Malware Trend Report H2 2017

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

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 Science, Technology and Innovation Malaysia and 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 about 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 organisations and products mentioned herein are the trademarks of their respective owners. Use of the logo and name do not imply any affiliation with or endorsement by the respective organisations.

Contents

About the OIC-CERT Malware Trend Report H2-2017

The OIC-CERT Malware Trend Report H2-2017 is the 3rd of its kind covering malware trends for the 2nd half of 2017. This is an outcome of the Malware Research and Coordination Facility project which is a collaborative effort from the Organisation of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**), the Asia Pacific Computer Emergency Response Team (**APCERT**) and other organisations of various countries in malware threats analysis.

This project is an initiative by CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation Malaysia and the Permanent Secretariat of the OIC-CERT. The background of the project and the participating agencies / organisations is provided in **Appendix A**.

Introduction

Today, most industries are now dependent on the use of computers and internet to conduct business. Thus attacks on the industrial control systems applications could wreak havoc, leading to a significant amount of damage and downtime.

2017 has presented us with a number of cyber-attacks. One of the biggest ransomware attacks was the WannaCry ransomware which happened in May 2017. It struck hospitals belonging to the United Kingdom's National Health Service (**NHS**) [2], [3], internet service provider Telefonica, and other high-profile targets around the world. By exploiting EternalBlue, a vulnerability which Microsoft patched in a security bulletin in March 2017, it demands $300 in Bitcoin as ransom.

Not too long after that, another attack named NotPetya [4] was discovered on 27 June 2017 when power distributors in Ukraine and the Netherlands confirmed hacking attacks that affected their systems. Not long after that, Ukraine's government, the offices of multinationals in Spain, and the British advertising group WPP confirmed similar incidents.

Summary

2017 saw a huge number and a variety of cyber-attacks, ranging from data leakages to ransomware attacks. MyCERT has released a total of 38 advisories and 11 alerts on security updates, vulnerabilities and ransomware including those of WannaCry, New Petya@NotPetya, and Bad Rabbit Ransomware.

Further information can be found at *https://www.mycert.org.my/en/services/advisories/mycert/2017/main/index.html*.

With those occurrences, it is very important for organisations to realise that cyber criminals have the capability and capacity to inflict harm across the geographical borders. As we share common interests in the political and economic activities, cooperation among the countries and organisations is necessary to better mitigate malware threats. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always implement measures to protect their systems and networks from these threats.

With the cyber space growing too rapidly and new products and services coming online every day, the world is witnessing rapid advances in internet technologies, both for offensive and defensive purposes. Consequently, it is becoming more difficult to keep track of the vulnerabilities that come with these technologies. This can be seen when Google's Project Zero exposes the two critical vulnerabilities [5] affecting nearly every device made in the past 20 years.

While most people do not believe that they could be the target of an attack, hackers have tried to keep a low profile through gaining network access through those who least expect it and then move up the chain until they reach their intended goal.

Objectives

This Report aims to provide a better understanding of malware threats and analysis as well as the related potential impacts. 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 general Internet users.

Malware Types

The malicious software or known as 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, just a few of which include viruses, worms, Trojans, spyware and more.

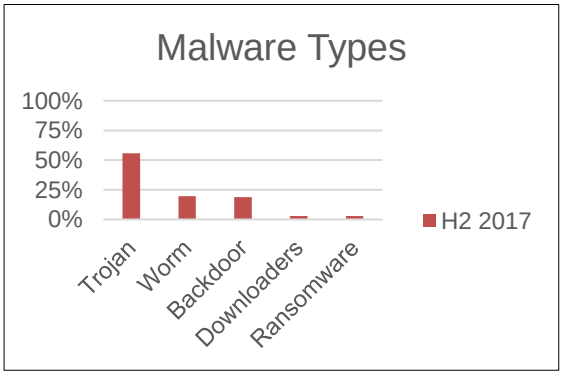

Figure 1 : Captured malware types

Malware Types	H2 2016	H1 2017	H2 2017
Trojan	12.04%	60.17%	55.73%
Worm	77.64%	27.11%	19.55%
Backdoor	9.03%	9.74%	18.92%
Downloaders	1.26%	2.95%	2.91%
Ransomware	0.03%	0.03%	2.89%

Table 1: Captured malware in the project

The malware data detected in this project for the second half of 2017 is compared with the first half of 2017 and the second half of 2016 which is presented in Table 1. The malware types show that from July to December 2017, the computers, servers, and users in this Project are infected primarily by Trojans followed by Worms. The malware infection detected through Trojan is comparatively higher at 55.73%, but less than reported in the previous report (H1 2017). Two figures that showed an increase compared to the second half of 2017 was Backdoor with 18.92% which is double (9.74% in H1 2017) and ransomware at 2.89% compared to 0.03% in H1 2017. The malware threats classification details are provided in **Appendix B.**

C&C Callback Destination

From July to December 2017, the majority of the malicious IP addresses serving Command and Control (**C&C**) servers came from the United States of America and Germany. Figure 2 shows the top ten C&C countries that were identified as callback destinations which contribute to 80.2% of all countries serving C&C servers.

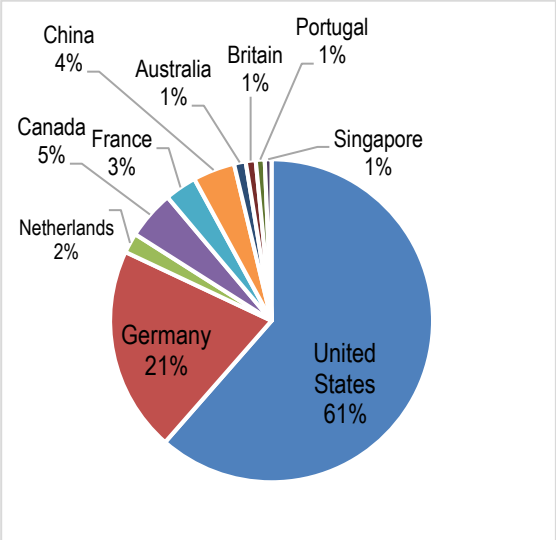

Figure 2 : C&C Servers distribution

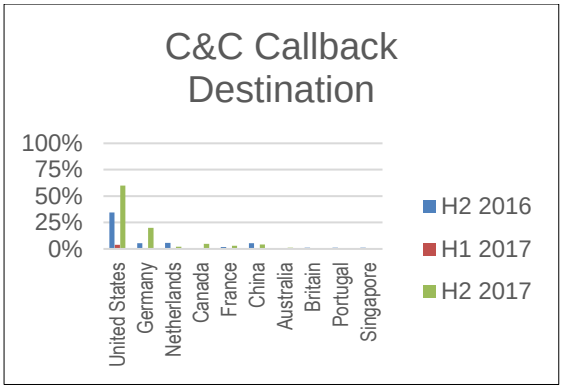

Figure 3 : C&C Callback destination

The following figure 3 also shows data comparison of top 10 callback destinations for H2 2017, H1 2017 and H2 2016, which three countries (United States of America, Germany and the Netherlands) still remain in the top 10 callback destination for the three halves.

PC Threats

	Malware Detected in the Region H1 2017	Malware Detected in the Region H1 2017	Most Common Malware
Windows	**Total 61.87%** Trojan 75.1% Backdoor 17.5% Downloader 5.3% Others 2.2%	**Total 50.05%** Trojan 55.8% Backdoor 37.9% Others 0.7%	Backdoor. Androm
GNU/LINUX	**Total 22.41%** Trojan 90.7% Downloader 0.1% Others 9.1%	**Total 34.65%** Trojan 80.3% Downloader 0.3% Others 19.3%	Trojan. Sinkhole Malware

Table 2: Overview of PC Malware threats

This section gives an overview of the PC threats. Table 2 shows the summary of malware detected based on the PC platform. 50.05% of the malware detected in this project infected the Windows Operating System (**OS**) with its most prominent malware being the Backdoor.Androm. Malware targeting other OS such as the Linux and Macintosh are increasing with a combined total of 34.65% (Trojan, Downloaders and Others malicious codes).

It is shown through the statistic of the second half of 2017 that Trojan.Sinkhole Malware is the top malware detected in this project.

Furthermore, Table 3 provides comparison between the Windows and mobile threats detected in this project. Malware threats detected targeting the PCs running Windows and other OS is totalling to 84.70%. As such, 15.30% of the malware detected targets mobile OS. It can be observed that malware activities on mobile OS are slightly decreasing where H2 2017 is at 15.30% as compared to the H1 2017 which is at 15.73%.

Malware threat category	Malware activity detected in the Region, H1 2017	Malware activity detected in the Region, H2 2017
PCs	84.27%	84.70%
Mobile (Android & iOS)	15.73%	15.30%

Table 3 : PC vs Mobile malware threats

Mobile Threats

	Mobile malware detected in the region H1 2017	Mobile malware detected in the region H2 2017
	99.8% With most common malware – HiddenApp (Trojan)	**100%** With most common malware – Android.Malware.Triada
	0.2% With most common malware – XcodeGhost (Backdoor)	**0%**

Table 4 : Overview of mobile threats

The usage of mobile devices are on the rise as smartphones and tablets are quickly becoming more powerful as companies embrace the idea of 'bring your own device' (**BYOD**) policies and allow users to access corporate networks with personal technologies. But along with the increased use comes an explosion of mobile malware, the malicious code designed to target smartphones and tablets.

Table 4 illustrates the mobile threats in H2 2017 and H1 2017. Android.Malware.Triada was detected as the most malware in H2 2017.

Android Malwares

Rank	Malware	%
1	Android.Malware.Triada	26.53%
2	Android.Riskware.Uuserv	20.22%
3	Android.Malware.Clicker	17.45%
4	Android.Malware.Axent	10.30%
5	Android.Malware.HiddenApp	9.41%
6	Android.Riskware.HiddenAds	6.69%
7	Android.Malware.Guerrilla	2.62%
8	Android.Riskware.Leech	2.37%
9	Android.Malware.HiddenAds	2.24%
10	Android.Malware.Ztorg	2.17%

Table 5 : Top 10 Android malware detected.

Table 5 lists the top 10 malwares detected infecting Android mobile users in this project. These malwares represent more than 94% of the total malware detected targeting Android smartphones.

Android.Malware.Triada, is ranked the highest on Android malware detected. Triada is a modular mobile Trojan that actively uses root privileges to substitute system files and exists mostly in the device's RAM, which makes it extremely difficult to detect.

Once Triada Trojan is downloaded and installed, it will try to collect some information about the system such as the device model, the OS version, the amount of storage on the SD card, and the list of the installed applications. Once collected, this trojan will send all that information to the C & C servers.

Network Services & Web Threat

Organisations should pay careful attention to the threats targeting their 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 days. In H2 2017, three network services attack detection functions were added to the project. The services are Universal Plug & Play (**UPnP**), Message Queuing Telemetry Transport (**MQTT**) and EndPoint Mapper.

UPnP is a networking platform that outlines a specific communication method that almost all devices such as printers can use to immediately communicate with one another on a network. The weakness of UPnP was discovered over a decade ago for a number of security vulnerabilities [6].

The MQTT protocol uses a publish/subscribe communication pattern, is used for machine-to-machine (**M2M**) communication and plays an important role in the Internet of Things (**IoT**). MQTT poor authentication mechanism will let subscribers free to get the overall published data.

The Endpoint mapper handles message exchange over TCP/IP. The vulnerability exists can result to incorrect handling of malformed messages which could lead to a denial of service [7]. An attacker can exploit this vulnerability by establishing a TCP/IP connection to the endpoint mapper process on a remote machine and transmitting a malformed message.

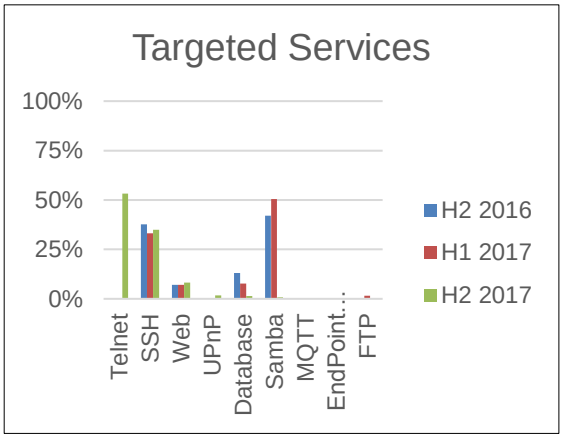

Figure 4 : Overview of targeted services.

Referring to Figure 4, during the H2 2017, Telnet becomes the main targeted services at 53.1% while the number of Samba attacks for the same period abruptly decreased compared to the first half of 2017. SSH also remains the top 3 targeted services. The attacks that targeted web services

also showed an increase to 8.1% compared to 7.1% during H1 2017.

As in Figure 5 below, there is a significant increase in the attack where the malware or the attacker is collecting open public web proxy server information as it 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 also shows that 18.5% of the targeted web application is phpMyAdmin scanning in 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 and 16% of malware or attacker is attempting to compromise the phpMyAdmin web application using CVE-2009-4605 vulnerability.

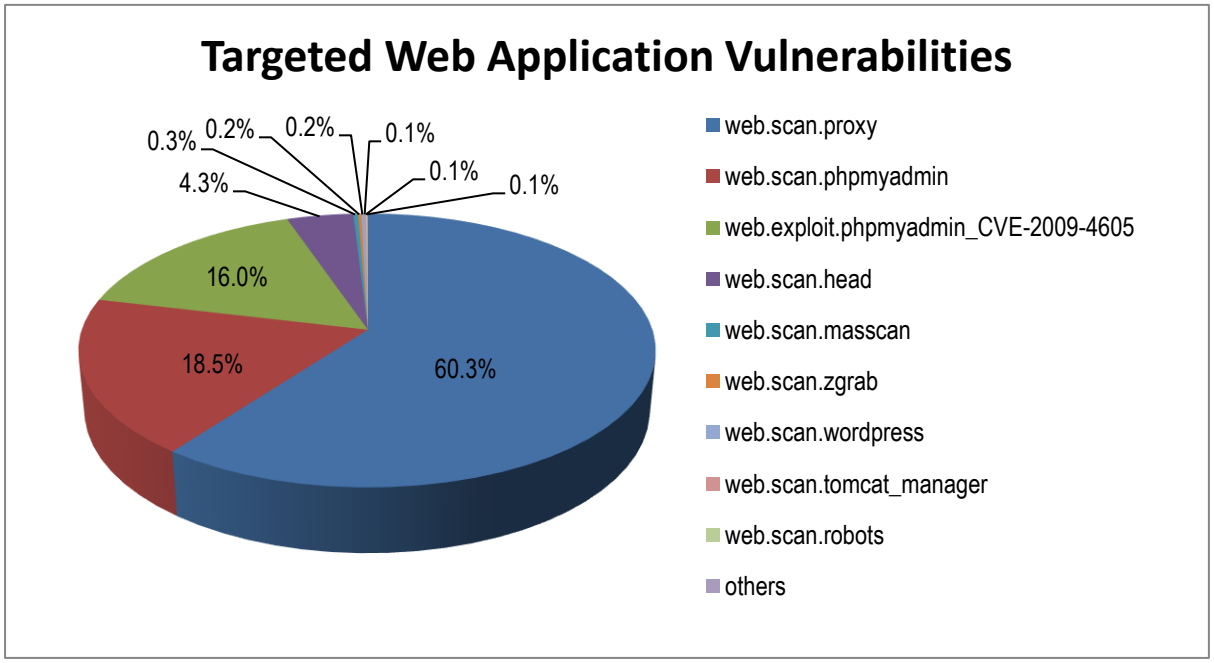

Figure 5 : Overview of the targeted web application vulnerabilities

Ransomware

Today, the ransomware attacks have become a new norm as most attacks are indiscriminate. For the most part, cyber criminals issue ransomware at random, hitting anyone and everyone it could. If an attacker can recognise the difference between an enterprise and a consumer target, he/she will be able to adapt the ransom demands to match the victims. Once a machine has been infected, ransomware will prevent or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

The intentions of the attacks are also likely to become more personal. In addition to encrypting files, ransomware attackers will soon be threatening to post data or information on social media, or to expose it in an equally destructive way. As with most cyber-attacks, ransomware will grow to take advantage of more human vulnerabilities.

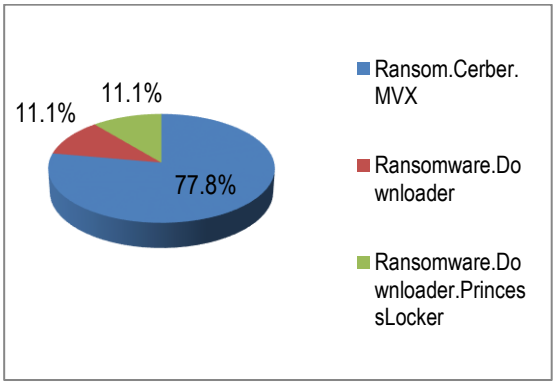

Figure 6 : Ransomware detected in H1 2017

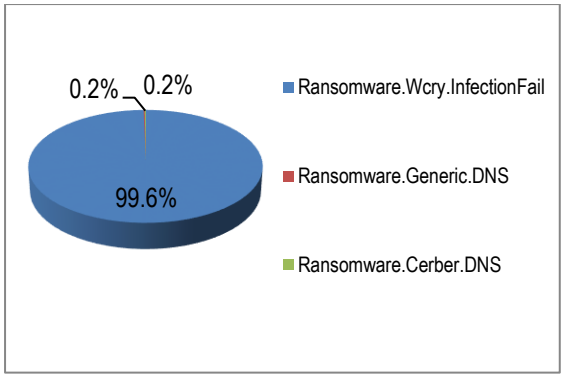

Figure 7 : Ransomware detected in H2 2017

Figure 7 shows the three ransomwares detected in this project for H1 2017 and H2 2017. There is only one (1) ransomware that appear in both halves which is Cerber. The other two (2) was not detected in H1 2017; Wcry and Generic. As in figure 7 above, WannaCry ransomware (99.6%) is still roaming around despite of the global attack that happened in May 2017.

Figure 8 : WanaCry ransomware screenshot
Source : MyCERT Advisory - Technical Detail: WannaCry Ransomware [8]

WannaCry is a ransomware worm that spread rapidly across a number of computer networks in May of 2017. The vulnerability WannaCry exploits known as EternalBlue [8] lies in the Windows implementation of the Server Message Block (**SMB**) protocol. The SMB protocol helps various nodes on a network communicate, and Microsoft's implementation could be tricked by specially crafted packets into executing arbitrary code.

The WannaCry is a worm that delivers a ransomware payload. It has two primary components: A worm module used for self-propagation and a ransom module used for handling the ransom extortion activities [9].

The program code is not obfuscated and was relatively easy for security pros to analyse. Once launched, WannaCry tries to access a hard-coded URL (the so-called kill switch) [8]; if it is unable to, it proceeds to search for and encrypt files in a slew of important formats, ranging from Microsoft Office files to MP3s and MKVs, leaving them inaccessible to the user. It then displays a ransom notice, demanding $300 in Bitcoin to decrypt the files.

Conclusion

The project data for 2017 has shown a significant increase in Ransomware and Backdoor and not much change on the other malware types which continue to be threats that have to be dealt with. For the coming years, 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 for us to be better prepared for any future eventualities.

Appendices

Project Background

The Malware Research and Coordination Facility project was initiated by CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation Malaysia and 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.

At the moment, the organisations that participated in the projects are from Malaysia, Taiwan, France and Nigeria. The services of the Malware Research and Coordination Facility are also offered to the Asia Pacific Computer Emergency Response Team (**APCERT**) through a Memorandum of Understanding (**MoU**) between the OIC-CERT and APCERT and APCERT Malware Mitigation Working Group.

The participating agencies/organisations in the Project are listed below:

Country	Organization
Malaysia	1. University Teknikal Malaysia Melaka 2. University Putra Malaysia 3. Telekom Malaysia 4. AIMS 5. University Malaya
Taiwan	Taiwan National Computer Emergency Response Team (TWNCERT)
France	Alliacom
Nigeria	Ibrahim Badamasi Babangida University

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 provided in Table 6 below.

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 6: Definition of the threat categories.

Data Source

The data, information and analysis used to produce this Malware Trend Report H2 2017 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] n.d, "Meltdown and Spectre," 2018. [Online]. Available: https://meltdownattack.com/. [Accessed: 05-Jan-2018].

[2] K. Hall, "UK hospital meltdown after ransomware worm uses NSA vuln to raid IT," *The Register*, 2017. [Online]. Available: https://www.theregister.co.uk/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack/. [Accessed: 09-Jan-2018].

[3] NCSC, "Latest statement on international ransomware cyber attack," 2017. [Online]. Available: https://www.ncsc.gov.uk/news/latest-statement-international-ransomware-cyber-attack-0. [Accessed: 02-Jan-2018].

[4] msft-mmpc, "New ransomware, old techniques: Petya adds worm capabilities," 2017. [Online]. Available: https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/. [Accessed: 02-Jan-2018].

[5] M. Linton and P. Parseghian, "Google Online Security Blog: Today's CPU vulnerability: what you need to know," 2018. [Online]. Available: https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html. [Accessed: 07-Jan-2018].

[6] H. Moore, "Security Flaws in Universal Plug and Play: Unplug, Don't Play," *Rapid7*, 2013. [Online]. Available: https://blog.rapid7.com/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play/. [Accessed: 10-Dec-2017].

[7] Microsoft, "Microsoft Security Bulletin MS01-048 - Critical," 2017. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/ms01-048. [Accessed: 10-Dec-2017].

[8] MyCERT, "MA-663.052017: MyCERT Advisory – Technical Detail: WannaCry Ransomware," 2017. [Online]. Available: https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1265/index.html. [Accessed: 10-Dec-2017].

[9] Symantec, "Ransom.Wannacry," 2017. [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99. [Accessed: 10-Dec-2017].

If you have any enquiries or comments about this 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