

MALWARE TREND REPORT

H2 2018

 July - December 2018



*"To educate and improve awareness, preparedness,
and readiness in facing cyber threats."*

CONTENT

The OIC-CERT Malware Trend Report H2 2018	2
Introduction.....	2
Objectives.....	3
Target Audience	3
Malware Types	4
C&C Callback Destination	5
PC Threats	6
Mobile Threats.....	7
Android Malwares.....	7
Network Services & Web Threats.....	7
Ransomware	9
Conclusion.....	9
About the project	10
Background	10
Threat Categories.....	10
Data Source	11
References	12

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 organisations 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 organisations.

THE OIC-CERT MALWARE TREND REPORT H2 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 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 H2 2018 is the 5th Malware Trend Report published covering the period of July until December 2018.



INTRODUCTION

The year 2018 has come to an end with a number of cyber incidents stealing news headlines. It was arguably the 2018 devastating data breaches that have brought cyber security into mainstream focus. Billions of data were breached affecting millions of customers. The attacks are not only targeting single sector, but spanned across various critical information infrastructure, from the health, telecommunication and financial sectors to the transportation sector.

In a cyber attack in November 2018, Marriott International announced that 500 million customers data have been stolen due to unauthorized access to the Starwood network [1], [2]. The breach occurred on the systems supporting the Starwood hotel brands way back in 2014. The breach remained unnoticed after Marriott acquired Starwood in 2016 and were only discovered in September 2018. Marriott declared that for some of the victims, only name and contact information were compromised while on the other hand, they also believed that credit card numbers and expiration dates of more than 100 million customers were stolen.

However, the company is uncertain whether the attackers were able to decrypt the credit card numbers.

...devastating data
breaches have brought
cyber security into

The Starwood incidents proved that every organisation today requires a holistic and modern approach to secure information due to the complexity of cyber-attack pattern that we have experienced continues to grow [3]. In securing their information, some organisations are using the data leakage/loss prevention (DLP) strategy to secure their information. However, based on a study conducted on three DLP products in 2015, deploying a single DLP product is not enough and pose a security risk to the environment if no additional security control points installed to prevent basic data leakage caused by internal attackers or malware [4]

As the implementation of a complete security control might be quite costly, the implementation of a cyber early warning system could be another alternative to ensure the security of an organisation network and information [5]. The cyber early warning mechanism can be in the forms of a proxy firewall, network monitor, honeypot, and intrusion detection module. The cyber early warning system can quickly react like sending alerts, tracking, and blocking when any form of cyber-attack is detected.

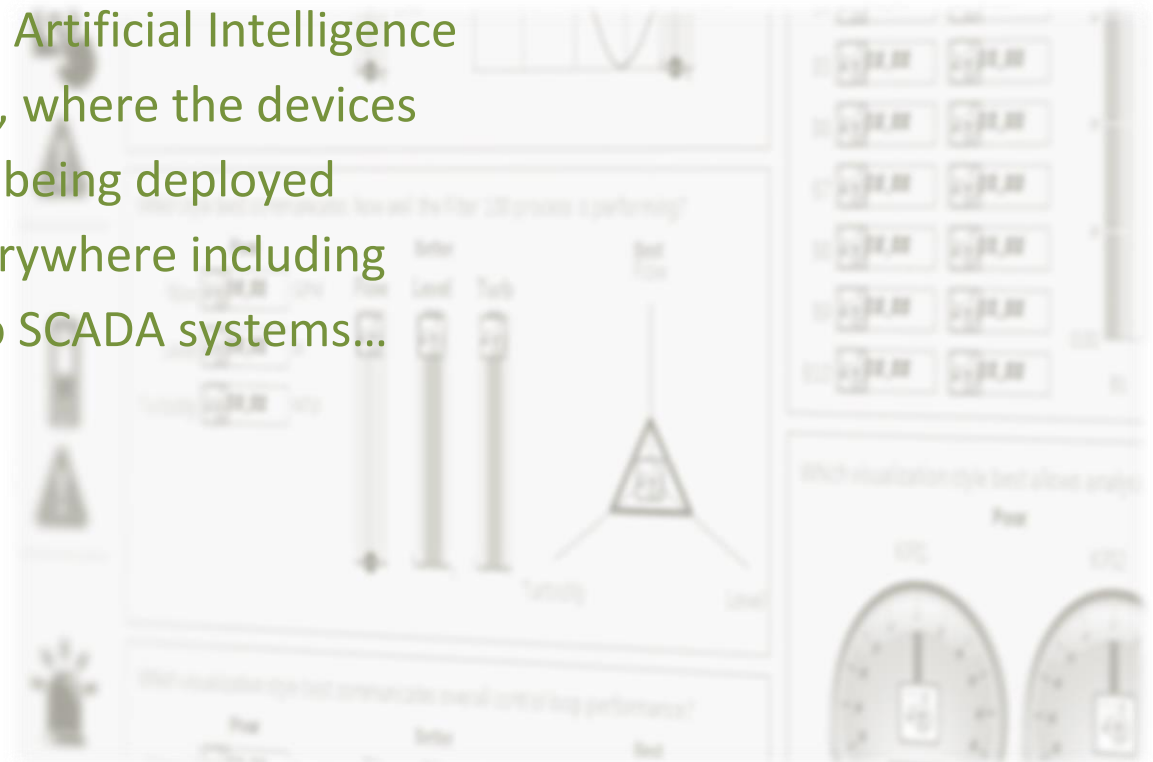
OBJECTIVES

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 general Internet users.

... new emerging technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), where the devices are being deployed everywhere including into SCADA systems...



MALWARE TYPES

Malicious software or malware runs much like any other software. The key difference between malware and non-malware is the behaviour because a malware is designed to infect a legitimate user's computer and inflict harm on it in multiple ways such as stealing user data, replicating, disabling certain security features, serving as a backdoor, or executing commands not intended by the user [5]. A malware can infect computers and devices in several ways and comes in number of forms such as viruses, worms, trojans and spyware.

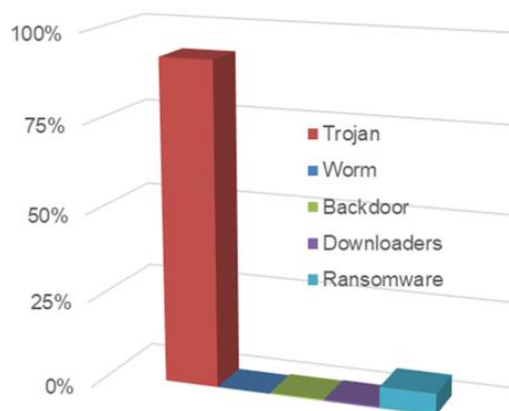


Figure 1: Captured malware type in H2 2018

Malware Type	Percentage (%)			
	H1 2017	H2 2017	H1 2018	H2 2018
Trojan	60.17%	55.73%	73.56%	98.89%
Downloaders	2.95%	2.91%	1.90%	0.59%
Backdoor	9.74%	18.92%	1.78%	0.43%
Worm	27.11%	19.55%	0.01%	0.05%
Ransomware	0.03%	2.89%	22.76%	0.04%

Table 1: Statistics comparison of detected malware by reports

Table 1 illustrates the statistics of malwares detected in this project for the period of 2017 and 2018 based on the malware types. According on the figures shown in Table 1, Trojan has become the top malware infecting computers in 2017 and 2018 replacing Worms. For this report period (**H2 2018**), the Trojan malware detected is at 98.89% of the malwares detected. This show an increase of 25.33% from the previous period. There are various types of Trojan malwares detected, the highest being the CoinMiner Trojan, a malware that infects computer resources in order to mine digital currencies. Like other miners, it can cause infected computers to run slower than usual.

Comparing the trend in the previous reports, the Backdoor, Downloaders and Ransomware

detected in this project reduced tremendously compared to the first half of 2018.

...the Trojan malware is the most detected...

The malware threats classification details are provided in the “About the Project” section at the end of this report.

C&C CALLBACK DESTINATION

The command-and-control (**C&C**) servers are computers controlled by an attacker or cyber criminal that is used to send commands to systems compromised by malwares and receive stolen data from a target network. Spamhaus, an organisation that aggregates data on abusive web hosts as part of several blacklists, stated that the number of C&C servers used for managing IoT botnets has more than doubled in 2017 [6].

Figure 2 shows the distribution of malicious IP addresses serving as C&C servers by countries for the second half of 2018.

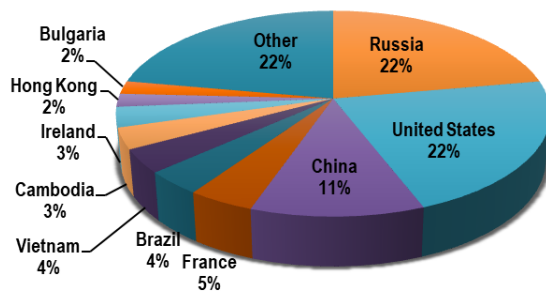


Figure 2: C&C Servers distribution

Figure 3 shows the data comparison and statistics of the top 10 callback destinations for H2 2018 and the previous statistics for respective origin.

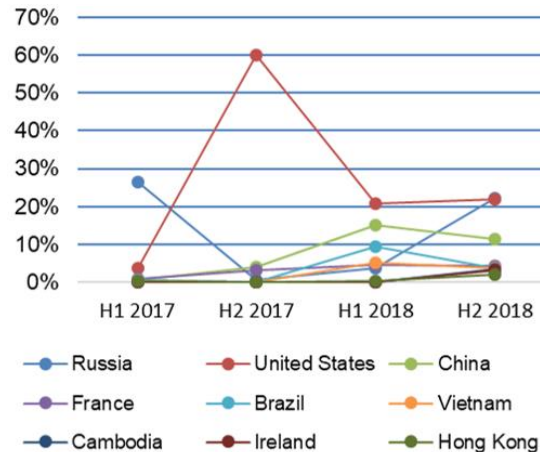
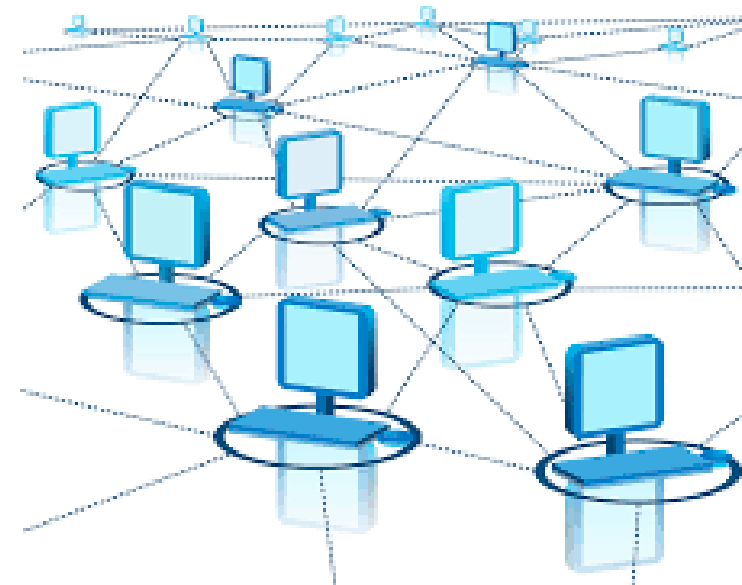


Figure 3: C&C Callback destination



PC THREATS

This section provides an overview of the personal computer (PC) threats. As shown in Table 2, Trojan is the main malware detected in Windows Operating System (OS) which is 75.6% from the total malware detected for Windows. Even though trojan contributed the highest percentage for Windows platform, Backdoor.Androm become the most prominent malware infecting the Windows based system as CoinMiner Trojan is placed second.



	Malware detected in the region		Most Common Malware
	H1 2018	H2 2018	
	Total 57.58% -Trojan 69.9% -Backdoor 2.3% -Downloader 27.8% -Others 0.0%	Total 63.93% -Trojan 75.6% -Backdoor 19.0% -Downloader 0.0% -Others 5.4%	Backdoor.Androm
	Total 34.82% Trojan 25.4% Downloader 0.5% Others 74.2%	Total 23.41% Trojan 90.6% Downloader 0.4% Others 14.5%	Backdoor.JBOSS.SHELL

Table 2: Overview of PC Malware threats

Malware targeting non-Windows based OS in second half of 2018 (H2 2018) is lower compared to the first half with a consolidated

aggregate of 23.41% (Trojan, Downloaders and Others malicious codes).

From Table 3 above, it also shows that for the second half of 2018, the malware identified as Backdoor.JBOSS.SHELL is the top malware detected for other OS in this project.

... malware activities targeting mobile OS are increasing...

Table 3 depicts the figures of the PCs and mobile threats detected during the period of this report. During this period, it is also found that the malware threats detected targeting PCs running on Windows and other OS is at 87.34%. It can be observed that malware activities targeting mobile OS are increasing whereas for the second half of 2018 they were at 12.66% as compared to the first half of 2018 which was at 7.60%.



Malware threat category	Malware activity detected in the Region,	
	H1 2018	H2 2018
 PCs	92.40%	87.34%
 Mobile (Android & iOS)	7.60%	12.66%

Table 3: PC vs Mobile malware threats

MOBILE THREATS

Mobile device security threats are on the rise. McAfee in 2018 reported that as of Q3 2017, more than 20 million of mobile malware were detected and more than 2.5 million are new mobile malwares [7]. These numbers make mobile security to be the top of every organisation's worry list these days. Nearly all workers now routinely access corporate data from smartphones, and this means that keeping sensitive information out of the wrong hands is an increasingly complicated puzzle [8].



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

Table 4: Mobile threats comparison of recent periods

Table 4 illustrates the mobile threats in H1 2018 and H2 2018. The Android presents a much bigger target for malware where the malware Android.Riskware.UuserV was detected as the most common malware in H2 2018.

ANDROID MALWARES

Rank	Malware	%
1	Android.Riskware.UuserV	69.26%
2	Trojan.Android.Guerrilla	7.14%
3	Android.Malware.Rooter	4.84%
4	Android.Malware.Axent	4.72%
5	Android.Malware.HiddenAd	3.20%
6	Android.Malware.Triada	3.09%
7	Android.Malware.HiddenAds	2.73%
8	Android.Malware.Clicker	2.07%
9	Android.Monitor.Spy	1.71%
10	Android.Malware.Shedun	1.23%

Table 5: Top 10 Android malware detected

Table 5 list the top 10 malwares detected infecting Android mobile users in this project. These malwares represent more than 95.9% of the total malware detected targeting Android smartphones.

Android.UuserV, is ranked the highest on Android malware detected in this period. Android.UuserV is a trojan that comes hidden in malicious programs. The malware will attempt to gain "root" access to the devices without the users' knowledge [9], [10].

NETWORK SERVICES & WEB THREATS

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.

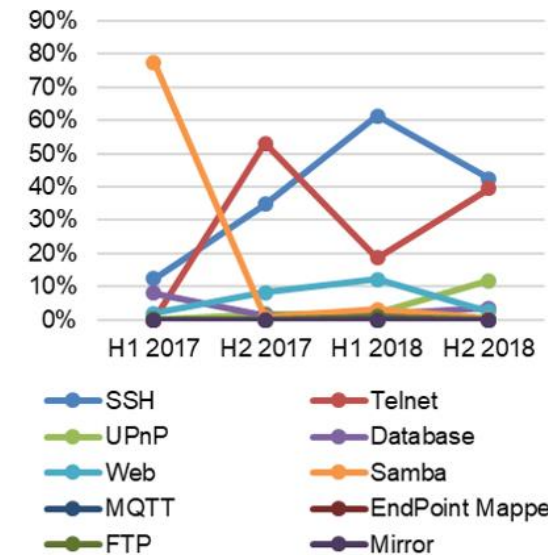


Figure 4: Overview of the targeted services

Referring to Figure 4, during the H2 2018 period, SSH services still becomes the main targeted services at 42.4%. Meanwhile, the number of Telnet attacks for the same period also increase compared to the first half of 2018. The attacks that target the web services also show a decrease from 12.1% to 2.6%. The Samba services attack detected also decrease from 3.1% to 0.3% in this project.

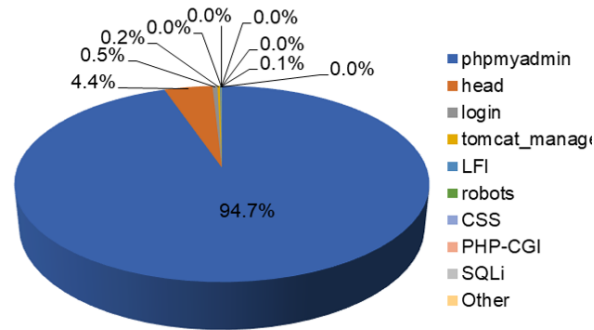


Figure 5: Overview of the targeted web application vulnerabilities

Figure 4 also indicate a huge increase in the attack involving phpMyAdmin from 48.8% in H1 2018 to 94.7% in H2 2018 which involved scanning activities to collect the details of the phpMyAdmin web application version. This information can be used to enhance further attack through vulnerability list.

Figure 5 shows that the activity of scanning using HEAD request is increasing slightly from 2.3% (H1 2018) to 4.4% (H2 2018). By utilizing the HEAD request the targeted server will only return the headers of a resource, rather than the resource itself [11]. This means the attacker can find out the Content-Type or Last-Modified of a document without downloading the resource. This information can be used when troubleshooting or when planning an attack against the web server.



... access corporate data
from smartphones, thus
keeping sensitive
information out of the
wrong hands is an
increasingly complicated
puzzle...

RANSOMWARE

For the period of this report, which is H2 2018, only 3 types of ransomware were detected as shown in the Table 8. Even though WannaCry global outbreak was 20 months ago, the WannaCry ransomware (99.40%) is still roaming around due to its nature which is self-propagating causing it to attempt to infect thousands of systems each month.

Ransomware	Detected
Ransomware.Wcry	99.40%
Ransomware.Downloader.Locky	0.52%
Ransomware.Win.GandCrab	0.09%

Table 6: Ransomware detected in H2 2018

Kaspersky Lab in their Q3 2018 threat report states that WannaCry ransomware top the list of the most widespread Cryptor families, with attempted attacks against 74,621 of the security firm's users across the globe between July and September. WannaCry ransomware attacks have risen in proportion of the total attack compared with the same period last year: in Q3 2017, Kaspersky figures suggest WannaCry accounted for 17 percent of ransomware attacks, but now that figure has

grown to account for 29 percent of all users targeted by ransomware [12].

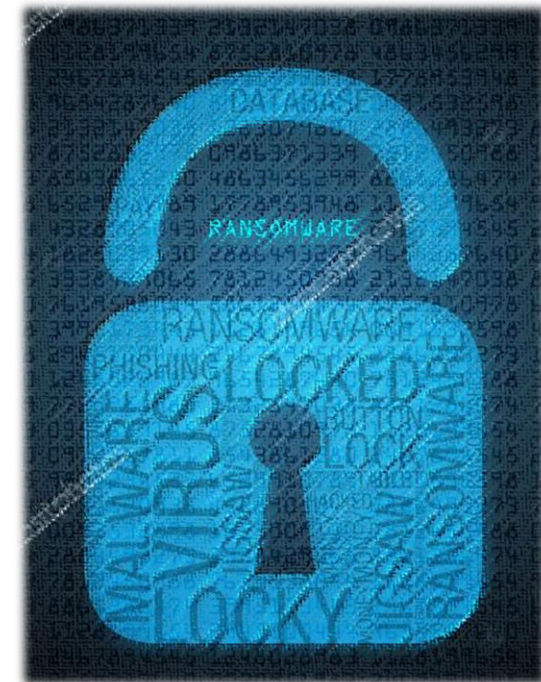
Locky (0.52%) is a type of ransomware released in 2016 by a group of highly skilled hackers. The malware spreads through fake emails and infected attachments, including .doc, .xls or .zip files. By using the social engineering technique, Locky trick victim by asking them to enable macro when opening the attachment [13].

GandCrab (0.09%) 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 [14].

CONCLUSION

Cyber threat analysis is a growing area of expertise due to the new challenges presented by modern cyber threats. In this report, the data are collected, analysed and produced from several sources for the purpose of extracting a holistic, evidence-based insights for the participating members. This report can make a significant difference to the parties' ability to

understand better the facts behind every cyber incident, before they occur, and the ability to respond quickly and proactively manoeuvrings defence mechanisms into place, prior to and during the attack. This report focuses on identifying and analysing the methods, capabilities and tools of adversaries who may seek to target an organisation by pairing external analysis with data that was once segmented within the organisation.



ABOUT THE PROJECT

Background

The Malware Research and Coordination Facility project was initiated by CyberSecurity Malaysia, which 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 9 lists the 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**) 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	<ol style="list-style-type: none"> 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 7: 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 <ul style="list-style-type: none"> • Desktop; • Laptop; and • Netbook. 	Linux / Unix Mac OS X Windows
Mobile	Mobile Devices <ul style="list-style-type: none"> • Smartphones; • Tablets/iPads; and • Wearables. 	Android iOS

Web	<p>Internet Browsers</p> <ul style="list-style-type: none"> • Internet Explorer; • Edge; • Chrome; • Firefox; • Opera; <p>Mobile Devices</p> <ul style="list-style-type: none"> • Safari, etc. <p>Servers</p> <ul style="list-style-type: none"> • Apache; • Internet Information Services, etc. <p>Personal Computers</p>	<p>Android</p> <p>Linux / Unix</p> <p>Mac OS X / iOS</p> <p>Windows</p>
Ransomware	<p>Mobile Devices</p> <p>Personal Computers</p>	<p>Android</p> <p>Linux / Unix</p> <p>Mac OS X / iOS</p> <p>Windows</p>

Table 8: Definition of the threat categories

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

Data Source

The data, information and analysis used to produce this Malware Trend Report H2 2018 are derived from the malware data generated by various sources within CyberSecurity Malaysia and the participating agencies / organisations in this project such as:

REFERENCES

- [1] Marriot International, "Starwood reservation database security incident," 2018. [Online]. Available: <https://answers.kroll.com/>. [Accessed: 10-Jan-2019].
- [2] J. Cook, "Private data of 500 million Marriott guests exposed in massive breach," *The Telegraph*, 2018. [Online]. Available: <https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/>. [Accessed: 10-Jan-2019].
- [3] H. Thompson and S. Trilling, "Cyber security predictions: 2019 and beyond," *Symantec*, 2018. [Online]. Available: <https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond>. [Accessed: 11-Jan-2019].
- [4] A. A. Ramaki and R. E. Atani, "A survey of IT early warning systems: architectures, challenges, and solutions," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4751–4776, Nov. 2016.
- [5] S. Z. Mohd Shaid and M. A. Maarof, "Malware behavior image for malware variant identification," in *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, 2014, pp. 238–243.
- [6] "Spamhaus Botnet Threat Report 2017." [Online]. Available: <https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017>. [Accessed: 17-Jan-2019].
- [7] McAfee, "McAfee mobile threat report q1, 2018," 2018.
- [8] A. Van Gysen, "Mobile device security," *Goldphish Ltd*, 2018. [Online]. Available: <https://goldphish.com/mobile-device-security/>. [Accessed: 11-Jan-2019].
- [9] Sophos, "Andr/Uuser-A," *Sophos Ltd*, 2013. [Online]. Available: <https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Andr-Uuser-A/detailed-analysis.aspx>. [Accessed: 18-Jan-2019].
- [10] J. Geater, "How to remove Android:Uuser-F," *Solvusoft Corporation*. [Online]. Available: <https://www.solvusoft.com/en/malware/trojans/android-uuser-fl>. [Accessed: 11-Jan-2019].
- [11] "HTTP/1.1: Method Definitions," *W3C*. [Online]. Available: <https://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html>. [Accessed: 11-Jan-2019].
- [12] V. Chebyshev, F. Sinityn, D. Parinov, O. Kupreev, E. Lopatin, and A. Liskin, "IT threat evolution Q3 2018. statistics," *Kaspersky Lab*, 2018. [Online]. Available: <https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/>. [Accessed: 02-Jan-2019].
- [13] Avast, "Locky ransomware." [Online]. Available: <https://www.avast.com/c-locky>. [Accessed: 18-Jan-2019].
- [14] 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 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 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