Malware Research and Coordination Facility Project

Monthly Trend Report

JANUARY 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 191 devices. It involves data unavailability, data breaches, and backdoor activities. The list of captured malware consists of WannaCry, Occamy, Small, Swisyn, Linux.XorDdos, Zombieboy and Tiggre.

The main threat is the WannaCry malware with 150 malwares captured. This is followed by Tiggre with 19 malwares captured; Occamy with 8 malwares captured; Swisyn with six (6) malwares captured; Small with four (4) malwares captured; and finally, the Linux.XorDdos and Zombieboy malware with 2 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

Swisyn Small

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

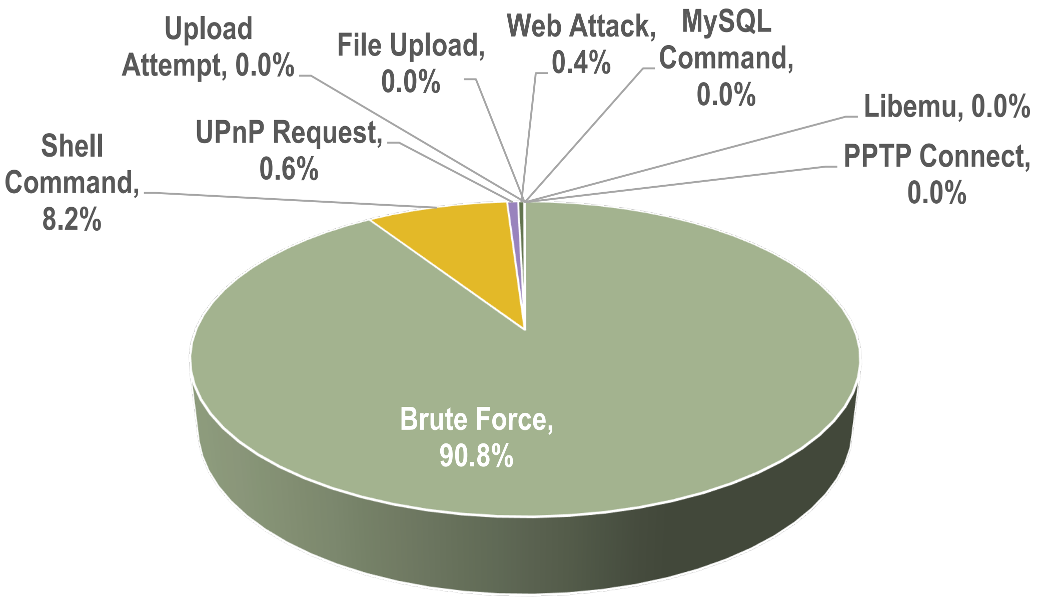

Figure 1 Attack Types

Figure 1 above illustrates the statistics of attack types recorded in January 2020. Based on Figure 1, Brute Force recorded the highest attack with 90.8%, followed by Shell Command attack with 8.2% and UPnP Request with 0.6%.

Table 1 Attack Types

ATTACK TYPE	TOTAL
Brute Force	22,401,776
Shell Command	2,015,154
UPnP Request	156,315
Web Attack	86,605
File Upload	7,556
MySQL Command	2,342
Libemu	405
Upload Attempt	166
PPTP Connect	17
MQTT Publish	6

Targeted Services

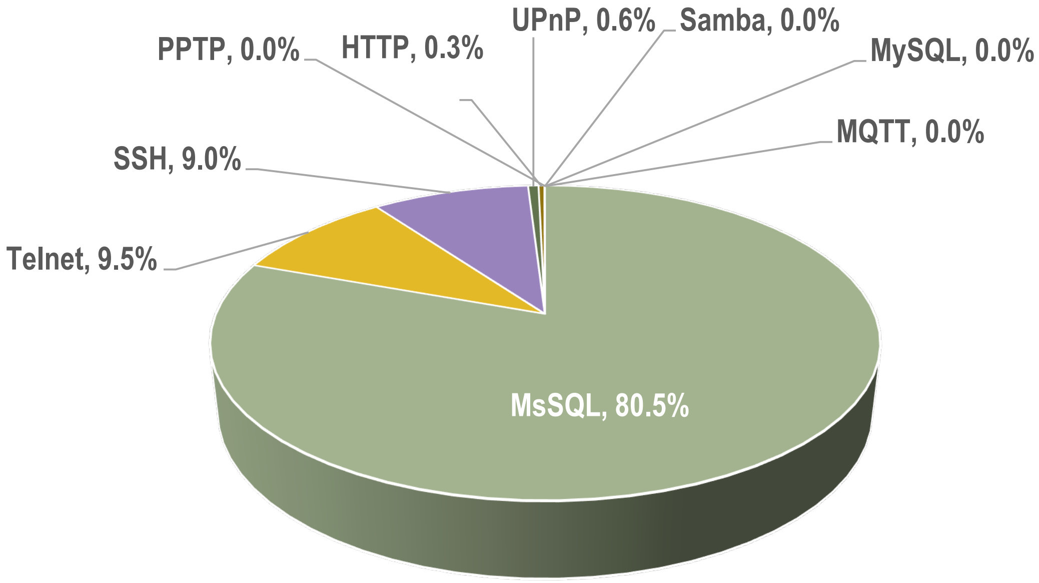

Figure 2 Targeted Services

In Figure 2, nine (9) targeted services data are recorded during in January 2020. From Table 2 on the right, MsSQL became the main target with 20,804,150 or 80.5% closely followed by Telnet (9.5%) and SSH (9.0%). MQTT is at bottom with only 6 attacks logged.

Table 2 Targeted Services

TARGETED SERVICES	TOTAL
MsSQL	20,804,150
Telnet	2,445,214
SSH	2,337,033
UPnP	156,315
HTTP	86,605
Samba	6,078
MySQL	2,505
PPTP	17
MQTT	6

Top Malware Detected

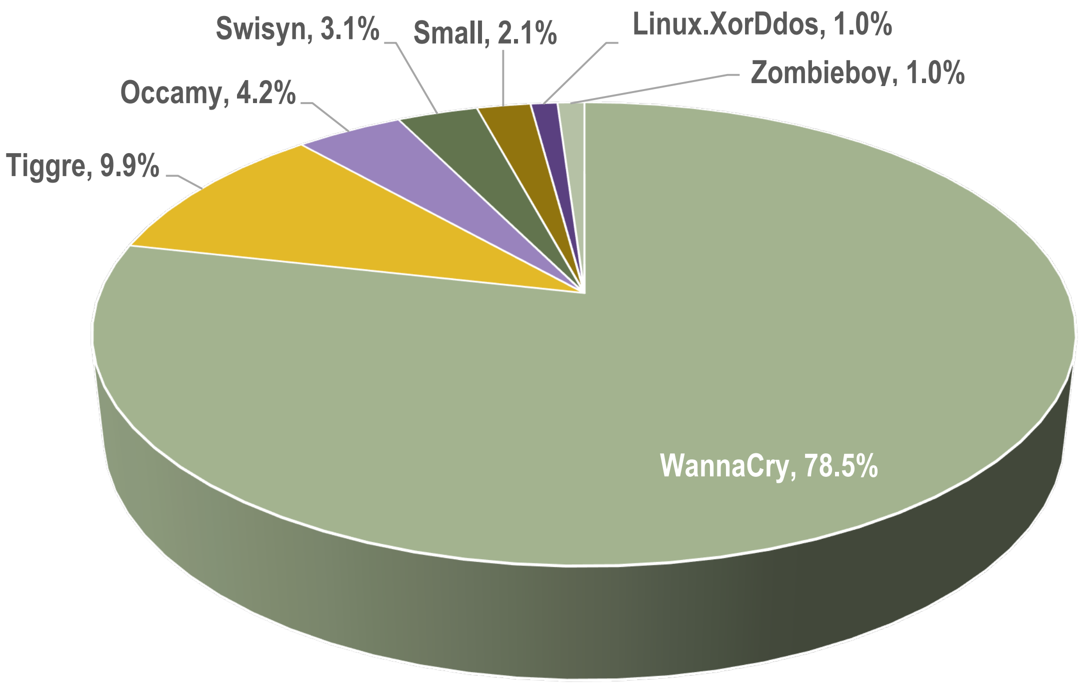

Figure 3 Detected Malwares

Table 3 Malwares Counts

MALWARE TYPE	MALWARE NAME	SEVERITY	EVENT COUNT
Ransomware	WannaCry	High	150
Trojan Downloader	Occamy	High	8
	Swisyn	High	6
	Small	High	4
	Linux.XorDdos	High	2
Cryptocurrency Mining	Tiggre	High	19
	Zombieboy	High	2

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 150 detections. The ransomware captured is WannaCry having a total of 63 unique hashes. This month, cryptocurrency mining malware become second impact to the detection count with 21 detections; Tiggre (19 detections, 1 unique hash) and Zombieboy (2 detections, 1 unique hash) . The lowest detection count is the trojan downloader malware type with 20 detection count by the sensors; Occamy (8 detections, 3 unique hashes), Swisyn (6 detections, 1 unique hash), Small (4 detections, 1 unique hash) and Linux.XorDdos Small (2 detections, 1 unique hash) . 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

2.136.58.69
2.228.94.52
5.117.218.0
5.123.186.187
5.125.45.97
5.236.62.136
14.139.253.18
14.161.40.66
14.171.96.2
14.187.136.189
14.188.113.176
14.190.215.69
27.74.232.57
36.84.63.141
36.227.80.12
36.228.229.103
36.234.211.35
37.194.54.206
42.112.112.62
42.112.156.70
43.229.88.101
45.113.248.131
45.124.144.130
46.34.133.82
49.145.235.167
49.146.45.100
49.149.101.101
49.206.10.32
59.145.184.74
61.2.64.81
61.5.55.22
70.63.90.254
77.94.106.91
78.154.170.232
91.185.16.130
92.45.67.34
95.174.125.239
98.113.35.10
101.99.13.45
103.8.125.194
103.82.80.46
103.82.211.64
103.95.48.210
103.199.161.79
103.203.254.118
103.209.81.22
110.137.178.180
111.92.87.174
112.133.237.17
113.170.158.160
113.176.95.154
113.176.107.26
114.57.46.136
114.143.182.230
115.127.39.21
116.103.150.87
116.193.223.164
117.0.33.174
117.97.132.218
117.193.35.208
117.207.37.124
117.207.43.230
117.213.84.34
117.216.142.193
117.254.108.76
118.68.122.30
118.69.37.1
118.69.70.169
118.69.234.227
119.15.86.186
119.92.10.161
119.94.155.209
119.148.35.142
119.153.135.180
122.53.62.20
122.54.17.194
122.170.12.200
122.176.105.159
123.18.108.67
123.25.30.79
150.107.222.74
151.254.129.251
157.37.202.78
164.100.131.125
171.4.236.231
171.6.229.192
171.243.62.12
171.243.240.192
177.23.119.254
177.72.44.196
177.73.101.24
177.107.192.6
177.155.185.221
180.241.45.181
180.241.132.165
182.253.11.234
183.82.57.106
183.83.167.64
184.7.187.7
186.91.137.29
186.251.79.132
187.155.91.238
187.188.172.70
190.64.95.85
200.29.238.60
200.49.60.66
200.161.117.65
200.201.199.178
200.250.55.145
201.24.82.11
201.123.167.25
201.208.113.221
201.245.200.122
202.57.45.50
202.83.56.20
202.83.56.106
202.88.250.74
202.93.115.51
202.137.154.82
202.142.151.162
202.164.148.36
203.125.217.54
207.236.104.37
210.212.78.34
210.245.34.243
211.181.237.98
221.120.32.118
222.252.15.39
222.254.3.16

Hash

ae12bb54af31227017feffd9598a6f5e
996c2b2ca30180129c69352a3a3515e4
414a3594e4a822cfb97a4326e185f620
0ab2aeda90221832167e5127332dd702
01bdc6fb077098f4a3b60f4b0e479a7f
a55b9addb2447db1882a3ae995a70151
a080ecd5cc48a42109d1a03128ea90a6
cd99e5e4f44621978faf8df0e01d2d2b
3695f6d3175e85e25ea3cc65ab3801cf
a48ca7b40ab2a6ebdd94dbd52164c6cf
a4d49eaf60a8e333708469606ad9e1a4
cf4f46336abeec03630297f846d17482
0326939d808f643b84bf516bb5cda218
033f9150e241e7accecb60d849481871
25990c829fa369b05d21c703edcc0624
33d373e264dc7fdb0bcdbd8e075a6319
398c9ce412840482219a86730d9853f1
39bad8f8d12a85f702891410b4e4a9e2
50b93e08b91de26b5487abe79afe1d4a
541244c6529f99813eae1f884512a978
58244389501ed08823b6c50702efca46
59136488b3b15c68244b31364f4eef97
5975054f96498f327e56c6cdcd24262c
5e83e812b06dd9d119c19cf03bb91a73
61334e77886abc4581ab37acfece1ffe
6350f8da991da9ee85c63e15cce88fbb
6e72ad805b4322612b9c9c7673a45635
8e6bfea06cb00553ee29b3822b349bd6
93f39d086beb478188bbd19ba1781382
95ae8e32eb8635e7eabe14ffbfaa777b
9c61679a214951336986efd07b59b8dd
b59a18f991d197e53b4305a571a331b5
bdcaf7ef34cd9b02932e5ee2297e4893
befc3ffc686d5c4b9f7b5c3d6966afae
c3a45f95679ec04abd7322ea9fe51755
caac065b2034b4bcecfdfebb6280b749
ce494e90f5ba942a3f1c0fe557e598bf
ceb4280d81cb4039295d5133c2520026
cfc424c730afcd48b93cbd3afddc16fc
d21f57481eb3463e5d0077ed2c4b019e
d25171479677bde36fba4f25c44bd851
d445e2e0b050ee7127cbe72fe13ee2b4
dee385512069d92fa4f4c84eed132415
dfac55e674f9d62589cd531ffe25fcac
e13c5a2cf223c57b61d71409218589cc
e49594ffa18e330c8692d88dc8e73752
e9d1ba0ee54fcdf37cf458cd3209c9f3
feae26f17da20dcf2f3b92c1e1384b0c
fecedeedc700847c52753f372c6b6357

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. 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[3].

IP

185.199.24.26
78.189.76.12
115.159.95.245
87.116.177.214

Hash

8831cfc4b15416f07eb34d944641e179
71fc738c05f995c28f0e18081c420e0c
4afa19658700de6d038b30f3376b462d

Reference

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

c. Swisyn – Severity: High

SWISYN is a Trojan family first spotted around 2009. It is known primarily as a malware that drops other malware and executes them on the system it affects. This causes the affected system to display the malicious routines of the dropped malware. SWISYN is also known to connect to possibly malicious URLs, as well as create registry entries in order to ensure its activation upon system startup [4].

IP

51.255.140.235

Hash

474ecb2fac7ef6f1b798d81d8a3ba5a2

Reference

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

d. 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 [5].

IP

113.161.210.170
115.74.215.136

Hash

685bc2af410d86a742b59b96d116a7d9

Reference

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

e. 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 [6].

IP

23.228.113.117

Hash

3e34bff8e13cf6068f4a30218b55b549

Reference

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

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

180.200.48.230
187.217.207.27
36.91.191.169
60.249.206.148
49.206.27.3

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

155.94.164.154
85.23.121.228

Hash

26f0446df04e1097f5575445fc0e6787

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	47
		996c2b2ca30180129c69352a3a3515e4	18
		414a3594e4a822cfb97a4326e185f620	14
		0ab2aeda90221832167e5127332dd702	12
		01bdc6fb077098f4a3b60f4b0e479a7f	4
		a55b9addb2447db1882a3ae995a70151	4
		a080ecd5cc48a42109d1a03128ea90a6	3
		cd99e5e4f44621978faf8df0e01d2d2b	3
		a48ca7b40ab2a6ebdd94dbd52164c6cf	2
		a4d49eaf60a8e333708469606ad9e1a4	2
		cf4f46336abeec03630297f846d17482	2
		3695f6d3175e85e25ea3cc65ab3801cf	2
		398c9ce412840482219a86730d9853f1	1
		39bad8f8d12a85f702891410b4e4a9e2	1
		9c61679a214951336986efd07b59b8dd	1
		0326939d808f643b84bf516bb5cda218	1
		033f9150e241e7accecb60d849481871	1
		25990c829fa369b05d21c703edcc0624	1
		33d373e264dc7fdb0bcdbd8e075a6319	1
		50b93e08b91de26b5487abe79afe1d4a	1
		541244c6529f99813eae1f884512a978	1
		58244389501ed08823b6c50702efca46	1
		59136488b3b15c68244b31364f4eef97	1
		5975054f96498f327e56c6cdcd24262c	1
		5e83e812b06dd9d119c19cf03bb91a73	1
		61334e77886abc4581ab37acfece1ffe	1
		6350f8da991da9ee85c63e15cce88fbb	1
		6e72ad805b4322612b9c9c7673a45635	1
		8e6bfea06cb00553ee29b3822b349bd6	1
		93f39d086beb478188bbd19ba1781382	1
		95ae8e32eb8635e7eabe14ffbfaa777b	1
		cfc424c730afcd48b93cbd3afddc16fc	1
		d21f57481eb3463e5d0077ed2c4b019e	1
		d25171479677bde36fba4f25c44bd851	1
		d445e2e0b050ee7127cbe72fe13ee2b4	1
		dee385512069d92fa4f4c84eed132415	1
Ransomware	WannaCry	dfac55e674f9d62589cd531ffe25fcac	1
		e13c5a2cf223c57b61d71409218589cc	1
		e49594ffa18e330c8692d88dc8e73752	1
		e9d1ba0ee54fcdf37cf458cd3209c9f3	1
		feae26f17da20dcf2f3b92c1e1384b0c	1
		fecedeedc700847c52753f372c6b6357	1
		ce494e90f5ba942a3f1c0fe557e598bf	1
		ceb4280d81cb4039295d5133c2520026	1
		b59a18f991d197e53b4305a571a331b5	1
		bdcaf7ef34cd9b02932e5ee2297e4893	1
		befc3ffc686d5c4b9f7b5c3d6966afae	1
		c3a45f95679ec04abd7322ea9fe51755	1
		caac065b2034b4bcecfdfebb6280b749	1
Trojan Downloader	Occamy	8831cfc4b15416f07eb34d944641e179	4
		71fc738c05f995c28f0e18081c420e0c	3
		4afa19658700de6d038b30f3376b462d	1
	Small	685bc2af410d86a742b59b96d116a7d9	4
	Swisyn	474ecb2fac7ef6f1b798d81d8a3ba5a2	6
	XorDdos	3e34bff8e13cf6068f4a30218b55b549	2
Cryptocurrency Mining	Tiggre	ca71f8a79f8ed255bf03679504813c6a	19
	Zombieboy	26f0446df04e1097f5575445fc0e6787	2
		Total	191