MALWARE TREND REPORT

H2 2016 : July – December 2016

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

List of Figures

List of Tables

EXECUTIVE SUMMARY

Having information access and sharing over the Internet are much easier with the use of Information and Communications Technology (**ICT**) and the advancement accomplished in this area. The government, private sectors, and individuals are relying on the Internet for their daily operations in economic growth, e-governance, business, and social as well as human development.

However, the increase usage and dependability on the Internet has also seen the rise of malicious activities such as cyber-attacks involving computer malicious codes or malwares. The evolution of malwares combined with the inexperience of Internet users makes such attacks detrimental to the victims.

It is important for organisations to realise that cyber criminals have the capability and capacity to inflict harm across 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.

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**) has embarked on the Malware Research and Coordination Facility project (hereinafter referred to as "the Project") as an initiative to enhance the mitigation of malwares. It is a collaborative effort of participants from the OIC-CERT members and information security organizations of multiple countries. The background of the Project and the participating agencies / organisations is available in **Appendix A**.

This Malware Trend Report, first published for the second half of 2016, is one of the outcomes of the collaboration effort.

1 INTRODUCTION

In the early 2010, the world observed a decline in the sales of personal computers (**PC**) and a rise in the sale of mobile devices such as smartphones, tablets, and more recently, the wearables. In a recent prediction by Gartner, the global PC market is expected to drop by 8% and the mobile phone shipment to decline by 1.6% in 2016 [1], indicating that the overall trend of using mobile devices instead of PC remains intact.

Portability and connectivity of these mobile devices encourage users to use applications ("**apps**") to perform more tasks, such as web browsing and emailing, using cloud-based services as well as seamlessly synchronising data between multiple devices. Unfortunately, the spread of computer malicious codes (malwares) are also moving in tandem with this.

More than three-quarters of the Internet-connected PCs worldwide are protected by real-time security software [2]. The security software constantly monitors the computers and network traffic for malware threats. For defined or known threats, the security software provides counter measures before they can infect the computers. Real-time protections for known threats are relatively effective; however, zero-day malwares are still prevalent.

Mobile devices are connected to 10 to 100 more networks than the traditional PCs [3]. Given the fast pace of mobile innovation and low barrier of entry for developing and publishing a mobile app, both apps and operating systems are usually full of vulnerabilities. According to Gartner, throughout 2015, more than 75 percent of the mobile apps failed the basic security tests [4] because the developers are more concerned with the functionality of the applications rather than its security.

1.1 Objectives

This Report aims to provide a better understanding of malware threats and analysis as well as related potential impacts. The ultimate objective is to educate and improve awareness, preparedness, and readiness in facing cyber threats.

1.2 Target Audience

The malware threat analysis presented in this Report is primarily for the consumption of the general Internet user

2 MALWARE TYPES

Malware, depending on the type and function, may be stealthy – intended to steal information or spy on computer users for an extended period of time without their knowledge, or it may be designed to cause harm – often as sabotage, or for financial gains – to extort payment from the users. Malware can infect any devices on any operating system (**OS**) platform

ranging from PCs to servers to smartphones and even smart TVs [5].

Figure 1 depicts the malware types infecting the computers during the implementation of this Project between July and December 2016. The malwares detected include Worms, Backdoor, Trojan, Downloaders, and Ransomware. The most common type of malware captured is Worms. As the anti-virus software evolved over time and nowadays become security suite, so does malwares which evolved from simple to complex, typically concealed in an application such as advertising-supported software (adware) that comes with spywares.

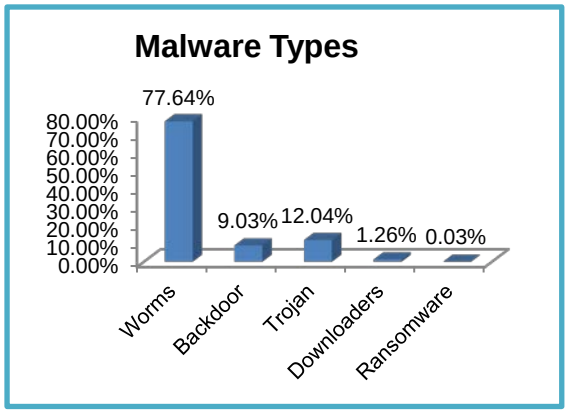

Figure 1 Captured malware types, H2 2016

In the first half of 2016, Microsoft released *Volume 21* of its half-yearly *Security Intelligence Report* using malware data from January to June 2016. One of the analyses available in this report is the comparison of infection and encounter rates, patterns, and trends in different locations around the world.

This analysis is made possible by the malware data generated by Microsoft security products from computers whose administrators or users choose to opt-in to provide data to Microsoft which includes information about the location of the computer, as determined by the IP geolocation.

The worldwide malware threats analysis, as included in Table 1, serves as a comparison reference to the threats detected in this Project.

Malware Types	Microsoft Security Intelligence Report	Malware Research and Coordination Facility
Worms	3.8%	**77.64%**
Trojans	11.3%	12.04%
Backdoors	0.4%	**9.03%**
Downloaders & Droppers	1.6%	1.26%
Ransomware	0.3%	0.03%
Browser Modifiers	**4.1%**	~0%

Table 1 Malware types comparison – Global vs Detected

Note: Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout"

The malware threats comparison above shows that the computers, servers, and users in this Project are infected primarily via Worms followed by Backdoors. The Malware infection detected through Worms is shockingly high at 77.64%, more than 20 times on those affecting the worldwide computers. Similarly, Trojan is the second common malware infection type at 12.04% and this figure is still relatively higher compared to the figures worldwide.

The Backdoors infection at 9.03% is alarmingly since the infection is more than 20 times the worldwide figure.

The Downloaders & Droppers are lower than the worldwide infection while the Ransomware, as a new comer, contributing 0.03% of the infection, is lower than the global figure of 0.3%.

By the first half of 2016, the global figures indicated that malware in the form of Worms have reduced in favour of Browser Modifiers. However, Browser Modifiers

are presently not a common malware detected in this Project.

The analysis shows two major trends: 1) malware types infecting the computers and users can be significantly different from one part of the world to another, and 2) malware threats evolve over time.

For the general Internet users, the malware type analysis above provides good knowledge but would probably provide little significance. Since the objective of this Malware Trend Report is to help the typical users at better understanding the malware threats and analysis as well as related potential impacts, the malware analysis presented and discussed in the following sections of this report have been reclassified.

The malware threats classification details are provided in **Appendix B**.

3 C&C CALLBACK DESTINATION

The callback destination of a malware to its servers, also known as the Command and Control (**C&C**), indicates that the computers and users involved in this Project have been exposed to infections. Malwares have successfully passed through the organisations' security perimeters and reach its internal hosts as there were large numbers of attempts towards the C&C servers observed.

From July to December 2016, the majority malicious IP addresses serving C&C servers came from the United States of America, Russia and the Netherlands. Figure 2 shows the top ten C&C countries that were identified as callback destinations which contribute to 75.34% of all countries serving C&C servers.

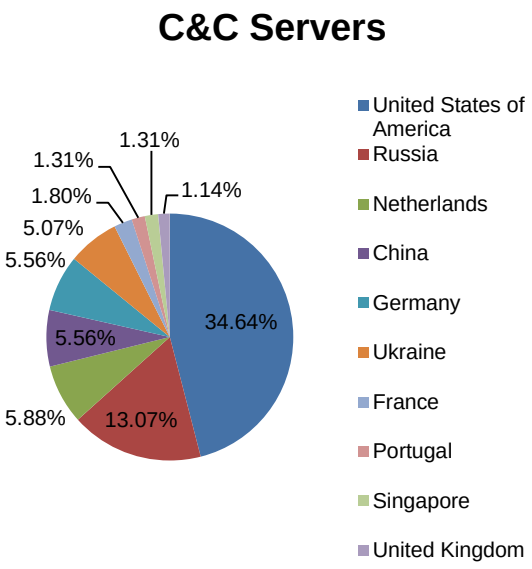

Figure 2 C&C servers distribution

4 PC THREATS

Global Operating System Market Share for Desktop PCs [6]		Malware Detected in the Region	Most Common Malware
	**Windows 83.13%** (XP, Vista, 7, 8, 8.1, 10)	**Total 58.34%** Backdoor 49.7% Trojans 43.3% Others 6.9%	**Backdoor.Androm**
	**Mac OS X 9.61%**	**Total 18.82%** Trojans 83.7% Adware 5.2% Others 11.0%	**Trojan.Malware. Sinkhole**
	**Linux 1.54% + Others 5.72%**		

Table 2 Overview of PC malware threats

The malware is as old as the software itself and PC running the Windows operating systems (**OS**) have been around for more than 20 years. By now, avid PC and Windows users are very familiar with the main symptoms of a malware infected system such as unwanted advertisement pop-up windows, anti-virus solution that doesn't seem to work properly or if the update module seems to be disabled, new browser homepage, and unwanted websites accessed without any input.

Table 2 shows the summary of global OS market share for desktop PCs for July 2016. The types of malware detected infecting the PC users in this Project and the most common malware between July and December 2016 are also highlighted. Compared to other operating systems, Microsoft Windows is the widely used OS globally at 83.13%. Mac OS X is currently at second place with 9.61% of the market share and the remaining 7.26% consists of other OS such as Linux and Solaris [6].

Windows, being the most used OS for PCs, is no doubt the common target of further malware threats. This known fact is supported since 58.34% of the malware detected in this Project infects Windows with its most prominent malware being the Backdoor.Androm. Malware threats targeting other OS has a combined total of 18.82% with the Trojan, Malware, and Sinkhole being the top malware detected during the second half of 2016.

Malware threats detected targeting the PCs running Windows and other OS is totalling to 77.16%. As such, 22.84% of the malware detected in this Project targets the mobile OS. Table 3 provides comparison between the PC and mobile threats detected globally as reported by Nokia, and the malwares detected in this Project.

Malware threat category	Global malware activity, H2 2015 (Reported by Nokia) [7]	Malware activity detected in the region, H2 2016
PCs (Windows)	22%	58.34% (18.82% for other than PCs-Windows)
Mobile (Android & iOS)	78%	22.84%

Table 3 PC vs Mobile malware threats

According to the *Nokia's Threat Intelligence Report*, for the first half of 2016, malware activities observed on smartphones running Android and iOS was ahead of Windows based computers and laptops and now account for 78%. The remaining 22% of the malware activity is still attributable to Windows PCs and laptops connected via dongles or tethered through phones [7].

5 MOBILE THREATS

Worldwide Smartphones and OS market share (2016) [8]	Mobile malware detected in the region	Most common malware
Android* 87.8 %	Android 91.2%	HiddenApp (Trojan)
iOS* 11.5%	iOS 8.8%	XcodeGhost (Backdoor)

Table 4 Overview of mobile threats

Note: * Remaining 0.7% are Microsoft 0.4%, RIM 0.1%, and Others 0.2%.

According to *IDC's Worldwide Quarterly Mobile Phone Tracker (January 27, 2016),* the world bought more than 1.4 billion smartphones in 2015, up by 10% from the 1.3 billion units sold in 2014. Ericsson predicts there could be as many as 6.4 billion smartphones subscriptions by the end of 2020, almost one smartphone per person [9].

Table 4 illustrates the key facts for mobile devices and its threats. Six (6) out of seven (7) or 86.2% new smartphones run on Android OS while one (1) in eight (8) runs Apple's iOS [8]. Holding the worldwide smartphone market share, it is no surprise then that Android, similar to Windows, is the main mobile operating system worldwide.

5.1 Android Malwares

Rank	Malware	%
1	Android.Malware.HiddenApp	41.11%
2	Android.Malware.Rootnik	26.48%
3	Android.Malware.GhostPush	10.62%
4	Android.Downloader	7.78%
5	Android.Malware.Guerrilla	3.37%
6	Android.Malware.Clicker	2.80%
7	Android.Malware.Kemoge.DNS	2.26%
8	Android.Riskware.Dropper	1.92%
9	Android.Malware.Ztorg	1.86%
10	Android.Malware.Kemoge	1.79%

Table 5 Top 10 Android malware detected

Table 5 list the top 10 malware detected out of 31 infecting the Android mobile users in this Project. These malwares represent more than 93% of the total malware detected targeting Android smartphones.

HiddenApp, the malware ranked highest on Android, targets the ever-expanding market of Chinese-Android device owners [10]. Once HiddenApp successfully infects a smartphone, it begins downloading and attempts to install android application packages (**APK**s) to external storage, like a secure digital (**SD**) card, without your knowledge. Those APKs could include spam, more malwares, or all sorts of other unwanted apps that could benefit the hacker at the victim's expense.

5.2 iOS Malwares

Apple's software repository, Apple Store, requires all submitted applications to pass a rigorous vetting process before they can be offered in the store, and has historically been admirably free of malware. Apple is well-known for its stringent screening processes, which is why the number of malicious iOS apps is so much smaller than for Android.

As Apple's mobile devices such as iPhones and iPads gain more market share, cyber criminals will most likely target Apple devices which are partly driven by the supposedly higher disposable income of their owners. iOS malware threats detected in this Project represent 8.8% of the total mobile malware detected. This figure is 4 times more than the iOS malware that Nokia reported at 2.07% of the total infections on the mobile platform [7].

Rank	Malware	%
1	**iOS.Malware.XcodeGhost**	41.11%
2	iOS.Malware.AceDeceiver	26.48%

Table 6 iOS malware detected

Table 6 provides the iOS malware detected in this Project. Unlike earlier versions of the iOS threats, the XcodeGhost malware does not require any iOS vulnerabilities or the iPhone /

iPad to be jail-broken in order to compromise the iOS device [9].

According to the *Internet Security Threat Report, Volume 21* by Symantec, in September 2015, malwares were discovered in a number of iOS applications that are legitimately available on Apple Store including WeChat, a popular cross-platform mobile instant messaging (**IM**) app. The worrying fact is that these apps are not intentionally designed to be malicious – their developers were compromised with malware that was embedded into the apps they develop [9].

6 WEB THREAT

Most users still surf the Internet from PCs but this behaviour is changing towards browsing from mobile devices. A joint study in the US in 2015 titled *The Generational Content Gap*, done by Fractl and BuzzStream, surveyed over 1,200 people across three generations about their digital content consumption. According to the survey, approximately 70% of the users browse the Internet using desktop and laptop. However, the Millennials, the generation born between 1977 and 1995, showed signs that this web browsing trend will change to browsing from mobile devices in the near future [11].

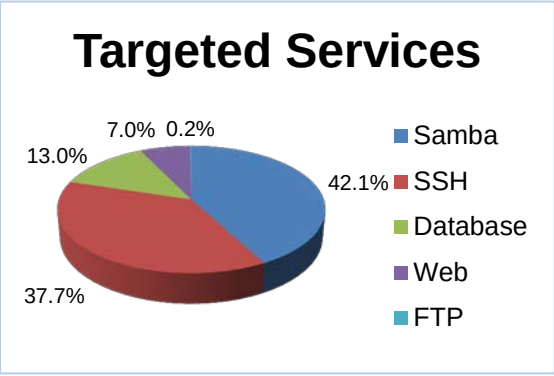

Figure 3 Overview of targeted services

Referring to Figure 3, apparently 7% of the malware is targeted specifically to the web services. However, it is common these days that web servers are connected to other related services including database and file sharing servers to provide users with more useful web applications and better browsing experience. In essence then, malware infection targeting the web is more than the obvious.

Through 7% of the malware or attacker are targeting the web service, referring to Figure 4, 31.4% of the malware or attacker is searching for phpMyAdmin web application version. This information is used in order to enhance further attack through vulnerability list based on its version information. 26.2% of malware or attacker is attempting to compromise phpMyAdmin web application using CVE-2009-4605 vulnerability. 17.9% of malware or attacker is collecting open public web proxy server information. The collected open public web proxy server can be used by an attacker as intermediary in order to access the Internet using the targeted proxy identity to hide their presence. The most popular web vulnerabilities detected in this Project are CVE-2009-4605, Open Web Proxy, Apache Tomcat default password, ShellShock and vulnerabilities existing in phpMyAdmin and WordPress.

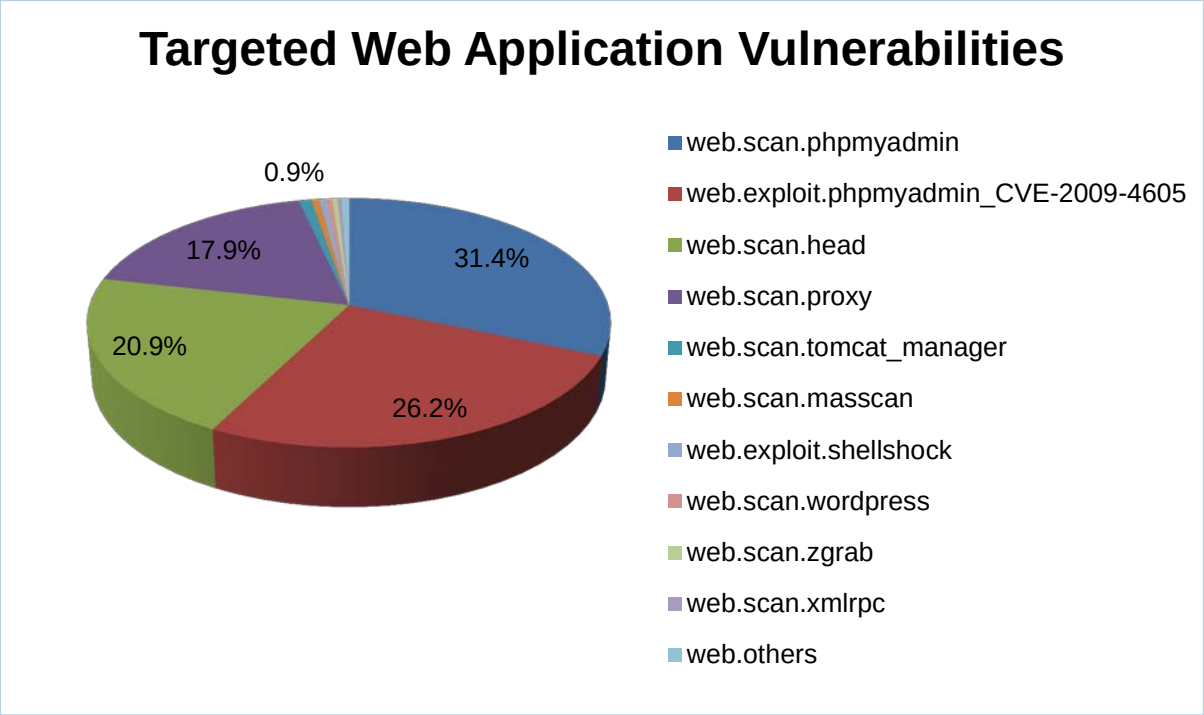

Figure 4 Overview of the targeted web application vulnerabilities

The ease of use and wide availability of web attack toolkits is feeding the number of web malware threats. In the middle of 2015, it was filled with accounts of malicious advertisement (malvertisement) affecting almost every segment of the ad-supported Internet.

On 19 March 2016, major news websites such as The New York Times, BBC, Newsweek and Aol.com began serving their visitors malware for the duration of the weekend. The malware did not come from these legitimate news pages; instead, the advertisements posted on these websites were remotely hijacked [12].

Table 4 lists the web threats detected within this Project. Malvertisement is the highest ranked web malware contributing to 83.26% of the web threats detected.

Rank	Malware	%
1	Exploit.Kit.**Malvertisement**	83.26%
2	Exploit.BeEF.Framework	5.17%
3	Exploit.Kit.TDS	3.31%
4	Exploit.Kit.Magnitude	2.69%
5	Exploit.Kit.Rig	1.65%
6	Exploit.Kit.Redirect	0.83%
7	Exploit.CVE-2014-6332	0.83%
8	Exploit.CVE-2016-0189	0.83%
9	Exploit.HTML.IframeRef.AA	0.62%
10	Exploit.Kit.MagnitudeRedirect	0.41%
11	Exploit.Kit.Goon	0.21%
12	Exploit.Dropper.url.MVX	0.21%

Table 7 Web threats captured – Exploit Kits

Malvertisements or adware are commonly placed on a website by one of these two ways:

- **Pop-up ads**: Pop-up ads typically deliver malicious payloads as soon as the ads appear on the user's screen. Scareware, disguised as an anti-virus application, is often delivered through pop-up ads. In some cases, the malware will execute when the user clicks the "X" to close the pop-up window; and
- **Legitimate ads**: Cyber criminals place a series of malware-free ads on a trusted site that runs third-party ads.

In order to establish a good reputation, the legitimate ads are left alone for a certain period of time, i.e. several weeks or even months. The cyber criminals will then inject malicious payloads into the ads, infecting as many computers as possible in a short amount of time. To avoid tracking, the malicious codes are quickly removed or the ads discontinued. This type of attack runs on websites that run third-party ads.

7 RANSOMWARE

Practicing safe web browsing should become a habit for all Internet users. Ransomware, despite being a relatively "newcomer", is similar to any other malwares in the sense that it can infect a user's PC or mobile device from practically any source including:

- Visiting unsafe, suspicious, or fake websites;
- Clicking on bad or malicious links in emails, Facebook, Twitter, and other social media posts, and instant messaging apps; and
- Opening emails and email attachments from unsolicited or unexpected sources.

Like other malwares, there are different types of ransomware. Figure 5 illustrates the ransomware detected globally as reported by Microsoft.

The figure shows that in the few months between December 2015 and May 2016, it can be seen the rise of Tescrypt globally.

Crowti remains near the top of the pack, as does FakeBsod and Brolo [13].

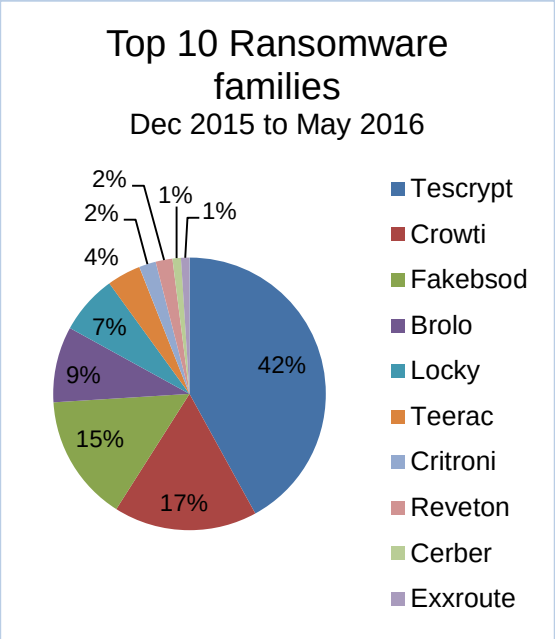

Figure 5 Prevalent ransomware – Global

Source: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

So, why have Ransomware attacks become increasingly sophisticated, targeted, and lucrative?

One of the reasons is that the profit potential cyber criminals use to gain from

exploiting stolen credit card details have reduced. This can be linked to the recent introduction of the more secure Europay, MasterCard and Visa (**EMV**) standard (chip-and-PIN) payment cards into the consumer market along with the abundant supply of stolen information on the black market.

Figure 6 shows the four ransomwares detected in this Project i.e. Petya, Cerber Downloader and Android.Congur. As stated earlier, malware types infecting the computers and users can be significantly different from one part of the world to another.

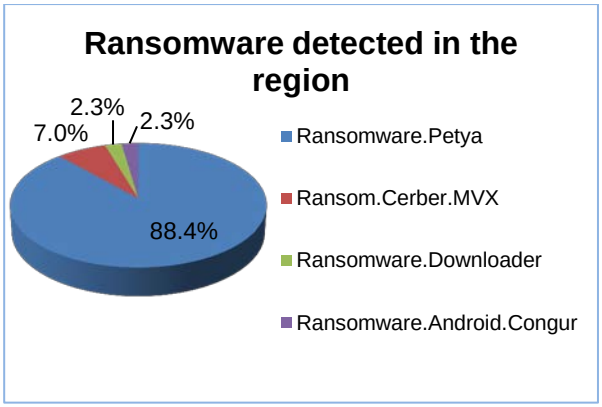

Figure 6 Regional ransomware

Petya is clearly the prominent ransomware making up 88.4% of the total ransomware detected during the second half of 2016. The ransom payments are at approximately 0.9 bitcoins (equivalent to US $657) and there is no way to decrypt hostage drives for free [14].

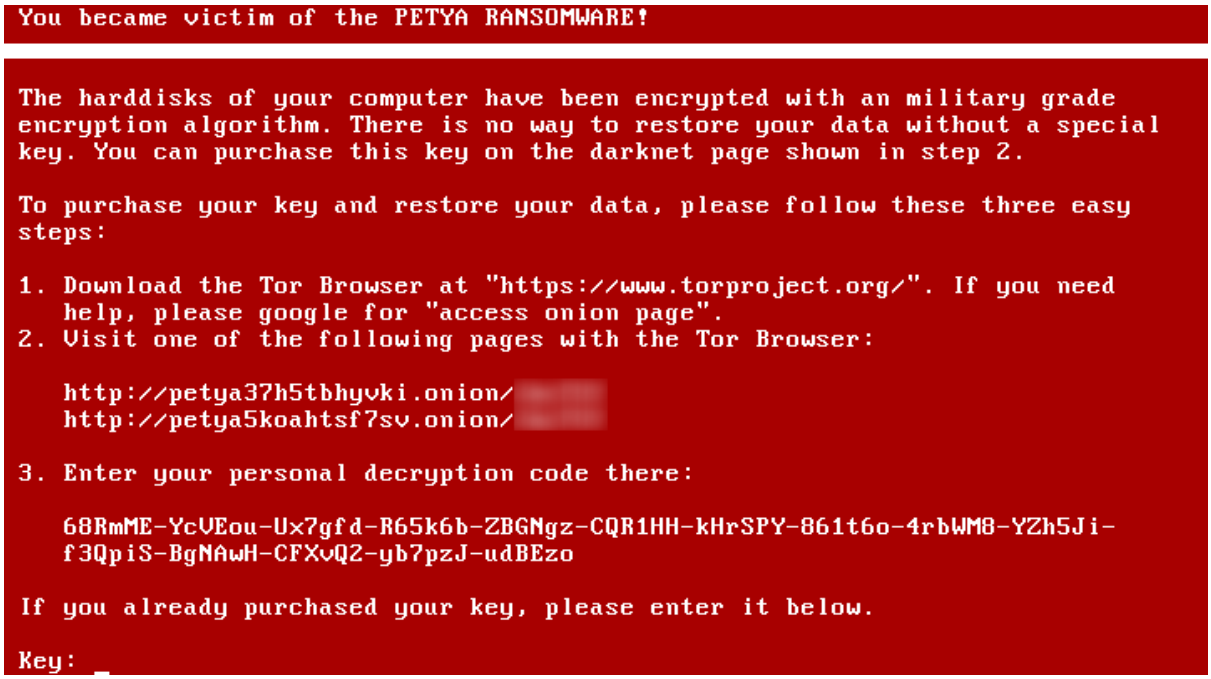

Figure 7 Petya ransomware screenshot

Figure 7 shows a snapshot of the Petya ransomware. Petya ransomware is delivered via scam emails themed as a job application. The e-mail comes with a Dropbox link, where the malicious ZIP is hosted. This initial ZIP contains two elements:

- a photo of a young man, purporting to be an applicant (in fact it is a publicly available stock image); and

- an executable, pretending to be a curriculum vitae (**CV**) in a self-extracting archive or in Portable Document Format (**PDF**), which is a malicious dropper in the form of a 32bit Portable Executable (**PE**) file.

8 CONCLUSION

Malware threats target vulnerabilities and / or operating system configurations as well as applications (commercial off-the-shelf or customized) that are unequally distributed around the world. Some threats reflect the online services offered by the government and industry sectors that are local to a specific geographic region or country.

The spread of malware can also be highly dependent on the socio economic factors as well as on the methods used for distribution (for example the ever-expanding market of Chinese-Android device vendors and cross-platform instant messaging apps). As such, significant differences exist in the types of threats that affect users in different parts of the world.

For better threat mitigation, information sharing of malware data and collaboration between related countries and organisations is crucial. It is learned, from McAfee's (Intel Security) interview of nearly 500 security professionals to understand their views and expectations about the sharing of cyber threats, that 97% of those who share cyber threat intelligence see value in it to help them to improve their preparedness and readiness to face the evolving cyber threats [15].

9 APPENDICES

9.1 A : Project Background

The Malware Research and Coordination Facility project was initiated by CyberSecurity Malaysia, an agency under the Ministry of Science 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, four countries that share their malware data include Malaysia, Brunei, and France. The services of the Malware Research and Coordination Facility are also offered to the Asia Pacific Computer Emergency Response Team (**APCERT**) through Memorandum of Understanding (**MoU**) between OIC-CERT and APCERT and APCERT Malware Mitigation Working Group.

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

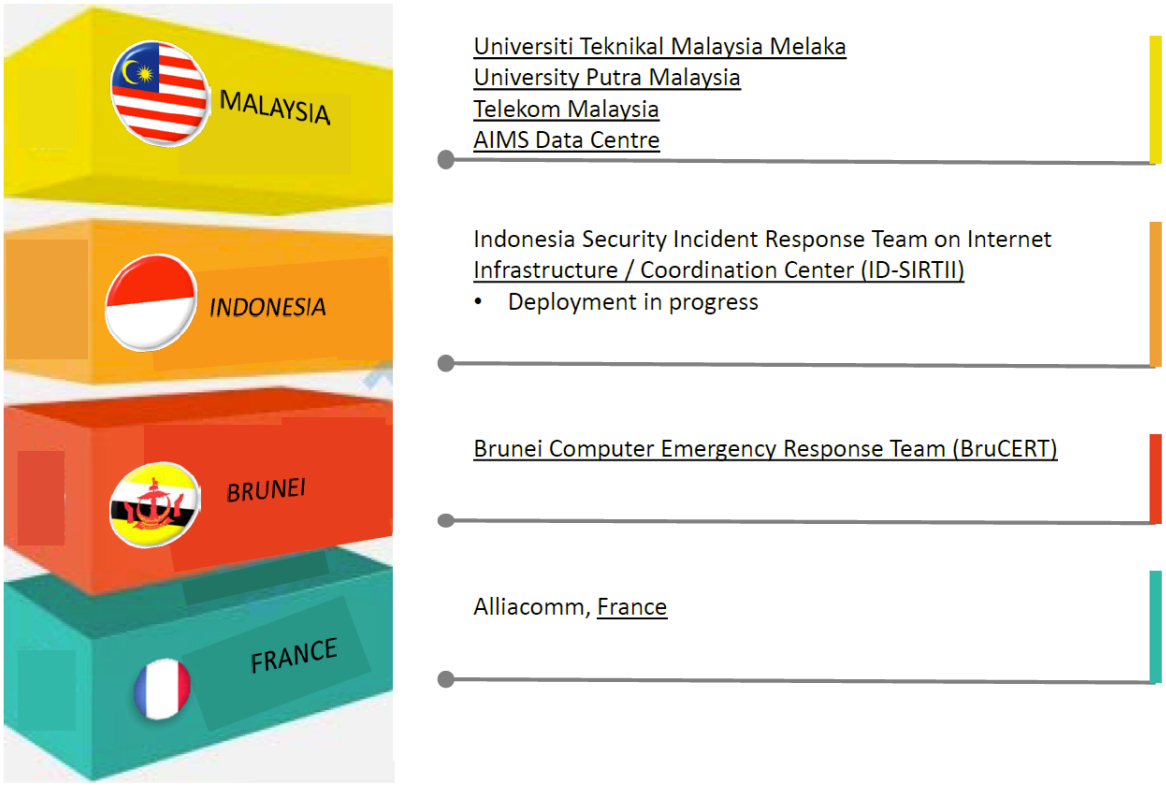

Figure 8 Participants for the Project

9.2 B : Threat Catergories

To simplify the presentation of the malware data and make the malware analysis easier to understand, this Malware Trend Report classifies the many types of malware threats into categories. Threat categorization 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 categorized as provided in Table 5.

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 8 Definition of the threat categories

9.3 C : Data Source

The data, information and analysis used to produce this Malware Trend Report H2 2016 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

9.4 D : References

[1] Gartner. (2016). *Gartner Forecasts Worldwide Device Shipments to Decline for Second Year in a Row* [Online]. Available: http://www.gartner.com/newsroom/id/3468817

[2] Charlie Anthe et al., “Microsoft Security Intelligence Report January throughJune, 2016,” Microsoft Corp., Redmond, WA, December 2016, vol. 21.

[3] Matt Louden. (2016, Jun. 1). *Mobility Menaces* [Online]. Available: http://mobiwm.com/technology/mobile-security/

[4] Gartner. (2014, Sep. 14). *Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015* [Online] Available: http://www.gartner.com/newsroom/id/2846017

[5] Mary-Ann Russon. (2016, Jan. 12). *It's official, your smart TV can be hijacked: Malware is holding viewers to ransom* [Online]. Available: http://www.ibtimes.co.uk/its-official-your-smart-tv-can-be-hijacked-malware-holding-viewers-ransom-1537533

[6] StatCounter. (2016, July). *Global operating systems market share for desktop PCs, from January 2012 to July 2016* [Online]. Available: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

[7] Nokia Threat Intelligence Laboratories, “Nokia Threat Intelligence Report – H1 2016,” Nokia Security Center, Berlin, September 2016.

[8] Gartner. (2016). *Global mobile OS market share in sales to end users from 1st quarter 2009 to 3rd quarter 2016* [Online]. Available: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[9] Paul Wood et al., “Internet Security Threat Report,” Symantec Corp., Mountain View, CA, April 2016, vol. 21.

[10] Jordan Minor. (2015, Aug. 31). *Mobile Threat Monday: By the Book* [Online]. Available: http://uk.pcmag.com/malwarebytes-anti-malware-for-android/70737/feature/mobile-threat-monday-by-the-book

[11] Fractl and BuzzStream. (2015). *The Generational Content Gap* [Online]. Available: http://cdn2.hubspot.net/hubfs/495782/Gated_Assets/Content_by_Generation/Content_Engagement_by_Generation_Whitepaper.pdf?submissionGuid=8ec61b78-5a9d-4289-b4ed-e35ff4b77791

[12] Carrie Mihalcik (2016, Mar. 16). *New York Times, BBC and others inadvertently serve up dangerous ads* [Online]. Available: https://www.cnet.com/news/new-york-times-bbc-dangerous-ads-ransomware-malvertising/

[13] Malware Protection Center. (2016). *Ransomware* [Online]. Available: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

[14] Alexander Gostev et al., “IT Threat Evolution in Q1 2016,” Kaspersky Lab, Moscow, May 2016.

[15] Diwakar Dinkar et al., “McAfee Labs Threats Report,” McAfee Part of Intel Security, Santa Clara, CA, March 2016.

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:

CyberSecurity MALAYSIA
An agency under MOSTI

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