65.164
189.254.158.194
190.37.62.5
190.75.96.62
190.205.174.157
193.0.206.148
197.165.222.235
200.195.138.91
201.158.107.123
201.230.158.90
201.248.21.31
203.34.117.5
213.166.136.238

Hash

95ae8e32eb8635e7eabe14ffbfaa777b
ce494e90f5ba942a3f1c0fe557e598bf
01bdc6fb077098f4a3b60f4b0e479a7f
e13c5a2cf223c57b61d71409218589cc
08f7b928261d121e1d5a40dbb95022a8
72790e6992073ccd0b5e3c37f6ee1965
86e4c4652ae173b1f378a22b5ad3f33d
9947feb0f1a5f0da5b58b1cf4568e2f6
d678a1b86735bc487635c6867774c486
daabf4beaaab704956f6a99d05cba9dc

Reference

[6] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win32.equated.lzcwo

f. Zombieboy – Severity: High

Zombieboy is a trojan horse that may perform malicious activities on the compromised computer [7].

IP

1.53.167.132
1.186.77.85
1.233.149.222
5.133.29.226
5.159.110.164
14.163.239.202
14.164.46.180
14.171.9.252
14.187.148.192
14.189.11.21
14.242.234.60
14.248.109.144
14.248.249.251
14.255.115.246
27.65.13.149
27.72.63.251
27.72.78.220
27.76.5.224
27.78.28.246
27.106.100.85
31.220.171.206
36.68.237.252
36.72.79.158
36.75.140.138
36.76.178.243
36.89.149.53
36.89.235.203
36.92.100.197
37.145.140.220
37.228.66.83
41.70.64.4
42.113.58.234
43.225.187.242
45.5.40.240
49.145.96.7
49.146.53.5
49.146.53.236
49.151.123.69
49.207.12.132
49.207.179.41
51.178.100.76
58.27.207.166
59.151.104.144
59.188.31.239
61.0.237.26
61.12.45.66
61.246.32.118
61.246.38.175
61.246.39.199
77.40.51.153
77.222.115.207
78.36.197.162
78.38.134.5
84.235.90.201
85.18.159.184
86.100.27.210
87.225.106.81
87.229.187.90
88.135.119.180
89.34.160.249
91.236.176.28
93.81.100.140
93.191.14.37
94.231.132.149
94.233.240.150
95.30.84.125
95.30.150.21
95.58.114.245
95.104.113.118
95.161.222.201
95.175.90.253
95.181.2.17
95.181.2.77
95.181.3.156
95.184.47.32
95.188.86.193
103.26.59.250
103.29.117.112
103.29.118.17
103.36.121.68
103.40.135.131
103.47.159.170
103.51.138.54
103.90.159.59
103.104.215.186
103.199.161.204
103.225.222.80
103.228.119.18
103.250.159.157
106.0.56.69
106.12.252.6
106.201.231.143
109.69.4.139
109.191.154.169
110.137.80.99
111.125.103.199
112.133.251.170
112.197.72.28
112.199.69.187
113.23.51.90
113.162.117.127
113.165.2.205
113.173.48.167
113.175.160.250
114.79.184.50
114.143.161.182
114.143.201.107
115.72.210.26
115.73.209.168
115.79.36.99
115.79.46.26
116.101.138.143
117.3.69.207
117.4.136.220
117.4.148.251
117.240.189.202
118.69.77.118
118.70.129.13
118.71.97.78
119.93.152.205
121.96.14.226
122.55.223.18
122.103.128.190
122.155.137.7
122.161.214.186
122.165.207.148
123.16.134.156
123.18.97.235
123.24.138.68
125.25.96.8
125.163.155.229
125.209.115.186
139.255.37.211
150.129.131.34
171.226.32.113
176.32.192.230
176.106.144.186
177.23.143.206
177.67.128.2
178.91.72.50
178.159.113.254
179.98.175.61
180.241.128.118
180.242.181.154
181.48.91.59
182.74.145.116
182.75.38.29
182.75.185.46
182.96.87.251
182.232.52.191
183.82.101.78
183.82.111.98
183.91.7.111
183.91.15.184
185.228.184.95
185.232.22.207
186.179.68.217
187.19.206.51
187.75.77.227
187.223.19.150
189.254.158.194
198.50.17.116
200.41.176.9
200.186.71.2
201.92.136.177
202.40.178.42
202.43.164.235
202.47.115.4
202.73.34.228
202.79.21.215
202.83.18.43
202.83.28.64
202.142.148.196
202.166.166.20
203.76.248.48
203.128.241.122
203.202.242.11
203.205.26.69
203.210.193.112
210.4.106.130
210.4.106.138
212.109.7.105
213.34.192.2
213.34.198.190
213.186.163.122
213.227.244.34
219.65.39.2
222.252.20.219
223.190.105.76

Hash

26f0446df04e1097f5575445fc0e6787
f70557802f671ae027d602d2bd3fd6cf
3062df26ec61ca773e8c7cd487322562
460d954551187b65670074c8d5a7210c
cbd91d483bc5d87b16938163e75ef67f
b401240ef456e33a7bfcdd47204eaab4

Reference

[7] https://www.symantec.com/security-center/writeup/2018-072406-4226-99#technicaldescription

g. Tiggre – Severity: High

Tiggre is a malicious trojan that have been used by attacker to mine cryptocurrency on victim's computer or device. The malware is sent to victim as a video file but technically is an AutoIt scripts. This Trojan infected on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites [8].

IP

1.161.101.49
1.168.82.89
1.172.177.99
1.173.36.248
1.173.46.246
2.244.115.57
24.242.130.158
24.249.44.236
27.105.113.222
31.40.41.36
31.45.225.168
36.91.191.169
36.232.39.115
37.73.5.155
37.73.41.81
37.145.125.249
37.146.107.196
38.100.27.130
41.41.203.83
41.165.18.18
41.226.25.161
42.187.121.111
46.55.73.208
46.219.214.229
46.233.239.201
49.158.0.171
60.245.42.89
60.245.45.121
60.249.206.148
61.12.37.14
61.178.118.183
61.227.14.197
61.227.28.74
61.228.115.95
62.253.102.1
69.80.55.131
70.23.31.53
78.49.170.86
78.84.254.168
78.85.48.107
79.143.46.105
79.170.27.106
82.238.168.107
85.90.220.250
88.81.238.106
91.76.231.210
91.202.135.241
91.241.150.177
93.118.100.222
93.124.10.67
93.177.2.57
94.41.11.167
94.41.243.73
103.14.38.130
108.49.186.51
109.48.232.62
109.70.184.50
109.87.48.68
109.252.118.59
111.246.23.168
111.251.41.170
113.255.115.180
114.26.31.91
114.36.88.42
114.39.87.219
114.39.192.67
114.40.82.4
114.44.72.5
114.45.18.90
114.45.161.125
114.47.43.71
114.169.236.202
114.198.174.230
116.254.102.154
118.166.180.245
118.167.97.81
118.169.151.112
119.240.122.22
121.116.237.64
123.195.224.61
125.23.134.110
125.230.192.178
125.231.101.206
134.255.152.24
145.253.191.53
145.255.9.68
150.116.201.151
168.194.116.246
170.78.104.10
175.98.120.15
175.99.152.178
176.100.161.22
176.226.160.20
178.78.152.177
178.137.160.251
178.150.42.121
178.216.161.161
180.200.48.230
186.233.74.121
186.233.77.202
187.45.106.183
187.134.158.254
187.170.43.226
187.189.18.44
187.217.124.179
187.217.207.27
188.113.166.101
188.121.200.105
188.163.46.125
188.164.162.210
188.169.148.64
189.146.194.209
189.254.244.35
190.34.206.124
190.34.212.202
194.186.152.10
195.3.247.250
195.239.131.222
200.107.150.20
201.186.149.25
201.201.230.92
202.162.78.198
203.114.125.69
211.72.113.219
212.5.158.144
212.116.104.22
217.219.192.115
218.173.27.35
218.173.97.137
218.173.98.100
219.84.229.101
219.84.254.10
220.129.116.55
220.129.192.66
220.130.233.29

Hash

ca71f8a79f8ed255bf03679504813c6a

References

[8] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_digminein.a

Appendix 1: List of MD5 Malware Hashes

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	ae12bb54af31227017feffd9598a6f5e	359
		996c2b2ca30180129c69352a3a3515e4	196
		414a3594e4a822cfb97a4326e185f620	194
		0ab2aeda90221832167e5127332dd702	160
		a55b9addb2447db1882a3ae995a70151	71
		cd99e5e4f44621978faf8df0e01d2d2b	46
		cf4f46336abeec03630297f846d17482	30
		e9d1ba0ee54fcdf37cf458cd3209c9f3	21
		6e72ad805b4322612b9c9c7673a45635	18
		a4d49eaf60a8e333708469606ad9e1a4	14
		ef894d1c6dd120fad5a885bc737d6338	12
		a48ca7b40ab2a6ebdd94dbd52164c6cf	10
		9ba5379aa41d707a4331d27a004baec1	9
		8e6bfea06cb00553ee29b3822b349bd6	9
		bdcaf7ef34cd9b02932e5ee2297e4893	9
		6633a19602561d359e76a67a008d62e8	9
		33d373e264dc7fdb0bcdbd8e075a6319	9
		879d69d4c18d6947f9ea5e545ac16d01	8
		aa718a028875637e1c6eb648706340b6	8
		fcdecb1304a1fc6d574e8337eaf4cdaf	8
		62186bebffffcfafb1c70a8ff03fa317	7
		3553aeb71299e94c2549f1b34f6c1a43	7
		095d83ee1494554d00b726cfddee494c	7
		2de98404eb4ac4a525ed1884f4ea445b	7
		7c7262d9e49a40a52d0040942810456c	6
		a2151cd48a3186290411217caf1016df	6
		ab5b987b02bed407d4833ba83a0878b8	5
		8bd8a9c3871c32f8dfbac7711a75dc52	5
		8fa0e5dd92185799b73cbfab3da3e919	5
		c16edec919fc35cb39097f84f1b87455	5
		e49594ffa18e330c8692d88dc8e73752	5
		e5840a9753ed8f90fbd7264c8db27c4b	5
		8b7137adb7aac5cbf55b039babb612bc	5
		5d19193a153ab77f7d3a5807fbf03767	5
		50b93e08b91de26b5487abe79afe1d4a	5
		59b5090fad3d62f05572470f0c79c9a4	5

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	2f76b88b420003516f90062940ef7881	5
		0ab9a60a55cb40fc338e8f4988feee2f	4
		30e3f8ebb578da4247b6bf7e43beda36	4
		4f53357da304a79b6cb55fd8de9a094c	4
		54dd9593fb858bb8b1a77fe5e9238ae2	4
		5ffdc8b7825f72a04d5c97b6a4d80e7e	4
		d58fef5143d515816faeeeacc1627286	4
		d3891f56ad175f9af1d21f3072f73ccb	4
		daf7e72c18545d74aa1cdcdd6b306dc7	4
		c475b82f1e0b421e051622f034b1d5e3	4
		c0d149a7828c3ad6046da2d897bcff0c	4
		c5ff03fe7bb4384a1814c3fe7fe84119	4
		caf082a135af8d966e8dc7fb9f619bba	4
		8da3345636b0f9b8c0acc811f5a26c61	4
		aa7d98d151002e997fdbf6f2dbe7b8ba	4
		a135677250b0007496c39cb5c876954d	4
		a1fb001af7f76d36d0ee85b3c6453ca7	3
		af76bbae1d51d04f1113bc225f979820	3
		8d340ce819b42f0c5a27753dd7170ff9	3
		951b218fab52434aa7d4624c03dd3415	3
		95ff0a735ffc1b048110d8d21924da66	3
		98df58e71b5202e49ba6f9e6e43ef6ef	3
		c024bd7b3e360bed37d815bdf106acdb	3
		da5eee93accd46fe8755b93a19ada407	3
		ed03cfcc81546aee052e5d3360abda8d	3
		6313dc47b8f44c9a808c0577ca7f4fcc	3
		6e1dfefa794474d92b9e4412aea69f77	3
		890d5aa0d18a6fca571cf710269c714c	3
		6567e663303386b7152d5fcab1f06cac	3
		729a5152f496cd96b653cca40a14eba4	3
		78eae7fce7c9388446dc27ff213fe28b	3
		398c9ce412840482219a86730d9853f1	3
		3c63f9be8f7752de7f002ed0c3bdfddf	3
		44bc540ed22c83517ff5068ba58da383	3
		033f9150e241e7accecb60d849481871	3
		0064e2641d419d2c68f9beb18246a297	3

Appendix 1: List of MD5 Malware Hashes (cont’d)

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	2b4d3c993bc777de8d10ac080e3e5c00	3
		2c003aef97036420170c481b10fc8da5	3
		1a8996bae6e4cde7e6e8322e787506d1	3
		f14afcac1094f1a6dfd84da5162a55c7	3
		f9ca5dc4c240d66aaf08b2853d1535ba	2
		fb1d03437dea96371c7c7d91e234c4d0	2
		fc1e617b1ff659f1826868baedc9c258	2
		fcb6b0f95853dfda72d5535a424b3a29	2
		2118ffc9aa1c4f3f2c209293d0b12c42	2
		2259ebf3658c2dd6ab1e53e3c23fad4d	2
		22bc832a16559912d53fbe83cab1a17b	2
		2ce0cc8415ef608a6c97e7848e29ba8e	2
		1844584ed70abd0c48cf3c4d68e9e15f	2
		2f92bf0bb72ed014b515e338c5bf0d59	2
		017f63d0be693e53bc5b8edd426cfbd1	2
		01d87121a4a589930d580a88e4df3640	2
		4c8168df8d268aa5b6d1b02145b20379	2
		3695f6d3175e85e25ea3cc65ab3801cf	2
		5265fc3146b7e3922c79ef463aaecd16	2
		6a139899acde9af3c79c024bee1a800b	2
		6b0ac3a36170aa066c86caec90aea67b	2
		7823636f9ce01306178c1ee7772ad831	2
		63c573c0e2eb59009ef97da2ecf73f0e	2
		4fbfa754204df11c5d7d4d76bb4b777f	2
		5a579e20d6fe26579648c3961ef179ca	2
		5a9e809ef287470a50cef41df8897b62	2
		ec53e27425a44def7eb3f950ed0cb6d0	2
		ed979ce49b3373765a91b15c1c37c00b	2
		e66a0f43a8a5220d362645a13569ebca	2
		e6a999cd5df18b0962b89e1a9c1ebfaf	2
		e14e4f339bb5dc690862e91cc6341137	2
		d5cf687cd06c000d9421413c18972c75	2
		dfac55e674f9d62589cd531ffe25fcac	2
		dce06798d1f588e14a50dd741ff7e8c1	2
		c2b8b099bb55f52e094d22266b6d7b34	2
		cc435ef3d7e00bcb2720743f17705323	2

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	c96b8c08aa8c7177a82b22d898eb1d79	2
		d31d25eedd79f744b8a3d58888fd668b	2
		ce223b231f2862124386c585e9b95ca1	2
		cebb64bfd042804239424fed482aa986	2
		951806fed26ede01685f03413607fe18	2
		978fcc48a006c05c94e626ccb2ddfe53	2
		9792cbeaa00a9e7f3a58b5827441e71d	2
		98abe26199f28ab4e2b42e85f975b9e4	2
		997e58102bf42ef2aade109867968160	2
		99cd95db92c4e4cb4b882eb034e75cab	2
		843ae62b27d29e88a4a5389dbf501ddd	2
		b294e857dbc07134be8c0624b94e6b69	2
		b794a273d022fc0c10d783afd6e1493b	2
		9df37b7f669ad8290c382975e961b600	2
		9ecca08445521f486fe9bff458817b2f	2
		9f0f848cc5f6daecccddf8ca0bed1f10	1
		9f61d37c99f647a1b0b3d0a431e4db24	1
		9fe0b783f824bdac40dc63586086224e	1
		a1192132123bfd5c9f3b916ee332fe8f	1
		9e1b0a51e149acfa5937bf52bd9e3b9e	1
		a143dc870869cc275ef35dbf733e046d	1
		a3115fd8e1717b46a08dd2100b625e6d	1
		a5e5710ba3eb92ff1010bba4642517a7	1
		a725bf924d21fc981dd173fa66bca35f	1
		a73c89e52851553a63963fd0f790c789	1
		a821b8ced79eeff440a64b3d87e984c6	1
		a917c331735c46c1aec3e23fba88e7a0	1
		b7c30ca8a05951ed1c76ae4a62749f6a	1
		b9de290ef3ec191950f0550cf6d14a6f	1
		bb1cf62b506c0848a878a1526efa1357	1
		bc4756aae7540d6073d9f440da474481	1
		bd675a31ff5ea593c51e9bad87917784	1
		b37d1c7a3260e50826b3cbd6ceb203e2	1
		b46b61f29402626a483f28f99644b8b7	1
		b6d1f1d400b26f78039216850f50dc88	1
		b72ba971ee250f3f493008a638040fad	1

Appendix 1: List of MD5 Malware Hashes (cont'd)

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	b016a2d5e8963fb6bb1f810502e1562f	1
		b075ffe9788c0befe9ba892d0844bfd0	1
		b0a5f29fc283d06db2109d62bd0aa9df	1
		b153ea5ba3e0e4e285e2394be2af3784	1
		aa884946d64a8967cdc994872990a299	1
		abf42da16e0971ff966687c6e7d21987	1
		ad7134b925745229f56b8fbff4a4e84c	1
		8c74951768866866ed126be277e09d87	1
		8ce48814e2d2289caa614f87856cb5f1	1
		8e6635b3dcb090c8478fc392ca94722e	1
		8e909510d1a1ac5ace42ed5e1afaea33	1
		8f6a66a53beb129cd07a8520e1326041	1
		967d46d8baa5152f7f366571b39225dd	1
		96b11451d63b36111ba78a37532e97f3	1
		901decc503049bc0108dc9cd5eb94ffc	1
		9155183e0b2031ba0c7159f76840ffed	1
		94b1b4ca313dc3ae348fa5a79b36ad34	1
		9a142dcdc57eac7225800aa114f1fdb5	1
		9a1768e5531d0852278b95e4d0137977	1
		9aa3637857d84aa040c097ba0be6b900	1
		9aa42e3fba9d860fd23c3dc54cf65d0b	1
		9aae6412b2dfc9ed503e6c7123e95579	1
		9b26bb265141692a7b81cef74fa9bf8a	1
		9baf8ffbe84fdb05ad355f75d4ac73e4	1
		9cabb6302630ba5b43b166575f157db4	1
		9cc600b0c21a0ee60257aa9d5aaf0b44	1
		ceeea870bf5ecffb612cc284e14ffb2b	1
		d251dc6ccf4c3a88b7c6a97abb64e2a5	1
		cab74b35aa582da53c621a442ec5ee33	1
		cacbe198c83c1e1420c2f0bde401585d	1
		c688aaf68c68b2570d10258d7e435de4	1
		c69d230d92302dafb9f6f3a93113ec0e	1
		c71854ceb8c814bd85c0663c72c1a5a5	1
		c72e5e053e21231065d266fd3eaa708a	1
		c75e04ce201b41356cb3befe228a23df	1
		c881745e136cd982aee1cb9edffb0020	1

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	c2c4612c2138df47a52a526fbae3ab92	1
		c3d8b9d5bb048eebca994cdce641f885	1
		c04e6ce0dafa8fd0c005f90f997083d1	1
		c4fca61333b642e21c2b1ba417c0100d	1
		c0f043df3a5f47dc6bde71922417df86	1
		c1045e165824a769408792e176290035	1
		c14432e2751479323db1fe1f185e5c6c	1
		be6da1c267fc762b8e26a57e3026abef	1
		be9bdee97e6142aeb032bda086b983f7	1
		bf137d87e79f68177dd1eb0b780a35e4	1
		bff0aa6595e3fc250a32ada5ca1c0cfe	1
		bff63cefd43b6a881ffc1e61dd0215ac	1
		de5d77be7e096b08f8eb25cabe59d16c	1
		de5e5585f3e65d16cc19af7b2daf3090	1
		dee385512069d92fa4f4c84eed132415	1
		e07b1006b251db11368b60f57e13cb0e	1
		e12d0c0ba668e1592c5de9390f3005dc	1
		dbd4a6eb6f597b3f53e66e5284d05e23	1
		d8730841f4ace471fdd23544cc27b1d5	1
		d8eedc656348729aea8571c5640d9b87	1
		da2506e63930938a41ad2bf44d59697b	1
		dab719e743b33b9b4f47a49a6a21d966	1
		d52f3678521d2330610811723f1c2891	1
		d540f05b1d45787a0bf809f115855134	1
		e2f6cd5e295645e69b6f1e5e0fc56964	1
		e4cc9844574dec633d8adc474215159c	1
		e5551e9a1ef43d37bfe254e39afeab4a	1
		e6cc34d3d80b6941ac7fbd8bbb1ddbc5	1
		ef308fb6f974a766ab59bb68b1864aa1	1
		f0b0714d21283cbb8429edae07962291	1
		f0e4df1d50065af086a85c17103c57f1	1
		ed39402aa43bebf9dc6839dcb9cecf03	1
		5ab41fee92e06daffa1276902b90f7c2	1
		51724a2aa578961ed6784b711c164b58	1
		51f74846b7f7ea38ea74758c2cdf5adf	1
		552e88c8f7678d685b0498dd6c50245d	1

Appendix 1: List of MD5 Malware Hashes (cont'd)

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	56319a9877f62b75bafe89300d324090	1
		56fd3342b2996306982bcbb578115e33	1
		5778216a90f804958862d66af3ceeb87	1
		5818d137c6c7324aa05a01c8c3cfe9d9	1
		58686fd92b0cf4183e84c2017b37d46e	1
		58a20a3827a0e27c337fce30efacce7b	1
		6442441eb52236bbf78d67820f833fe9	1
		654ae4e4c97fb243a71a15532e3287f0	1
		6350f8da991da9ee85c63e15cce88fbb	1
		675ca172a6c351db3f43d328c7347097	1
		678323b12f8ae74c7bf406efced5f476	1
		68e889e597051dc2bba55f53c69d5c73	1
		61371b4c0b9e0250d5b3273f58780df4	1
		614cbd6036e337f710caa34c66ba5a69	1
		6207b75cae51b6f73891a014863845b4	1
		5dbb17f0ac41162154e1690d25483e68	1
		5eca730845d10f71d767d5a3f3119b15	1
		6293f4978ec83cf7c6ad8f9baef25743	1
		62af43d2b728f200f8d576f095fc85cd	1
		8b9d53fad84c0d7972484bbd8f258127	1
		89e18532ea2245deb8af6585708e7d74	1
		8a4f6a3629fe6ad3ae8b0e7101d252d8	1
		8af6e4ce4bffac0b4807851250709943	1
		8b31308f2bf97e940dab49334d2d2011	1
		7cf21cdad3e9afe55c93277c8a6bdf05	1
		7dccf1d3a50c9d76557d0fbb68cdfc22	1
		7f6c952f2cdd24fe828f30f0d2433d72	1
		7f7fc6a29e4b39b530e6ace0ae8d7bdc	1
		804748534449ce9b2b081831567b806f	1
		809456dd1cbe82ab1a13473bfb638ba4	1
		8110273cddd766bda4aab40e443427e0	1
		827e7a475c522b2c6d81fa99154dcb8f	1
		8337e6b54b5a982f20228ed33adefa9f	1
		83544683ea936a82697a465bdf6093e1	1
		837b7a7a2f4b984cfda9a83199f767b0	1
		83a1896164025997d76a7dd94393db3e	1

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	6b17566ae9ed0fae76f1fd0b9a9029ef	1
		6b5a9da099c8dd5b63a63c01c0256210	1
		6cb21deaca071ac4d8c3a6f9cdc17f58	1
		711a166b88ac297cc530b8140119841d	1
		791af1c17458398c52f4aa53770dea37	1
		79762e653db25e4af8d1233059005745	1
		79e1e07fce2b0436cfb643ee8465dbbe	1
		7a60943b74e7d36a2b1b922f07432a83	1
		733c67a5a392b66b8b8259169ef240f7	1
		74b16d9cf7d09b4878401401a481223b	1
		75c75db2124405f06a8351465d7892c3	1
		76b47e0829177757b39cf3c3672049dd	1
		36d7c42d5490b82267a617b1d6bd5c96	1
		36e5f7f493f155a87baedf34c2705b6a	1
		372a3f6e2b9752a2035c673b6dd7fe32	1
		37984af86c5d8c00c8456c1292771c72	1
		37a3ca268f5d7379fcb5268296336771	1
		38ab7916fc2ba54ec6ade58a137556b2	1
		3116ac3731d2d5688452074d7fb5a6c9	1
		3151485a025cb17bc3732533209a9f79	1
		345ea68ae2052193e6a5c34806801550	1
		347cc5676fceecc0598a4d62c2c36b7e	1
		3ce7baba17fcf32f7310e9ab435b9511	1
		3d71c399da5b2f7bd4208c740231979a	1
		3e1f1ab7eb22b54d451f764377d869ab	1
		3e655040fe787d7ec833fa019fc3a5a6	1
		3f3d6691012cff45f5fbf67a0c65a6fb	1
		3b34cfe3ec07b73d508edda28e3ffffe	1
		3be07dbcc9dcf772a64bebf30bc8d1c0	1
		3c3591eb1df1f5f60cc846685303fb58	1
		4dcb93a3f82760112c1ac9cebc3f44ff	1
		358ebe06d58df0203a6067d0575e9d7e	1
		42708471bba43fab8c0834de27a7a3a4	1
		429e6c88db4d5fc81669f5987abf110d	1
		42cc3dc485724f134451fb157eb77213	1
		430599e85618bd750b5bbfb21cb5f857	1

Appendix 1: List of MD5 Malware Hashes (cont'd)

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	4306b68e3ca2d7ed71364acb8a6939c3	1
		44ade454a487822f1c9d75aa7d8df907	1
		4535d83ee1b6cc87b19eb788f0961422	1
		45735a816370f26b06e053656ca7315d	1
		46590d5fc431f79c2abfc7783c21f409	1
		47bc7c8f1ac38746f74e543a4c421d75	1
		499482e2c2069f814dc9e1e9a16952d5	1
		49e38bc384b99902d6dca4754c63edee	1
		4a4de629b32cfbe6b19f12bddc3ebef3	1
		4adc61cc12645a3318edbcfee460a3e5	1
		4b2d8f066eb5a0438f855201d1a1b3b9	1
		4bb7874325d95b3f1fcb57ac10bdba45	1
		4c50e407de345c5544d27fa28315519a	1
		00c9e54f5c2c31cf4bc2bb0a178712ec	1
		081967adb6eaab608a891f96f520d5e3	1
		08bcd0b071a5ea741d60269654223c37	1
		09900abd691ab580d9ddf0b20c8671ce	1
		0a3a089906fcbd25904c8c8d7464ffda	1
		0b57fe54929b51600497598c03408806	1
		0c8caa346454bb05990d4fe63465da26	1
		1367ff38c61bd7deff3837c4f24ca4ef	1
		15a0cf8350ef9bd4222d203dbe437977	1
		15b30b0a2e52a673af3137e586ef2d64	1
		1815f0196e040bc3eaf33915bd783c3f	1
		30bca04ec262394f907bc24f1c403f25	1
		2f2356b9514e121a978e83571642db0d	1
		1906fb2a0a7504b7681b9cd53f09b653	1
		1a400481251fac98bc574c0aed7beca8	1
		24b6839687dba863ac1e9c19c1a6284a	1
		28ec18a041331d264e3836ddcc25f022	1
		1af0aeb8c8fafd1f46cc5ba04bd64994	1
		1ba63cac44899c36555f2ecc792e81f9	1
		1cf9f30d114f6ec60778e47b7059f99b	1
		20f22ed774bb74a36bb7701cf74e2be0	1
		fce216145469021d65b5cd206ef6a016	1
		fd7c451d538bde5e7f4c44f9adcd9f20	1
Ransomware	WannaCry	feae26f17da20dcf2f3b92c1e1384b0c	1
		fecedeedc700847c52753f372c6b6357	1
		fa0776d8538fcff32441a3715f5671d1	1
		fa59ff8aaa60b1c40ee893c6ddf1ded4	1
		fada11e2b67669f57cf1bab8734f86a4	1
		fb04dd5a154182887cae35c3834719af	1
		f2b799946df7a339075e94b7243cdfb2	1
		f3ffc458ba9943d13842677eaf1d3b5a	1
		f4467cf9b7f5c536f0766ac2851b53b7	1
		f72f081b765a58da02a1d6d3069965b2	1
Trojan Downloader	Small	685bc2af410d86a742b59b96d116a7d9	398
		474ecb2fac7ef6f1b798d81d8a3ba5a2	236
		b3812008522d080fcbdec1adc499df2b	42
		235e9af4c6f5b5de7d30d0589bbcff14	29
		0129086ae5fa2269d1037ff0ac0fca48	16
		0cad216d1be79f216e76bb561bb0f67f	11
		64f62894e7b8f7574cb8ccea414d768f	4
	Occamy	9e19876ac649ec0cd226fd2240b09a07	44
		ce1db9113237975df9965eff3d0c8754	23
		8831cfc4b15416f07eb34d944641e179	12
		72a300f8574f78906277b84a8c332532	11
		7f51d4359d732b0a2b035d08ef10798a	6
	Eqtonex	95ae8e32eb8635e7eabe14ffbfaa777b	36
		ce494e90f5ba942a3f1c0fe557e598bf	34
		01bdc6fb077098f4a3b60f4b0e479a7f	14
		e13c5a2cf223c57b61d71409218589cc	3
		08f7b928261d121e1d5a40dbb95022a8	1
		72790e6992073ccd0b5e3c37f6ee1965	1
		86e4c4652ae173b1f378a22b5ad3f33d	1
		d678a1b86735bc487635c6867774c486	1
		daabf4beaaab704956f6a99d05cba9dc	1
		9947feb0f1a5f0da5b58b1cf4568e2f6	1
	Linux.XorDdos	42ba80053b0e744346236592b01949d0	14
		55a111f4625348cffd6d910e49f5dbdc	12
		2004f9f08f281f8d4ea7c913573dd6cc	11
		28b4c1d34913014f2ea43298db493216	11

Appendix 1: List of MD5 Malware Hashes (cont'd)

Type	Malware Name	Malware Hash	Detection
Trojan Downloader	Linux.XorDdos	3e34bff8e13cf6068f4a30218b55b549	8
		232e172f7a005dd12d4aad55e0c4a331	8
		bcf80d78a918b22179c51cc68d671840	7
		79a7792955c2e7137c68bec4803ce65b	5
		8c8da16a2b9e7c318a9544ff032bddbe	5
		b9cb431c103bd716493a7b70133012de	5
		c663827b1cf068ff2e2b1a731bbf2826	2
Cryptocurrency Mining	Tiggre	ca71f8a79f8ed255bf03679504813c6a	655
	Zombieboy	26f0446df04e1097f5575445fc0e6787	212
		f70557802f671ae027d602d2bd3fd6cf	7
		3062df26ec61ca773e8c7cd487322562	5
		460d954551187b65670074c8d5a7210c	3
		cbd91d483bc5d87b16938163e75ef67f	2
		b401240ef456e33a7bfcdd47204eaab4	1
		Total	3630