Malware Research and Coordination Facility Project

Monthly Trend Report

DECEMBER 2019

CyberSecurity MALAYSIA

Powered by:

LebahNET.MY
CyberSecurity Honeynet Project

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 557 devices. It involves data unavailability, data breaches, and backdoor activities. The list of captured malware consists of WannaCry, Small, Linux.XorDdos, Occamy, Linux.Morila, Zombieboy and Tiggre.

The main threat is the WannaCry malware with 435 malwares captured. This is followed by Small with 134 malwares captured; Tiggre with 27 malwares captured; Zombieboy with seventeen (17) malwares captured; Linux.XorDdos with sixteen (16) malwares captured; and finally, the Occamy and Linux.Morila malware with 1 being captured respectively.

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.

WannaCry Tiggre

Occamy Linux.XorDdos Zombieboy

Small Linux.Morila

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.

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

Attack Type

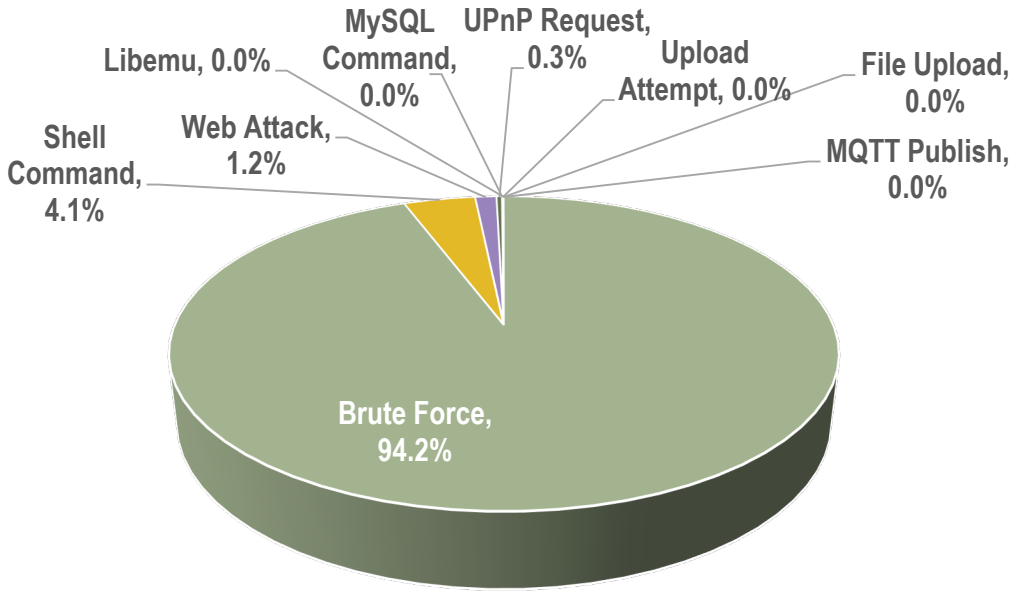

Figure 1 Attack Types

Figure 1 above illustrates the statistics of attack types recorded in December 2019. Based on Figure 1, Brute Force recorded the highest attack with 94.2%, followed by Shell Command attack with 4.1% and Web Attack with 1.2%.

Table 1 Attack Types

ATTACK TYPE	TOTAL
Brute Force	3,832,755
Shell Command	167,788
Web Attack	49,992
UPnP Request	12,929
MySQL Command	1,665
Upload Attempt	1,176
File Upload	1,049
Libemu	76
MQTT Publish	27
PPTP Connect	1

Targeted Services

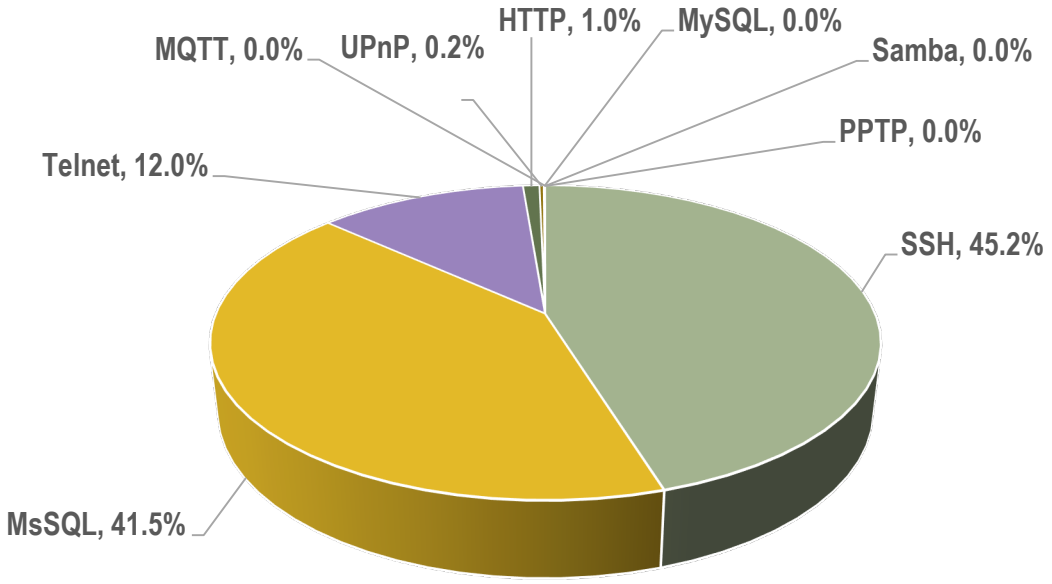

Figure 2 Targeted Services

In Figure 2, nine (9) targeted services data are recorded during in December 2019. From Table 2 on the right, SSH became the main target with 2,375,771 or 45.2% closely followed by MsSQL (41.5%) and Telnet (12.0%).PPTP is at bottom with only 1 attack logged.

Table 2 Targeted Services

TARGETED SERVICES	TOTAL
SSH	2,375,771
MsSQL	2,181,721
Telnet	631,782
HTTP	49,992
UPnP	12,929
MySQL	2,464
Samba	1,898
MQTT	27
PPTP	1

Top Malware Detected

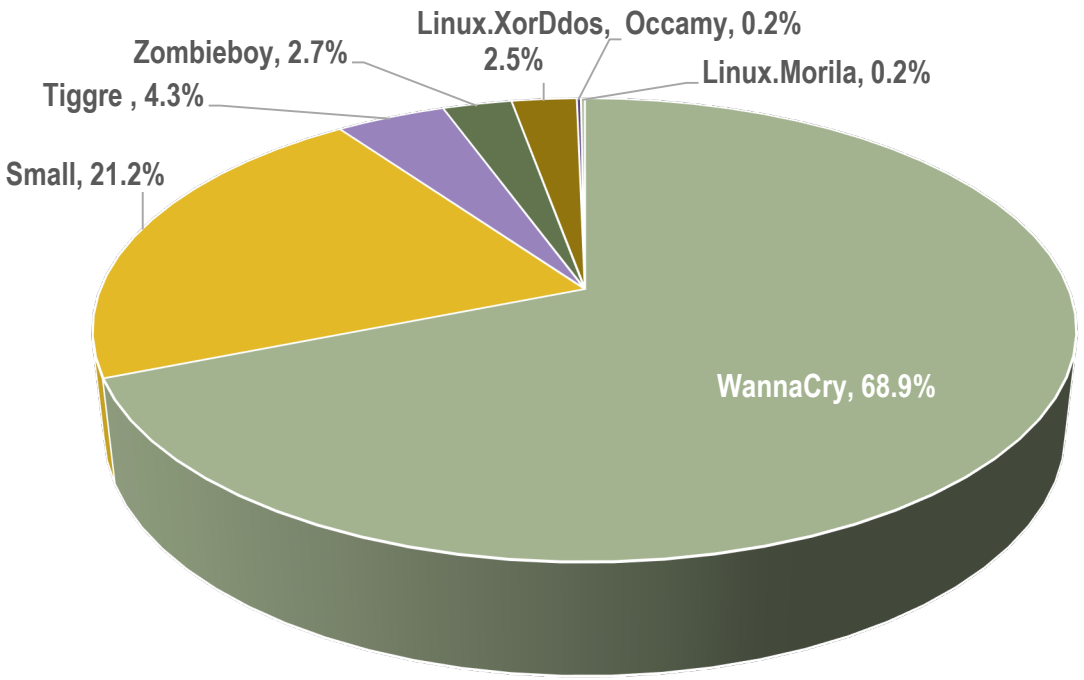

Figure 3 Detected Malwares

Table 3 Malwares Counts

MALWARE TYPE	MALWARE NAME	SEVERITY	EVENT COUNT
Ransomware	WannaCry	High	435
Trojan Downloader	Small	High	134
	Linux.XorDdos	High	16
	Occamy	High	1
	Linux.Morila	High	1
Cryptocurrency Mining	Tiggre	High	27
	Zombieboy	High	17

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 435 detections. The ransomware captured is WannaCry having a total of 88 unique hashes. This is followed by trojan downloader malware type with 152 detection count by the sensors; Small (134 detections, 3 unique hashes), Linux.XorDdos (16 detections, 8 unique hashes), Occamy (1 detections, 1 unique hash). The lowest detection count is the cryptocurrency mining malwares with 64 event count from Tiggre (27 detections, 1 unique hash) and Zombieboy (16 detections, 8 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

1.161.235.226	109.184.87.147	115.78.95.90	119.147.212.244	14.163.110.83	14.254.73.54	180.241.45.197	183.91.4.40	200.0.102.2	218.248.49.2	36.84.187.196	49.149.77.236	78.85.49.245
1.161.250.118	109.234.112.72	116.103.219.247	119.42.114.232	14.169.10.242	14.98.213.134	180.242.212.229	185.15.131.248	200.111.237.218	221.120.32.118	36.91.213.115	49.230.142.206	79.23.59.47
1.172.210.119	109.234.112.73	116.193.222.123	119.93.87.169	14.169.27.99	154.120.230.250	180.247.168.156	185.17.128.202	200.116.209.114	221.132.113.188	36.92.104.13	49.231.202.132	81.163.139.116
1.52.168.216	110.137.179.108	117.198.199.154	119.94.155.209	14.169.88.150	159.192.104.69	180.253.46.198	185.216.194.222	200.142.99.134	221.133.16.226	37.230.183.31	49.248.120.75	81.214.143.143
1.52.206.128	110.37.223.122	117.2.143.46	12.20.137.71	14.170.152.1	166.130.116.101	180.254.137.178	186.103.213.2	200.32.10.210	222.174.251.202	37.239.255.245	49.48.134.29	82.142.173.230
1.54.45.176	111.125.230.42	117.2.171.125	121.123.29.27	14.176.168.16	171.213.29.107	181.143.210.114	186.114.50.133	200.5.119.43	222.252.30.7	37.57.71.90	5.201.176.167	83.110.2.115
1.54.5.143	111.93.146.210	117.2.35.216	121.196.204.23	14.176.5.30	171.224.180.113	181.151.233.43	186.170.28.202	201.144.42.104	223.176.5.66	37.79.255.188	5.206.18.24	83.148.94.213
1.55.167.64	111.93.169.98	117.2.84.28	122.180.254.245	14.183.90.200	171.230.252.32	181.206.79.58	186.67.109.171	201.175.52.71	23.99.137.54	41.32.223.29	5.41.223.77	83.239.36.122
1.55.239.137	111.93.41.206	117.200.202.154	122.5.32.250	14.186.185.200	171.232.135.116	181.48.126.186	187.147.214.180	201.234.52.37	27.254.12.20	41.75.89.118	5.58.58.216	83.96.6.210
1.6.164.37	112.209.188.83	117.216.13.163	123.16.73.29	14.186.203.35	171.236.204.60	182.180.130.88	187.211.12.237	201.255.142.153	27.3.33.4	42.112.108.143	5.62.34.22	84.53.236.87
101.108.126.142	113.104.178.207	117.247.84.194	123.18.227.2	14.188.123.21	171.243.181.91	182.253.60.98	189.20.255.213	201.91.44.206	27.54.187.229	42.112.181.180	59.125.237.127	85.105.120.215
101.50.76.96	113.160.147.138	117.254.49.226	123.21.88.149	14.189.7.192	171.255.77.221	182.31.152.2	189.203.77.162	202.162.194.218	27.66.116.28	42.113.63.130	59.52.20.3	85.99.254.210
103.101.44.1	113.160.166.205	117.3.47.188	123.25.234.1	14.190.191.153	176.104.191.9	182.71.169.146	189.234.97.35	202.164.152.71	27.67.183.165	42.113.98.131	61.91.57.150	88.233.31.156
103.206.188.182	113.160.66.22	117.4.113.146	124.123.20.42	14.226.86.178	176.236.16.6	182.72.212.114	189.243.200.100	202.47.33.233	27.68.48.19	42.114.151.90	61.94.143.73	90.189.113.86
103.214.128.5	113.161.218.165	117.4.137.72	124.123.92.113	14.228.75.19	176.236.77.177	182.73.130.27	189.251.49.123	203.128.246.226	27.72.174.252	42.114.56.95	61.94.162.13	91.215.204.170
103.232.245.226	113.161.94.73	117.6.128.23	124.158.109.232	14.231.233.52	176.237.93.244	182.73.135.94	189.254.158.194	203.130.11.243	27.74.243.201	42.115.55.23	62.149.99.215	91.217.5.109
103.236.134.34	113.162.173.15	117.6.130.56	124.62.255.1	14.232.214.223	176.32.139.195	182.73.214.226	190.103.183.55	203.205.28.116	27.74.254.12	42.118.218.111	62.183.52.238	92.45.67.34
103.238.74.86	113.174.246.24	117.6.87.7	125.212.178.2	14.232.214.36	176.32.186.146	182.74.204.226	190.181.4.2	203.205.51.86	27.75.53.107	42.118.80.158	62.98.129.192	93.147.249.235
103.249.80.122	113.176.81.31	118.167.187.128	125.214.51.67	14.233.198.129	176.88.80.239	182.75.38.122	190.221.50.211	203.99.182.2	27.78.59.71	45.118.205.229	64.129.148.74	93.94.217.141
103.37.181.170	113.181.20.69	118.179.216.254	125.23.220.150	14.237.191.215	177.125.222.78	182.96.186.3	190.78.176.28	204.18.196.172	27.79.176.26	45.118.32.149	66.61.194.149	94.137.15.73
103.37.82.74	113.184.25.56	118.69.186.183	128.65.190.9	14.237.31.79	177.139.248.221	183.154.106.242	191.241.242.112	208.122.73.127	27.79.243.50	45.220.184.69	70.169.40.166	94.25.167.126
103.59.142.179	113.184.26.156	118.69.35.240	128.68.112.40	14.241.247.228	177.72.14.67	183.171.227.34	191.97.55.99	211.152.35.9	31.181.144.111	46.188.65.73	71.40.70.34	95.161.225.58
103.59.213.2	113.188.234.220	118.69.67.248	13.211.66.199	14.242.103.171	177.97.188.11	183.177.239.1	195.91.252.234	211.24.85.217	36.239.241.140	47.15.228.146	77.245.101.5	95.188.17.210
103.74.111.20	113.189.57.107	118.70.119.62	137.59.64.178	14.242.54.178	178.151.125.45	183.81.121.105	196.189.5.141	211.44.171.8	36.255.91.70	49.145.199.87	77.89.156.4	95.220.49.233
103.74.121.31	113.190.234.218	118.70.126.160	14.0.19.82	14.243.161.194	178.252.149.115	183.82.106.107	196.204.23.209	212.107.250.120	36.37.74.122	49.145.206.182	78.178.18.177	95.9.110.162
103.80.210.80	113.190.235.91	118.70.131.157	14.139.238.130	14.248.100.59	178.34.161.125	183.82.114.15	196.218.180.94	212.113.253.50	36.66.243.2	49.145.233.184	78.179.224.154	98.101.27.52
103.87.104.179	114.143.219.67	118.70.171.91	14.141.79.27	14.248.219.77	178.72.121.54	183.82.115.38	197.156.123.88	212.12.4.39	36.68.73.172	49.145.235.37	78.186.142.15	
103.88.126.229	114.43.151.59	118.70.184.247	14.143.53.14	14.248.80.107	179.108.113.125	183.82.131.44	197.50.105.85	212.45.14.158	36.71.234.133	49.146.36.199	78.188.165.215	
103.99.75.164	114.47.94.100	118.70.186.67	14.160.49.82	14.250.58.89	180.191.86.71	183.82.134.112	2.180.118.170	212.58.121.170	36.77.139.5	49.146.39.110	78.36.10.128	
106.51.72.112	115.166.140.190	118.70.42.79	14.162.201.100	14.253.158.35	180.211.243.254	183.83.171.243	2.91.153.119	213.55.90.49	36.80.70.133	49.146.43.177	78.36.138.157	
109.165.44.5	115.78.1.36	118.71.97.34	14.162.4.19	14.254.229.76	180.241.44.233	183.89.160.103	2.92.14.64	217.118.14.40	36.82.101.38	49.149.107.98	78.39.233.172	

Hash

ae12bb54af31227017feffd9598a6f5e
414a3594e4a822cfb97a4326e185f620
0ab2aeda90221832167e5127332dd702
996c2b2ca30180129c69352a3a3515e4
cd99e5e4f44621978faf8df0e01d2d2b
ce494e90f5ba942a3f1c0fe557e598bf
95ae8e32eb8635e7eabe14ffbfaa777b
6e72ad805b4322612b9c9c7673a45635
a4d49eaf60a8e333708469606ad9e1a4
2f76b88b420003516f90062940ef7881
8fa0e5dd92185799b73cbfab3da3e919
cf4f46336abeec03630297f846d17482
e9d1ba0ee54fcdf37cf458cd3209c9f3
a48ca7b40ab2a6ebdd94dbd52164c6cf
33d373e264dc7fdb0bcdbd8e075a6319
50b93e08b91de26b5487abe79afe1d4a
1037d7e765377bcee9de808ba80753f2
1a6a8bac6fa32599a5d446977079f3b0

58a20a3827a0e27c337fce30efacce7b
7823636f9ce01306178c1ee7772ad831
9155183e0b2031ba0c7159f76840ffed
9aae6412b2dfc9ed503e6c7123e95579
b016a2d5e8963fb6bb1f810502e1562f
bcf9302e2998ce0f4a783237c90d1112
e5840a9753ed8f90fbd7264c8db27c4b
f7885b1000767b585a2604bdeab98498
01bdc6fb077098f4a3b60f4b0e479a7f
094950cccbbdc8b9a3661d3c43bb940e
0e80a07bf580016d84894dcef82a8f55
1bda83265aeaeda718ef23fca3e1fe8d
1f2a546e40d29e90707c574f9656054a
2178bd43ffa9dc3708702c9c6867f023
248200829c1a5eb111b12c2bb0818ff8
30e3f8ebb578da4247b6bf7e43beda36
312a0b021749822bd4e58fdbe3275c21
3695f6d3175e85e25ea3cc65ab3801cf

398c9ce412840482219a86730d9853f1
43d1b7c9d0a2ad17457ef6199c16a6c6
47bc7c8f1ac38746f74e543a4c421d75
49a24e8288fd725f37f6bbea56974f0a
4fbfa754204df11c5d7d4d76bb4b777f
541244c6529f99813eae1f884512a978
54dd9593fb858bb8b1a77fe5e9238ae2
58244389501ed08823b6c50702efca46
5ffdc8b7825f72a04d5c97b6a4d80e7e
62186bebffffcfafb1c70a8ff03fa317
6350f8da991da9ee85c63e15cce88fbb
65d4907f54faebb3b1e1178235acb986
6633a19602561d359e76a67a008d62e8
6a139899acde9af3c79c024bee1a800b
74896a9964bdcd24cdc3375f7b7e2482
79752fabcc6d2b305510531b0c998f6c
7da3c3d5e15c486334ce0b1d0325026c
7f1d353278ff9f75819009e0b4df84ca

82fd236a238401d22a81802040988580
8765a22a8b6da7e4a45849b90249eb65
8d340ce819b42f0c5a27753dd7170ff9
917622dd22d73f7c36f3af6a0eeb9a2b
96b11451d63b36111ba78a37532e97f3
978fcc48a006c05c94e626ccb2ddfe53
98df58e71b5202e49ba6f9e6e43ef6ef
9aa42e3fba9d860fd23c3dc54cf65d0b
9ba5379aa41d707a4331d27a004baec1
9de48d5fbc876dde8133e62e88e8d68c
a297ec94785cdf9c33225a24041477d3
a817c68ceb7be5ad467dad8c70391662
ac8aabd6a5c8a2472097ebf0d55b2cfb
bdcaf7ef34cd9b02932e5ee2297e4893
bf137d87e79f68177dd1eb0b780a35e4
c2b3f51728001fbaaa5a73fcaf3e1a68
c4478726a4d2110e1eb0a12f79de6e36
c475b82f1e0b421e051622f034b1d5e3

c96b8c08aa8c7177a82b22d898eb1d79
c9fd6166b9ec194215ff94e7b41c0ade
caf082a135af8d966e8dc7fb9f619bba
cb91d2e7317ec79536b3a4f5bf066785
da5eee93accd46fe8755b93a19ada407
daf7e72c18545d74aa1cdcdd6b306dc7
dd33dbc6c0832e4c8c8aec39b49eb4ab
e8dadbed82f4fe52e93c907b955845ea
edc7790ce477938713183f7a441d1298
ef4df7aa5b6901a1e5aad776c2d87912
ef7830b025d48ebe98a692b14acf4c01
f4467cf9b7f5c536f0766ac2851b53b7
f48d512a5502f8d32554f1c762a84836
f7b1bd2aa9ce09a273243560db7bad8a
f7c11071b3bf039f237468dd04959a88
fcb6b0f95853dfda72d5535a424b3a29

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

112.78.133.170 188.165.195.174 51.255.140.235 58.137.160.233
180.178.108.107 203.210.84.63 51.255.29.165

Hash

474ecb2fac7ef6f1b798d81d8a3ba5a2 685bc2af410d86a742b59b96d116a7d9
0cad216d1be79f216e76bb561bb0f67f

Reference

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

c. 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 [4].

IP

104.148.42.209 23.228.113.117
107.179.31.66 23.228.113.244

Hash

c663827b1cf068ff2e2b1a731bbf2826 8c8da16a2b9e7c318a9544ff032bddbe 28b4c1d34913014f2ea43298db493216
42ba80053b0e744346236592b01949d0 2004f9f08f281f8d4ea7c913573dd6cc 3e34bff8e13cf6068f4a30218b55b549
b9cb431c103bd716493a7b70133012de 232e172f7a005dd12d4aad55e0c4a331

Reference

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

d. 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[5].

IP

84.22.47.122

Hash

4afa19658700de6d038b30f3376b462d

Reference

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

e. Linux.Morila – Severity: High

This Trojan download and install other programs, including malware into the user PC without user consent [6].

IP

112.133.227.107

Hash

de055a28c11134dd59114343b51ecba1

Reference

[6] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:Linux/Morila!MTB&threatId=-2147221724

f. 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 [7].

IP

1.172.46.54	109.70.184.50	188.163.81.92	220.142.42.165
102.184.87.118	114.198.174.230	195.3.247.250	42.187.121.111

Hash

ca71f8a79f8ed255bf03679504813c6a

References

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

g. Zombieboy – Severity: High

Zombieboy is a trojan horse that may perform malicious activities on the compromised computer [8].

IP

1.55.142.136	120.29.77.211	202.131.232.34	77.28.243.36
110.137.80.230	128.69.46.231	37.224.20.33	84.235.90.201
116.212.48.247	14.185.185.82	46.180.230.53	91.205.128.233
117.1.249.200	149.202.100.241	77.235.118.169	94.97.127.87

Hash

26f0446df04e1097f5575445fc0e6787 f70557802f671ae027d602d2bd3fd6cf
8c81ab1ed40c6a1b1d359b305c1c8d7d

Reference

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

Appendix 1: List of MD5 Malware Hashes

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	ae12bb54af31227017feffd9598a6f5e	120
		414a3594e4a822cfb97a4326e185f620	67
		0ab2aeda90221832167e5127332dd702	48
		996c2b2ca30180129c69352a3a3515e4	48
		cd99e5e4f44621978faf8df0e01d2d2b	11
		ce494e90f5ba942a3f1c0fe557e598bf	9
		95ae8e32eb8635e7eabe14ffbfaa777b	8
		6e72ad805b4322612b9c9c7673a45635	6
		a4d49eaf60a8e333708469606ad9e1a4	6
		2f76b88b420003516f90062940ef7881	5
		8fa0e5dd92185799b73cbfab3da3e919	5
		cf4f46336abeec03630297f846d17482	5
		e9d1ba0ee54fcdf37cf458cd3209c9f3	5
		a48ca7b40ab2a6ebdd94dbd52164c6cf	4
		33d373e264dc7fdb0bcdbd8e075a6319	3
		50b93e08b91de26b5487abe79afe1d4a	3
		1037d7e765377bcee9de808ba80753f2	2
		1a6a8bac6fa32599a5d446977079f3b0	2
		58a20a3827a0e27c337fce30efacce7b	2
		7823636f9ce01306178c1ee7772ad831	2
		9155183e0b2031ba0c7159f76840ffed	2
		9aae6412b2dfc9ed503e6c7123e95579	2
		b016a2d5e8963fb6bb1f810502e1562f	2
		bcf9302e2998ce0f4a783237c90d1112	2
		e5840a9753ed8f90fbd7264c8db27c4b	2
		f7885b1000767b585a2604bdeab98498	2
		01bdc6fb077098f4a3b60f4b0e479a7f	1
		094950cccbbdc8b9a3661d3c43bb940e	1
		0e80a07bf580016d84894dcef82a8f55	1
		1bda83265aeaeda718ef23fca3e1fe8d	1
		1f2a546e40d29e90707c574f9656054a	1
		2178bd43ffa9dc3708702c9c6867f023	1
		248200829c1a5eb111b12c2bb0818ff8	1
		30e3f8ebb578da4247b6bf7e43beda36	1
		312a0b021749822bd4e58fdbe3275c21	1
		3695f6d3175e85e25ea3cc65ab3801cf	1

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	398c9ce412840482219a86730d9853f1	1
		43d1b7c9d0a2ad17457ef6199c16a6c6	1
		47bc7c8f1ac38746f74e543a4c421d75	1
		49a24e8288fd725f37f6bbea56974f0a	1
		4fbfa754204df11c5d7d4d76bb4b777f	1
		541244c6529f99813eae1f884512a978	1
		54dd9593fb858bb8b1a77fe5e9238ae2	1
		58244389501ed08823b6c50702efca46	1
		5ffdc8b7825f72a04d5c97b6a4d80e7e	1
		62186bebffffcfafb1c70a8ff03fa317	1
		6350f8da991da9ee85c63e15cce88fbb	1
		65d4907f54faebb3b1e1178235acb986	1
		6633a19602561d359e76a67a008d62e8	1
		6a139899acde9af3c79c024bee1a800b	1
		74896a9964bdcd24cdc3375f7b7e2482	1
		79752fabcc6d2b305510531b0c998f6c	1
		7da3c3d5e15c486334ce0b1d0325026c	1
		7f1d353278ff9f75819009e0b4df84ca	1
		82fd236a238401d22a81802040988580	1
		8765a22a8b6da7e4a45849b90249eb65	1
		8d340ce819b42f0c5a27753dd7170ff9	1
		917622dd22d73f7c36f3af6a0eeb9a2b	1
		96b11451d63b36111ba78a37532e97f3	1
		978fcc48a006c05c94e626ccb2ddfe53	1
		98df58e71b5202e49ba6f9e6e43ef6ef	1
		9aa42e3fba9d860fd23c3dc54cf65d0b	1
		9ba5379aa41d707a4331d27a004baec1	1
		9de48d5fbc876dde8133e62e88e8d68c	1
		a297ec94785cdf9c33225a24041477d3	1
		a817c68ceb7be5ad467dad8c70391662	1
		ac8aabd6a5c8a2472097ebf0d55b2cfb	1
		bdcaf7ef34cd9b02932e5ee2297e4893	1
		bf137d87e79f68177dd1eb0b780a35e4	1
		c2b3f51728001fbaaa5a73fcaf3e1a68	1
		c4478726a4d2110e1eb0a12f79de6e36	1
		c475b82f1e0b421e051622f034b1d5e3	1

Appendix 1: List of MD5 Malware Hashes

Type	Malware Name	Malware Hash	Detection
Ransomware	WannaCry	c96b8c08aa8c7177a82b22d898eb1d79	1
		c9fd6166b9ec194215ff94e7b41c0ade	1
		caf082a135af8d966e8dc7fb9f619bba	1
		cb91d2e7317ec79536b3a4f5bf066785	1
		da5eee93accd46fe8755b93a19ada407	1
		daf7e72c18545d74aa1cdcdd6b306dc7	1
		dd33dbc6c0832e4c8c8aec39b49eb4ab	1
		e8dadbed82f4fe52e93c907b955845ea	1
		edc7790ce477938713183f7a441d1298	1
		ef4df7aa5b6901a1e5aad776c2d87912	1
		ef7830b025d48ebe98a692b14acf4c01	1
		f4467cf9b7f5c536f0766ac2851b53b7	1
		f48d512a5502f8d32554f1c762a84836	1
		f7b1bd2aa9ce09a273243560db7bad8a	1
		f7c11071b3bf039f237468dd04959a88	1
		fcb6b0f95853dfda72d5535a424b3a29	1
Trojan Downloader	Small	474ecb2fac7ef6f1b798d81d8a3ba5a2	102
		0cad216d1be79f216e76bb561bb0f67f	23
		685bc2af410d86a742b59b96d116a7d9	9
	Linux.XorDdos	c663827b1cf068ff2e2b1a731bbf2826	4
		42ba80053b0e744346236592b01949d0	3
		b9cb431c103bd716493a7b70133012de	3
		8c8da16a2b9e7c318a9544ff032bddbe	2
		2004f9f08f281f8d4ea7c913573dd6cc	1
		232e172f7a005dd12d4aad55e0c4a331	1
		28b4c1d34913014f2ea43298db493216	1
		3e34bff8e13cf6068f4a30218b55b549	1
	Occamy	4afa19658700de6d038b30f3376b462d	1
	Linux.Morila	de055a28c11134dd59114343b51ecba1	1
Cryptocurrency Mining	Zombieboy	26f0446df04e1097f5575445fc0e6787	14
		8c81ab1ed40c6a1b1d359b305c1c8d7d	1
		f70557802f671ae027d602d2bd3fd6cf	3
	Tiggre	ca71f8a79f8ed255bf03679504813c6a	27
		Total	632