MALWARE TREND REPORT

H1 2020

JANUARY - JUNE 2020

TABLE OF CONTENT

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, the Permanent Secretariat of the Organisation of the Islamic Cooperation – Computer Emergency Response Team **(OIC-CERT)**, shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Information on the malware trend is made available by CyberSecurity Malaysia for the purposes of providing awareness and improving the preparedness and readiness in facing malware threats.

The logo and names of organizations and products mentioned herein are the trademarks of their respective owners. The use of the logo and name do not imply any affiliation with or endorsement by the respective organizations.

THE OIC-CERT MALWARE TREND REPORT H1 2020

The OIC-CERT Malware Trend Report is a series of reports produced half yearly for the Malware Research and Coordination Facility Project (the Project). The Project is a collaborative effort of the Organisation of the Islamic Cooperation – Computer Emergency Response Team **(OIC-CERT)**, the Asia Pacific Computer Emergency Response Team **(APCERT)** and other organisations from various countries. The Project is an initiative by CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT. The background of the Project and the participating agencies / organisations is listed in "About the Project" section at the end of this report.

This Malware Trend Report published covering the period of 1 January 2020 until 30 June 2020.

INTRODUCTION

As the COVID-19 pandemic is likely affected everyone, malware and other cyber threats have also drastically increase. Malware is a malicious software intended to cause harm to the user system or network. Each malware has various capabilities in order to cause changes/damage to the infected system or network such as the ability to spread itself in the network and remain undetectable. They can bring down the machine's performance to knees and can cause a destruction of the network. Consider the case when the computer becomes infected and is no longer usable, the data inside becomes unavailable – these are some of the malware damage scenarios. Malware attacks can be traced back to the time, even before the internet became widespread.

LebahNet is one of the initiatives from CyberSecurity Malaysia to carried out research and gather data of malware trends and activities. Thus, the development of LebahNet is to monitor malware threats, give awareness to the public, and for the IT security authority to act based on the shared information.

OBJECTIVES

This report aims to provide a better understanding of the malware threats and analysis as well as the related potential impacts mainly within the participants' community. The objective is to educate and improve awareness, preparedness, and readiness in facing cyber threats.

TARGET AUDIENCE

The malware threat analysis presented in this report is primarily for the consumption of the Project participants and the general Internet users.

TOP ATTACK TYPE

Cyber-attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer device; using various methods to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin privileges on it. Based on the history of famous battles, none of their battle tactics are exactly alike. Still, there are similarities between the strategies and tactics often used as they are time-proven to be effective. Similar to cyber-attacks, when an attacker is trying to gain access to an organization, they will not invent new wheels unless they absolutely have to do it. The attacker will draw upon common types of hacking techniques that are known to be highly effective.

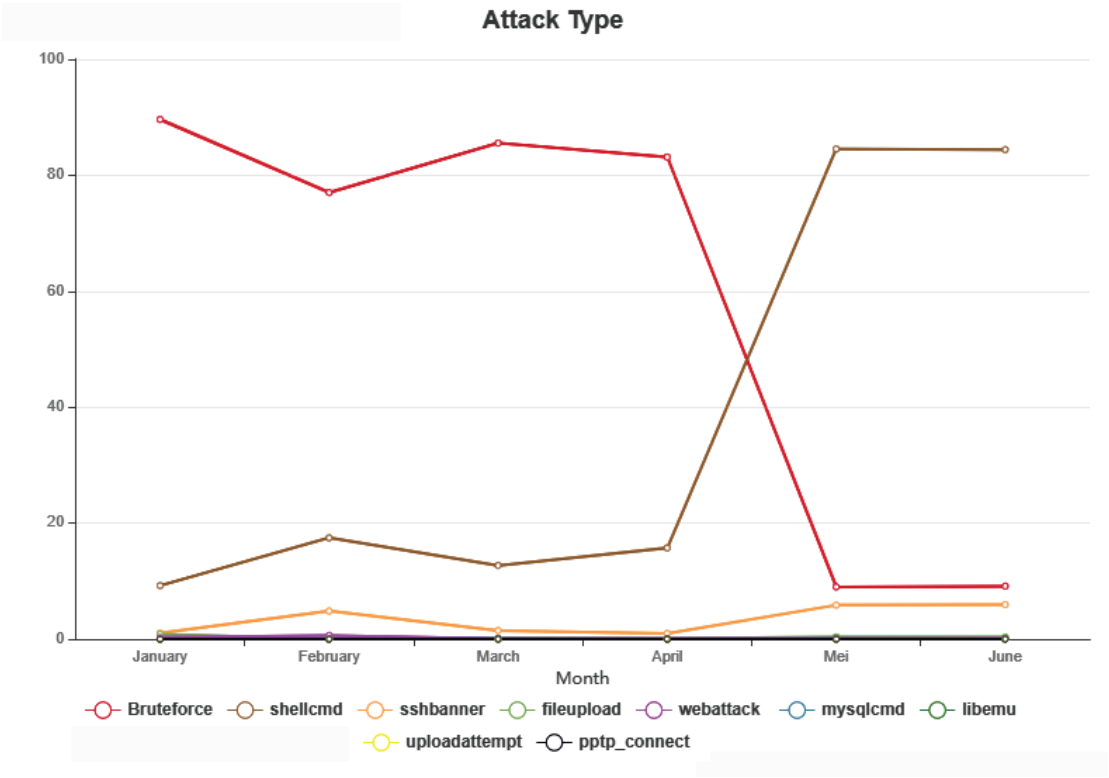

Figure 1 : Top Attack Type

Figure 1 above illustrates the statistics of top attack types logged for the Project from January to June 2020. Based on Figure 1, attacks using Bruteforce was recorded as the highest attack for January until April but dropped drastically for May and June while Shellcmd attack showed an increase in April until May. Figure 1 also illustrated that the Shellcmd attacks and Brute Force attacks are in inverse number. sshbanner attacks showed an increase in May.

THREAT ORIGIN (TOP 10)

Threat origin refers to the malicious traffic by country. However, the attacker may not necessary stay in the same country where the traffic is sent. The origin of the attack is driven by the mechanisms available to the bad actor. Cyber criminal or attacker might not expose their real IP address or location, keep in mind that many sophisticated computer hackers will be more cautious about tracing their steps. They will use a proxy to keep their location remain hidden and anonymous, so the data might not show the real location of the attacker but only show the origin of the network traffic performed by the attacker. The country that placed at the top maybe due to the robust networks and volume of devices within its borders. For malicious traffic by country of origin, the monthly data is as below.

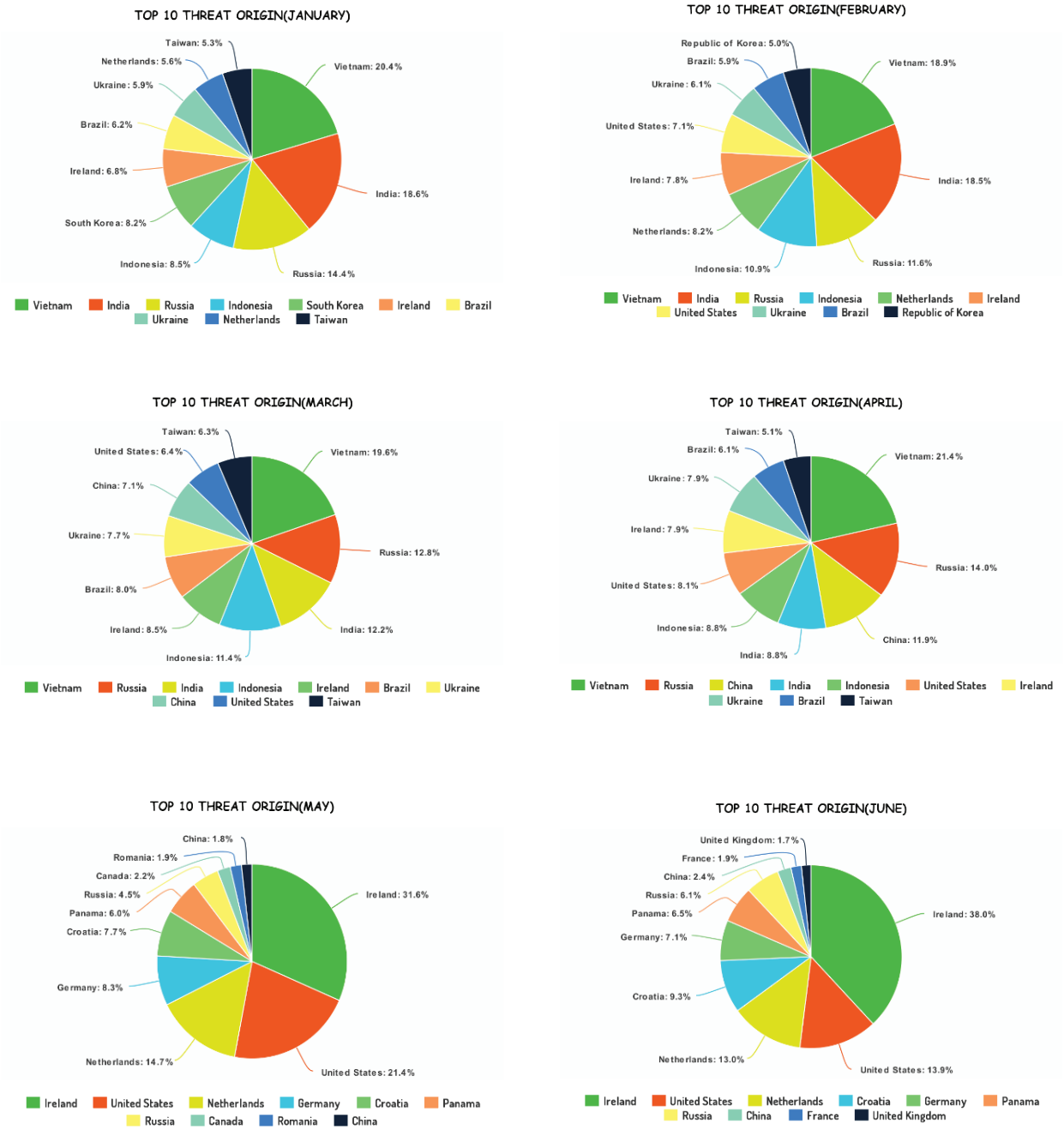

Figure 2 : Threat Origin

Figure 2 shows the top 10 of origin of threats for each month from January to June 2020. As stated before, kindly note that the attacker may not be in the same country where the traffic is sent as the attacker may be using infrastructure in the country to launch the attack.

TARGETED SERVICES

The computer network technology is developing rapidly, and the development of internet technology is more quickly, people are more aware of the importance of the network security. Network security is one of the main issues of computing because the attacker today is utilizing network services to gain access to the targeted organization.

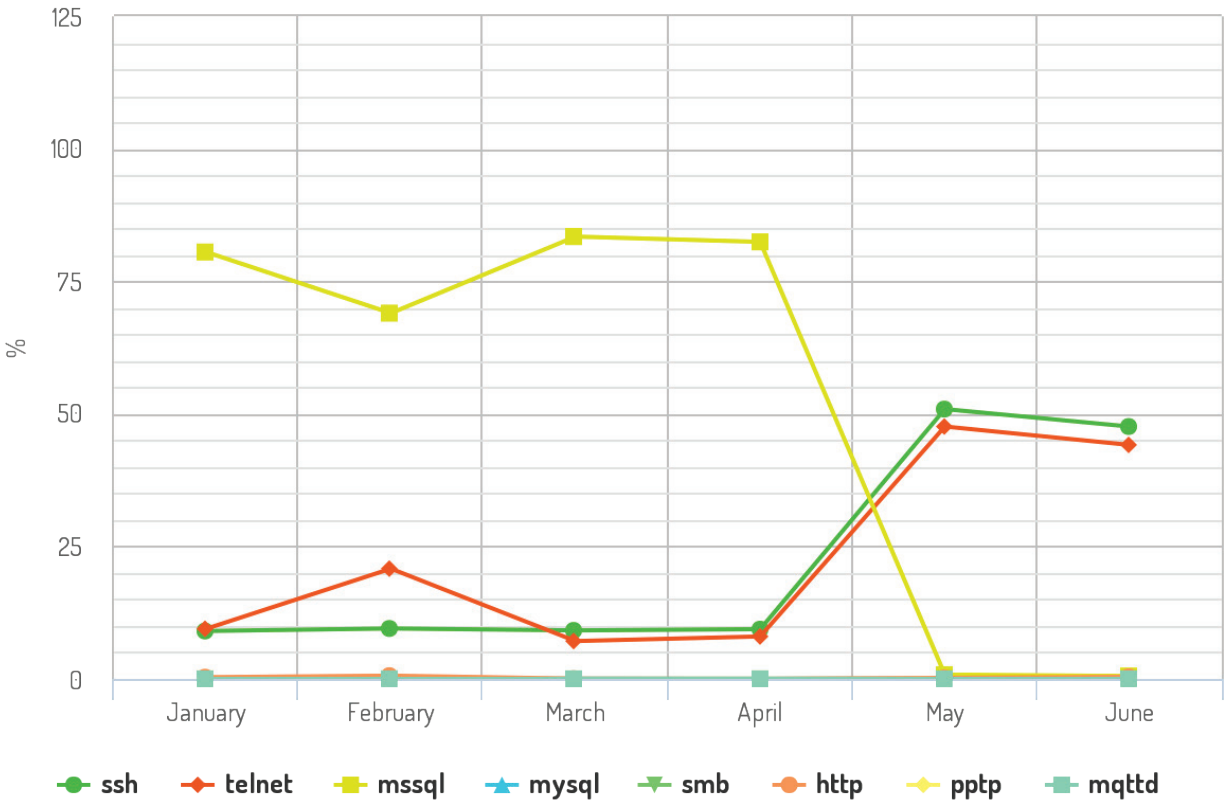

Figure 3: Overview of the targeted network services

As threats increase in volume and intensity, various network service will provide more opportunity for an attacker to gain access to targeted system. Figure 3 shows the type of services that were attacked from January to June 2020. Mssql is the highest targeted service from January until April while SSH and Telnet become the highest targeted services in May with 50.89% and 47.60% respectively. On June 2020, SSH and Telnet still become the highest targeted service with 54.50% and 44.14% respectively.

TOP 10 PASSWORD

A password is a set of character to authenticate a user to a digital system. Based on the statistics from January to June 2020, the attacker Brute force a system authentication based on a collection of passwords. Based on the trend of passwords used by attacker, “admin”(38.82%) is the most used password by attacker to brute force a system followed by “solokey’(27.65%) and “tsgoingon”(3.99%).

The Project also captured the passwords used by attackers. The results in Table 1 below list the regularly used passwords in attempts to breach the system to access sensitive information.

Password	Percentage (%)
admin	38.82%
solokey	27.65%
tsgoingon	3.99%
{blank}	3.45%
taZz@23495859	3.29%
connect	3.18%
download	2.22%
tor	2.05%
kernal	2.02%
vizxv	1.77%

Table 1: Top 10 Password

MALWARE BINARY

Table 2 shows the summary of malware detection which is classified by malware types. As expected, Ransomware has the highest detection with a total of ninety-six thousand five hundred fifty-four (96554) detections. The Ransomware that been captured is WannaCry with total one thousand four hundred eighty (1480) unique hashes. Furthermore, Trojan Downloader become the second impact to the detection count as many as eight hundred and eighty-five (39975) and with the unique total hash is one hundred sixty-eight (169). Other than that, Trojan also become the third impact to the detection count in the sensor from January to June which is one hundred fifty-seven (157) and with the unique total hash is forty-five (45).

Malware Type	Malware Name	Severity	Unique binaries
Ransomware	WannaCry	High	1480
Trojan	Berbew	High	26
	Skeeyah	High	3
	Derflop	High	1
	Eqtonex	High	4
	Dorv	High	1
	Shellbot	High	6
	Wacatac	High	4
Trojan Downloader	ShWg	High	16
	Small	High	15
	Morila	High	119
	Mirai	High	4
	Adload	High	3
	Occamy	High	8
	Zegost	High	1
	Malagent	High	3
Cryptocurrency Mining	Zombieboy	High	3
	Tiggre	High	3
Exploit	CVE-2015-1701	High	2

Table 2 Malware Types

The list of malware hashes is shown in Table 4 Top 50 MD5 Malware Hashes. Cryptocurrency Mining become the fourth impact to the detection count as many as two hundred forty-four (244) and with the unique total hash is six (6).

CONCLUSION

This report can make a significant difference to the parties' ability to understand better the facts and would be useful to everyone involved in decision-making. Although it is difficult to be fully prepared for any incoming threat, having threat intelligence and regular audit are essential for an organisation to eradicate and remediate any threats. Furthermore, it provides insight for both strategic direction and areas to address technically.

ABOUT THE PROJECT

Background

The Malware Research and Coordination Facility Project was initiated by CyberSecurity Malaysia, whom is also the Permanent Secretariat of the OIC-CERT. The participating agencies / organisations subscribing to this Project share malware data that allow collective malware threat analysis to be done. Such analysis provides early detection of malware for the corresponding advisories to be provided. The analysis and recommendations allow government and organisations to react against the malware threats and protecting their assets against the detrimental effect of malware infection which typically leads to cyber-attacks.

Table 3 list the agencies and organisations that are participating in the Project. The services of the Malware Research and Coordination Facility are also offered to the members of the Asia Pacific Computer Emergency Response Team (APCERT) and the APCERT Malware Mitigation Working Group based on the Memorandum of Understanding (MoU) between the OIC-CERT and APCERT.

The participating agencies / organisations in the Project are:

Country	Percentage (%)
Bangladesh	1. Bangladesh Computer Emergency Response Team (bdCERT) 2. Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
France	Alliacom
India	Indian Computer Emergency Response Team (CERT-In)
Japan	Japan Computer Emergency Response Team / Coordination Center (JPCERT/CC)
Malaysia	1. AIMS 2. Politeknik Mersing Johor 3. Telekom Malaysia 4. Universiti Malaya 5. Universiti Teknikal Malaysia Melaka 6. University College of Technology Sarawak
Nigeria	Ibrahim Badamasi Babangida University
Philippines	Cyber Security Philippines Computer Emergency Response Team (CSP-CERT)
Taiwan	Taiwan National Computer Emergency Response Team (TWNCERT)

Table 3: List of participating countries and organisations

Data Source

The data, information and analysis used to produce this Malware Trend Report H1 2020 are derived from the malware data generated by various sources within CyberSecurity Malaysia and the participating agencies / organisations in this Project such as:

- Network security devices (active and passive) installed regionally;
- Managed security services; and
- User reported cases.

Top 50 Malware Hash

Below are lists of hashes of the files which contain malware detected in this Project:

685bc2af410d86a742b59b96d116a7d9	8e6bfea06cb00553ee29b3822b349bd6
ae12bb54af31227017feffd9598a6f5e	9ba5379aa41d707a4331d27a004baec1
414a3594e4a822cfb97a4326e185f620	8fa0e5dd92185799b73cbfab3da3e919
996c2b2ca30180129c69352a3a3515e4	bdcaf7ef34cd9b02932e5ee2297e4893
0ab2aeda90221832167e5127332dd702	97f647f8b5e1c1f276a479c4935b0c5f
a55b9addb2447db1882a3ae995a70151	ef894d1c6dd120fad5a885bc737d6338
a4d49eaf60a8e333708469606ad9e1a4	2f76b88b420003516f90062940ef7881
6e72ad805b4322612b9c9c7673a45635	fa9b08a5b590461d7cc6a895b52a65b4
cf4f46336abeec03630297f846d17482	0503439b8a9963c4e8b074889f9742a1
95ae8e32eb8635e7eabe14ffbfaa777b	54dd9593fb858bb8b1a77fe5e9238ae2
b026324c6904b2a9cb4b88d6d61c81d1	59b5090fad3d62f05572470f0c79c9a4
a449e84cc83240bb415fef48ff25e9e9	50b93e08b91de26b5487abe79afe1d4a
ce494e90f5ba942a3f1c0fe557e598bf	2de98404eb4ac4a525ed1884f4ea445b
e9d1ba0ee54fcdf37cf458cd3209c9f3	c96b8c08aa8c7177a82b22d898eb1d79
33d373e264dc7fdb0bcdbd8e075a6319	e5840a9753ed8f90fbd7264c8db27c4b
6ce44624f939869bd71436d483c35d39	567726f7f9fe2f15b99738c2a5a7c505
01bdc6fb077098f4a3b60f4b0e479a7f	8d340ce819b42f0c5a27753dd7170ff9
c6905f13850a6375aac7618719d9f1f7	3352a87a86cfe7d4df2d5ccd7fe2c627
3553aeb71299e94c2549f1b34f6c1a43	afada2df173abe2e8a1dfcae0d6da678
a48ca7b40ab2a6ebdd94dbd52164c6cf	549ae01010e6b826a301851393ea8433
1a400481251fac98bc574c0aed7beca8	c73c222af23f0c22a444cd519601c28e
aa718a028875637e1c6eb648706340b6	3caf3d73cd95a94cbbab15307d191f08
85a337912e1f6ec79a064bbc28d9df0e	d31d25eedd79f744b8a3d58888fd668b
7823636f9ce01306178c1ee7772ad831	45735a816370f26b06e053656ca7315d
844290834b6450425b146d4517cdf780	ce223b231f2862124386c585e9b95ca1

Table 4: Top 50 MD5 Malware Hashes

OIC-CERT Permanent Secretariat:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

secretariat@oic-cert.org
www.oic-cert.org