MALWARE TREND REPORT

H1 2018 (JANUARY – JUNE 2018)

to educate and improve awareness, preparedness, and readiness in facing cyber threats

CONTENT

DISCLAIMER

THE OIC-CERT MALWARE TREND REPORT H1 2018

The OIC-CERT Malware Trend Report is a series of reports produced half yearly for the Malware Research and Coordination Facility project. The project, in malware threats analysis, 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. This 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.

The H1 2018 is the 4th Malware Trend Report produced covering the period of January till June 2018.

INTRODUCTION

Cyber security has become a critical issue in all the economic sectors in every country today. Organisations are spending more than ever on cyber security, from appliances to hiring IT security professionals to protect their digital network and keeping unwanted parties out of the IT networks. However occurrences of cyber security incidents like data breaches are still increasing. In the long run, data breaches can give severe strategic and financial impact on companies [1].

Halfway through 2018, it can be seen that the number of data breaches are rising and continue to be a threat mainly on customer personal information especially in the healthcare sector. The data that is potentially at risk includes customer contact information, such as email addresses and physical addresses, as well as login information, such as usernames and passwords. The passwords were stored with encryptions, which need to be unencrypted before they could be used [2].

It is noted that cyber-attacks such as ransomware and data breaches particularly in the healthcare sector has been increasing and become the target of attackers [3]. The healthcare sector digital network is classed as a national critical information infrastructure, alongside financial, utilities and transport networks. This makes it an attractive target for those hackers wanting to cause chaos, which might be from a hostile foreign country. Attacking a healthcare organisation that is part of a wider network of infrastructure could also provide a way in to other critical facilities.

For this year, the data breaches do not only threaten the related national critical information infrastructure, but also third-party services [4]. As these third-party services are being breached, the customers' data being stolen from multiple companies are done in one go. The saying "there is no such thing as bad publicity" may portray the effect of the incident where the customers will think of the incident as a violation of trust. It is not just loss of trust by current customers, but it has ripple effects in terms of negative word-of-mouth, especially in the age of social media.

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 ultimate 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.

MALWARE TYPES

Malicious software or malware refers to a type of computer program designed to infect a legitimate user's computer and inflict harm on it in multiple ways. Malware can infect computers and devices in several ways and comes in a number of forms such as viruses, worms, Trojans and spyware.

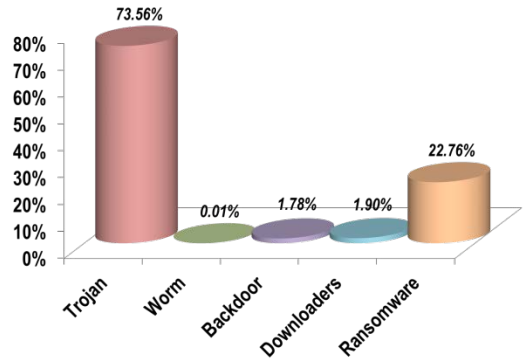

Figure 1 : Captured Malware type in Hi 2018

Malware Type	Percentage (%)			
	H2 2016	H1 2017	H2 2017	H1 2018
Trojan	12.04	60.17	55.73	73.56
Worm	77.64	27.11	19.55	0.01
Backdoor	9.03	9.74	18.92	1.78
Downloaders	1.26	2.95	2.91	1.90
Ransomware	0.03	0.03	2.89	22.76

Table 1 : Statistics comparison of detected malware by reports

Table 1 depicts the figures of the malware types detected in this project for the period of second half of 2016 (H2 2016) till first half of 2018 (H1 2018) according to the respective Malware Trend Reports. The trend of the malware types detected in January to June 2018 shows that Trojan is still the top malware infecting computers, servers, and users. The malware infection detected through Trojan is at 73.56%, which increases by 17.83% than reported in the previous report (H2 2017). This might be caused by the increase infection of the CoinMiner Trojan that infect computer resources to mine digital currency.

However, the Backdoor and Downloaders malware detected during this period, reduced tremendously compared to the second half of 2017. This could be due to the antivirus companies updating the malware signatures. The Backdoor.Androm which was mostly detected in the last reporting period has decreased significantly during this period.

The malware threats classification details are provided in the "About the project" section at the end of this report.

C&C CALLBACK DESTINATION

Figure 2 shows the distribution of malicious IP addresses serving the Command and Control (C&C) servers by countries for the first half of 2018. Figure 3 and Table 3 shows the data comparison and statistics of the top 10 callback destinations for H1 2018, H2 2017, H1 2017 and H2 2016.

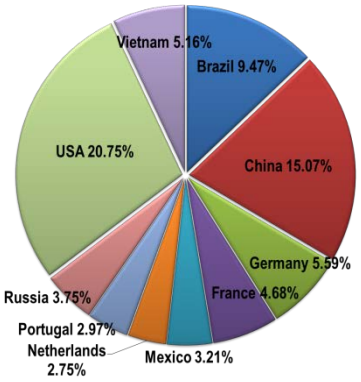

Figure 2 : C&C Servers distribution

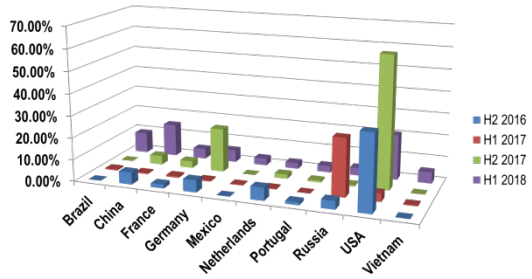

Figure 3 : C&C Callback destination

	Percentage (%)			
	H2 2016	H1 2017	H2 2017	H1 2018
Brazil	0.00	0.58	0.00	9.47
China	5.56	0.48	4.10	15.07
France	1.80	0.74	3.13	4.68
Germany	5.56	0.58	20.10	5.59
Mexico	0.00	0.21	0.00	3.21
Netherlands	5.88	0.38	1.96	2.75
Portugal	1.31	0.02	0.88	2.97
Russia	3.82	26.49	0.65	3.75
USA	34.64	3.78	60.10	20.75
Vietnam	0.01	0.37	0.00	5.16

Table 2 : Statistic comparison of C&C by report period

PC THREATS

This section provides an overview of the personal computer (PC) threats. As shown in Table 3, Trojan is the main detected malware in Windows Operating System (OS) which is 69.9% from the total malware detected for Windows. Its most prominent malware is the Tool.CoinMiner.

	Malware detected in the region		Most Common Malware
	H2 2017	H1 2018	
Windows	Total 50.05% -Trojan 55.8% -Backdoor 37.9% -Downloaders 5.6% -Others 0.7%	Total 57.58% -Trojan 69.9% -Backdoor 2.3% -Downloader 27.8% -Others 0.0%	Tool. CoinMiner
	Total 34.65% Trojan 80.3% Downloader 0.3% Others 19.3%	Total 34.82% Trojan 25.4% Downloader 0.5% Others 74.2%	Ransomware. Wcry

Table 3 : Overview of PC Malware threats

Malware targeting other OS such as the Linux and Macintosh in the first half of 2018 is are more or less the same as compared to the second half of 2017 with a combined total of 34.82% (Trojan, Downloaders and Others malicious codes).

From the statistic of the second half of 2017 and first half of 2018, it is shown that Ransomware.Wcry malware remains as the top malware detected by other PC OS in this project.

Table 4 presents the comparison between the PCs and mobile threats detected during the period of this report. Malware threats detected targeting PCs running on Windows and other OS is at 92.40%. As such, 7.60% of the malware detected targets mobile OS. It can be observed that malware activities targeting mobile OS are decreasing where for the first half of 2018 they were at 7.60% as compared to the second half of 2017 which was at 15.30%. This could be because of the implementation of the new Google security platform, Google Play Protect, which decrease

the Android application security threats through machine learning.

Malware threat category	Malware activity detected in the Region,	
	H2 2017	H1 2018
 PCs	84.70%	92.40%
 Mobile (Android & iOS)	15.30%	7.60%

Table 4 : PC vs Mobile malware threats

MOBILE THREATS

As the usage of smartphones and tablets increases, the cyber criminals are also changing their target to the mobile devices [5]. Some of the elements employed by these criminals are social engineering and searching for vulnerabilities that exist on the mobile OS. A group of researchers from the University of Cambridge has found that 87 percent of all Android smartphones are exposed to at least one critical vulnerability [6]. On the other hand, Zimperium Labs discovered that 95 percent of Android devices could be hacked with a simple text message [7].

	Mobile malware detected in the region	
	H2 2017	H1 2018
	100% Most common malware Android.Malware.Triada	100% Most common malware Android.Malware.Axent
	0%	0%

Table 5 : Mobile threats comparison of recent periods

Table 5 illustrates the mobile threats in H2 2017 and H1 2018. The Android presents a much bigger target for malware where Android.Malware.Avent was detected as the most common malware in H1 2018.

ANDROID MALWARES

Rank	Malware	%
1	Android.Malware.Axent	21.43%
2	Android.Malware.Clicker	15.98%
3	Android.Malware.Guerrilla	14.74%
4	Android.Malware.HiddenAds	14.04%
5	Android.Malware.Triada	13.29%
6	Android.Riskware.HiddenAds	13.24%
7	Android.Riskware.Leech	3.95%
8	Android.Riskware.Uuserv	2.15%
9	Android.Malware.Kemoge	0.90%
10	Android.Malware.FakeApp	0.30%

Table 6 : Top 10 Android malware detected

Table 6 list the top 10 malwares detected infecting Android mobile users in this project. These malwares represent more than 99.6% of the total malware detected targeting Android smartphones.

Android.Malware.Axent, is ranked the highest on Android malware detected. Android. Malware.Axent or Android/Axent.A is a malware that has the capability to propagate by attaching its code to other programs or files [8].

NETWORK SERVICES & WEB THREAT

Organisations should pay careful attention to the threats targeting the computers and networks as cyber-attacks can and do happen to anyone. Modern cyber threats go far beyond the capabilities of antivirus detection and email spam filters. Network security threats are a growing problem for users and organisations all over the world, and they only become worse and multiply with every passing day.

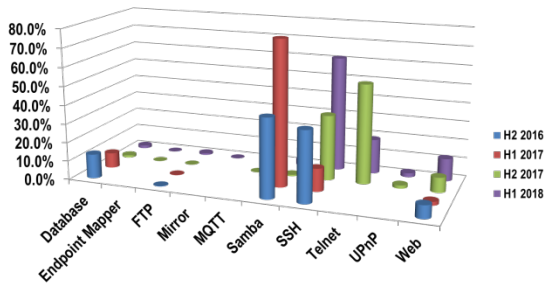

Figure 4 : Overview of the targeted services

	Percentage (%)			
	H2 2016	H1 2017	H2 2017	H1 2018
Database	13.0	8.1	1.3	1.6
Endpoint Mapper	0.0	0.0	0.0	0.0
FTP	0.2	0.2	0.0	1.0
Mirror	0.0	0.0	0.0	0.0
MQTT	0.0	0.0	0.0	0.0
Samba	42.1	77.4	0.8	3.1
SSH	37.7	12.3	34.9	61.4
Telnet	0.0	0.0	53.1	18.6
UPnP	0.0	0.0	1.7	2.2
Web	7.0	2.0	8.1	12.1

Table 7 : Statistics of the targeted services

Referring to Table 7, during the H1 2018, SSH services becomes the main targeted services at 61.4% while the number of Telnet attacks for the same period abruptly decreased compared to the second half of 2017. This is aligned with the global trend of the Mirai attacks that occurred last year which has been contained. Mirai is a malware that turns networked devices running on Linux into becoming remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks.

The attacks that targeted web services also showed an increase to 12.1% compared to 8.1% during H2 2017. The Samba services attacked increases due to the increase of WannaCry ransomware detected in this project (99.8%). WannaCry is a ransomware exploiting the SMB vulnerabilities.

As in Figure 3 below, there is a significant increase from 18.5% in H2 2017 to 48.8% in H1 2018 in the attack that involved phpMyAdmin scanning activities to collect the details of the phpMyAdmin web application version. This information can be used to enhance further attack through vulnerability list. Based on its version information, 16% of malware or attacker attempted to compromise the phpMyAdmin web application using CVE-2009-4605 vulnerability. Figure 5 shows that the activity of scanning open public web proxy server information is decreasing from 60.3% in H2 2017 to 5.1% in H1 2018. The information gathered from the proxy scanning can be used by an attacker as intermediary in order to access the Internet using the targeted proxy identity to hide their presence.

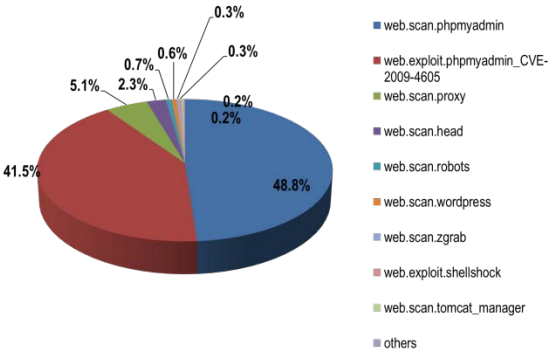

Figure 5 : Overview of the targeted web application vulnerabilities

RANSOMWARE

Ransomware is still the biggest security threat for 2018. Early this year, a new type of ransomware, GandCrab ransomware was found [9]. The operation method is the same with other ransomware, GandCrab ransomware is a Trojan horse that also encrypts files on the compromised computer and demands payment to decrypt them. GandCrab ransomware is sold cheaply on the dark web as 'malware-as-a-service'. It has regular updates from its developers and quickly rose to become one of the most popular forms of file-locking malware.

For the period of H1 2018, only 3 types of ransomware were detected as shown in the Table 8.

Ransomware	Detected
Ransomware.Wcry	99.8%
Ransomware.Win.GandCrab	0.1%
Ransomware.Downloader.Locky	0.1%

Table 8 :Ransomware detected in H1 2018

The WannaCry ransomware (99.8%) is still roaming around despite of the global attack that happened in May 2017.

CONCLUSION

More attacks are being launched by cyber criminals who are now far more sophisticated than what the security teams were facing a decade ago. With the advancement of the tools, the deployed attacks now may take place over several months. Long gone are the days when straightforward attacks such as SQL injections were the only worries for information security professionals. The dependency has inherent vulnerabilities and opportunities which place the critical national information infrastructure vulnerable to cyber exploitation. For the coming years, by using the data from the project and available incident statistics, we should be able to comprehend better the facts behind every cyber incident. This can be used as a basis to be better prepared for any future eventualities.

ABOUT THE PROJECT

Background

The Malware Research and Coordination Facility project was initiated by CyberSecurity Malaysia, 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 9 list the countries 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	Organisation
Bangladesh	Bangladesh Computer Emergency Response Team (bdCERT)
China	National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT)
France	Alliacom

India	Indian Computer Emergency Response Team (CERT-In)
Malaysia	1. University Teknikal Malaysia Melaka 2. University Putra Malaysia 3. Telekom Malaysia 4. AIMS 5. University Malaya
Nigeria	Ibrahim Badamasi Babangida University
Philippines	Cyber Security Philippines Computer Emergency Response Team (CSP-CERT)
Taiwan	Taiwan National Computer Emergency Response Team (TWNCERT)

Table 9 : List of participating countries and organisations

Threat Categories

To simplify the presentation of the malware data and making the malware analysis easier to understand, this Malware Trend Report classifies the many types of malware threats into categories. Threat categorisation is based on a number of factors such as similarities in threat function and purpose, how the threat spreads and what it is designed to do.

The threat categories described in this malware report are categorised as:

THREAT CATEGORY	PLATFORM(S) TARGETED	OPERATING SYSTEM
PC	Personal Computers • Desktop; • Laptop; and • Netbook.	Linux / Unix Mac OS X Windows
Mobile	Mobile Devices • Smartphones; • Tablets/iPads; and • Wearables.	Android iOS
Web	Internet Browsers • Internet Explorer; • Edge; • Chrome; • Firefox; • Opera; Mobile Devices • Safari, etc. Servers • Apache; • Internet Information Services, etc. Personal Computers	Android Linux / Unix Mac OS X / iOS Windows
Ransomware	Mobile Devices Personal Computers	Android Linux / Unix Mac OS X / iOS Windows

Table 10 : Definition of the threat categories

Data Source

The data, information and analysis used to produce this Malware Trend Report H1 2018 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.

REFERENCES

[1] "Risky business: the impact of data breaches." [Online]. Available: https://blog.kenan-flagler.unc.edu/risky-business-the-impact-of-data-breaches/. [Accessed: 11-Jul-2018].

[2] https://www.businessinsider.my/data-breaches-2018-4/?r=US&IR=T

[3] https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

[4] J. H. Gemano, "Third-party cyber risk & corporate responsibility," 2017.

[5] P. Ruggiero and J. Foote, "Cyber threats to mobile phones."

[6] D. R. Thomas, A. R. Beresford, and A. Rice, "Security Metrics for the Android Ecosystem," in Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '15, 2015.

[7] Z Team, "The biggest splash at blackHat and defcon 2015," Zimperium, 2015. [Online]. Available: http://blog.zimperium.com/the-biggest-splash-at-blackhat-and-defcon-2015/. [Accessed: 11-Jul-2018].

[8] FortiGuard, "Android/Axent.A," 2014. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/6439892. [Accessed: 11-Jul-2018].

[9] Symantec, "Ransom.GandCrab," 2018. [Online]. Available: https://www.symantec.com/security-center/writeup/2018-013106-5656-99. [Accessed: 11-Jul-2018].

If you have any enquiries or comments about the Malware Trend Report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone or email:

The Permanent Secretariat of the
Organisation of the Islamic Cooperation –
Computer Emergency Response Team (OIC-CERT)

Level 5, Sapura@Mines
The Mines Resort City
43300 Seri Kembangan
Selangor, Malaysia

+603 8992 6888
international@cybersecurity.my
secretariat@oic-cert.org