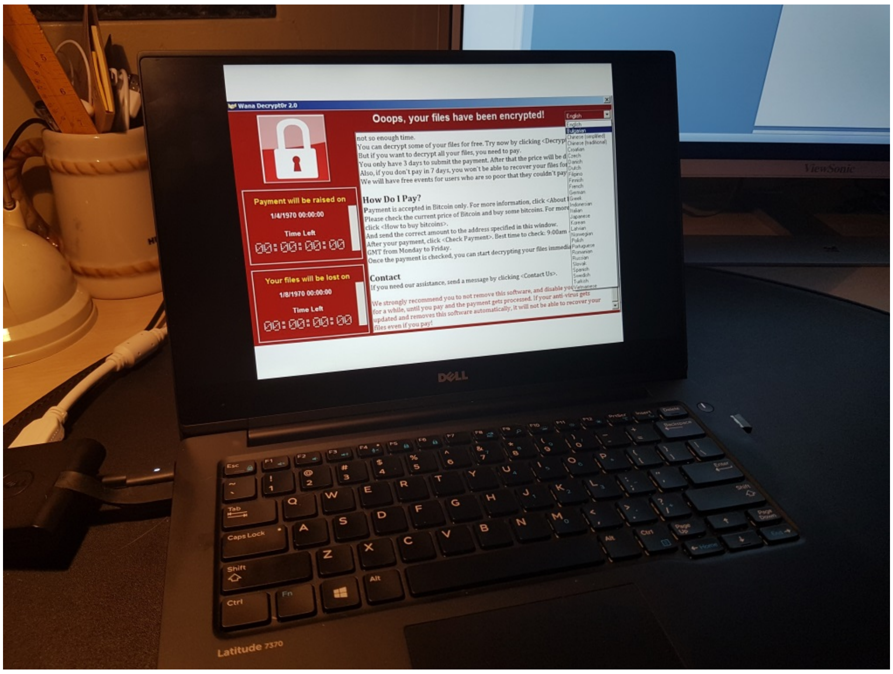
MALWARE TREND REPORT


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Payment will be raised on
Your files will be lost on
DELL
Latitude 7370

JULY 2017

H1 2017 : JANUARY – JUNE 2017

This is the 2nd report from the Malware Research and Coordination Facility Project, a cross border collaborative initiative.

The project is implemented by CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation of Malaysia and the Permanent Secretariat of the Organization of the Islamic Cooperation – Computer Emergency Response Team)

CyberSecurity MALAYSIA
An agency under MOSTI
Level 5, Sapura@Mines, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
+603 8992 6888
international@cybersecurity.my

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

Malware Trend Report

H1 2017 : January – June 2017

1 EXECUTIVE SUMMARY

In May 2017, the WannaCry ransomware attack has caught everyone by surprise. This cyber threat has launched a major worldwide attack which infected more than 2 million computers all over the world. The ransomware does not only attacked businesses, but also automatic teller machines (**ATM**), point-of-sale terminals, nuclear power plant and hospitals around the globe where it leads to the losses of hundreds of millions of dollars. While a large number of computer security teams were still struggling to patch their systems, came another global attack spreading the ransomware known as New Petya or NotPetya which behaves similar to WannaCry. Petya infects unpatched Windows devices by exploiting a vulnerability in the Server Message Block (**SMB**) server.

This report indicate that most of the malware detected are from Windows machine which is expected since the Windows Operating System (**OS**) is the most widely used and trailing far behind is the Mac OS X. On mobile devices, the main malware threats are found in Android apparatus since more than 85% of mobile devices are running on the android OS, which is followed by the iOS. This is the 2nd report of this project and in comparing the outcome with the 1st report, Russia, the USA, Ukraine, France and Germany are still the 5 top countries for callback destination.

RANSOMWARE
RESCUE PLAN
What is ransomware?
Ransomware is the term for malware that prevent or limit users from accessing their files or even computers. They force victims to pay ransom, usually in the form of Bitcoins, before they can get access back, hence the name.
PAY $$$ TO UNLOCK
Ransomware started preying on individuals but have since then become a huge threat to even the largest organizations. We've seen individuals, small businesses, and government agencies give in to ransom demands just to get back access to their files/systems.
How big is the ransomware problem?
Trend Micro blocked 100M+ ransomware threats September 2015–April 2016
Threats that use the ransomware business model spotted
50 new families (January–May 2016) > 49 families (2014–2015)
US$325M lost due to 1 ransomware family in 2015 – Cyber Threat Alliance (CTA)

The Malware Research and Coordination Facility project (**the Project**) is an initiative by CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation Malaysia and as the Permanent Secretariat of the Organisation of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) to provide analysis on malware threats to participating members and to enhanced the mitigation of malware threats. It is a collaborative effort by the participants from the OIC-CERT and the Asia Pacific Computer Emergency Response Team (**APCERT**) members and other information security organisations of various countries. The backgrounds of the Project and the participating agencies / organisations are available in **Appendix A**.

This OIC-CERT Malware Trend Report is published as one of the outcomes of the project.

2 INTRODUCTION

With the increase usage and dependability on the Internet, it is projected that cyber threats and cyber-attacks will be on the rise, which will lead to information and data breaches. Attacks involving computer malicious software (**Malware**) are geared for information and data breaches and will keep on evolving taking advantage of the new Internet technology and infrastructure.

Recently, the attack of the malware, WannaCry, classified as ransomware, had caught everyone by surprise. This worldwide attack has infected more than 2 million computers. WannaCry does not only attacked businesses, but also the automatic teller machines (**ATM**), point-of-sale terminals, nuclear power plant and hospitals around the globe where it leads to the losses of hundreds of millions of dollars.

Just when things were thought to subside and a large number of computer security teams were still struggling to patch their systems, another attack came using the ransomware known as New Petya or NotPetya which behaves similar to WannaCry. Petya infects unpatched Windows devices by exploiting a vulnerability in Server Message Block (**SMB**) server[1]. This ransomware encrypts the Master File Tree (**MFT**) tables for the New Technology File System (**NTFS**) partitions and overrides the Master Boot Record (**MBR**) of infected Windows computers, making the affected machines unusable.

Report's Objective:

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 as well as a deeper insight into the malware trends for the first half of 2017.

Target Readers:

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

As more and more devices are connecting to the Internet every day, this has provide cyber criminals with the opportunities to inflict greater harm to society. The increase in the growth of malware technology combined with the inexperience of new Internet users has made threats from malwares detrimental to the targeted parties.

Threat intelligence are curated data on the current or emerging cyber threat that can be shared for the purpose of enhancing defences against a specific cyber attack. It should offer insights on how the security teams can cooperate to minimise the impact of cyber-attacks on business operations. Through leadership within the threat intelligence sharing community and by developing technologies that are more easily shared and used[2], such insight will help internet users and organisations to identify and stop attacks.

The ransomware escalated across the globe as profit centres for criminals. Symantec identified 100 new malware families released into the wild[3], more than triple the amount seen previously, and a 36 percent increase in ransomware attacks worldwide.

3 MALWARE TYPES

A malware or malicious software is designed to intrude and damage computers without the users' consent. Malware which includes worms, spyware, viruses, and other malicious programs could be classified in several ways in order to differentiate them from one another and giving better understanding on how they infect. This report classified the best-known malware types that have been detected in this region which include Trojan, Worms, Backdoor, Downloaders, and Ransomware. Figure 1 represents the malware types detected in this region between January to June 2017.

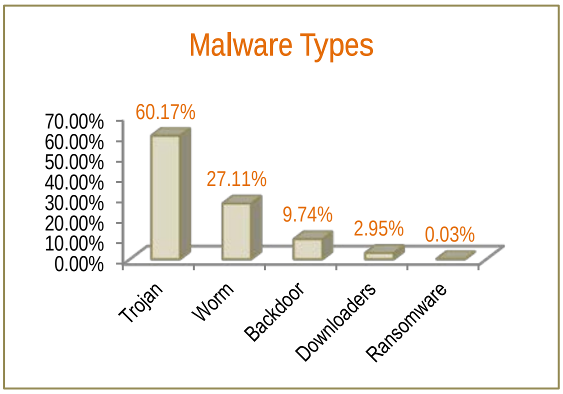


Figure 1 : Captured Malware types

The malware data detected in this project for the first half year of 2017 is compared with the second half year of 2016 and presented in Table 1. The malware types show that in the duration from January to June 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 60.17%, 5 times compared to previous report. In the previous second half year of 2016, worms are shockingly high at 77.64% compared to the first half year 2017 which is relatively lowed to 27.11%. The analysis shows that malware threats evolve over time.

Malware Types	H2 2016	H1 2017
Trojans	12.04%	60.17%
Worms	77.64%	27.11%
Backdoors	9.03%	9.74%
Downloaders & Droppers	1.26%	2.95%
Ransomware	0.03%	0.03%

Table 1 : Malware type comparison - H2 2016 vs H1 2017

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

4 C&C CALLBACK DESTINATION

The malware callback destination is referring to the Command and Control (**C&C**) servers which are centralised machines that are able to send commands and receive outputs of infected machines that are part of a botnet[4]. C&C servers are usually utilised by the attacker to send special commands to the infected machines mainly to launch coordinated cyber attacks.

Figure 2 shows the top ten C&C countries identified in January to June 2017 as callback destinations which contribute to 92.68% of all countries serving C&C servers. The major chunk of the malicious IP addresses serving C&C servers came from Ethiopia, Russia and Venezuela.

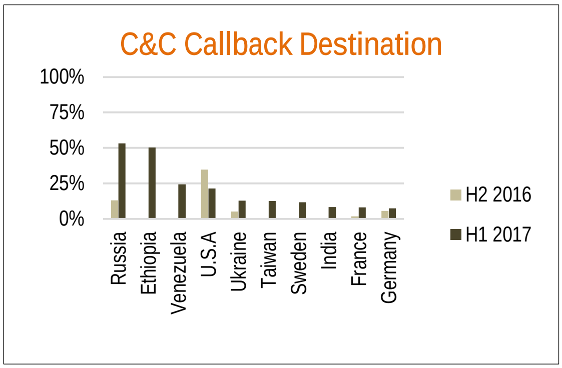


Figure 2 : C&C Servers distribution

The figure also shows data comparison of top 10 callback destination for H1 2017 and H2 2016, which five countries (Russia, United States of America, Ukraine, France and Germany) still remain in the top 10 callback destination for the two halves.

5 PC THREATS

No matter how sophisticated the tools used for protecting Personal Computers (**PC**s), there are still a rising number of threats to PCs especially to home users.

Global OS Market Share for Desktop PCs (February 2017) [6]	Malware Detected by the Project	Most Common Malware
Windows 84.14% (XP, Vista, 7, 8, 8.1, 10)	Total 61.87% Trojans 75.1% Backdoor 17.5% Downloaders 5.3% Others 2.2%	Trojan.Floxif
Mac OS X 11.6%	Total 22.41% Trojans 90.7% Adware 0.1% Downloaders 0.1% Others 9.1%	Trojan.Malware. Sinkhole
Linux 1.53% + Others 2.73%		

Table 2 : Overview of the PC malware threats

Table 2 shows the summary of the global operating systems' (**OS**) market share for desktop PCs for February 2017 and the types of malware detected in this Project. Compared to other operating systems, Microsoft Windows (**Windows**) is the widely-used OS globally at 84.14%. Mac OS X is currently at second place with 11.6% of the market share and the remaining 2.73% consists of other OS such as Linux and Solaris[5].

Windows become the main target of malware threats because a vast majority of the world's desktop computers and laptops are powered by Windows. By utilising the most used OS, the chances of the attackers to infect PCs are higher. This is supported by the findings in the first half of 2017 where 61.87% of the malware detected in this Project infects Windows. The most prominent malware detected is Trojan.Floxif. Malware threats targeting other OS has a combined total of 22.41% with the Trojan.Malware.Sinkhole being the top malware detected.

Malware threats detected targeting PCs running on Windows and other OS is totalling to 84.28%. As such, 15.73% of the malware detected in this Project targets mobile OS. Table 3 provides comparison between PCs and mobile threats detected globally as reported by Nokia, and the malwares detected in this Project.

Malware threat category	Malware activity detected for H2 2016	Malware activity detected for H1 2017
PCs (Windows)	**58.34%** **(18.82% for other than PCs-Windows)**	**68.17%** **(22.41% for other than PCs-Windows)**
Mobile (Android & iOS)	**22.84%**	**15.73%**

Table 3 : PC vs Mobile malware threats

In Table 3, malware activities observed on smartphones running Android and iOS are decreasing in the first half of 2017 to 15.73% compared to second half of 2016 where the figure was 22.84%.

6 MOBILE THREATS

Smartphones OS Global market share (Q1 2017) [8]	Mobile malware detected in the project	Most common malware
Android* 86.1 %	Android 99.8%	HiddenApp (Trojan)
iOS* 13.70%	iOS 0.2%	XcodeGhost (Backdoor)

Table 4 : Overview on Mobile threats

According to the global mobile OS market share in sales to end users from 1st quarter 2017 by Statista, six (**6**) out of seven (**7**) or 86.1% new smartphones run on Android OS while one (**1**) in eight (**8**) runs Apple's iO[6]. Holding the worldwide smartphone market share, it is no surprise then that Android is the main mobile operating system worldwide and also become the main target of malware threats with 99.8% of mobile malware detected is targeting windows Android.

6.1 Android Malware

Table 5 below list the top 10 malwares detected out of 37 infecting Android mobile users in this Project. These malwares represent 85.15% of the total malware detected targeting Android smartphones.

Ranking	Malware	%
1	Android.Malware.HiddenApp	27.86%
2	Android.Malware.Rootnik	13.74%
3	Android.Downloader	11.70%
4	Android.Monitor.TheTruthSpy	8.76%
5	Android.Malware.Kemoge.DNS	8.43%
6	Android.Riskware.Uuserv	7.14%
7	Android.Malware.Kemoge	6.59%
8	Android.Malware.GhostPush	6.46%
9	Android.Malware.Guerrilla	5.16%
10	Android.Malware.Clicker	4.15%

Table 5 : Top 10 Android malware detected

In first half of 2017, HiddenApp, the malware infecting Android is again ranked highest on Android malware. HiddenApp targets the ever-expanding market of Chinese-Android device owners[7]. 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 the user's 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.

6.2 iOS Malwares

In 2016, Palo Alto Networks, a security appliances company has discovered a new family of iOS malware named "AceDeceiver", which was able to infect non-jailbroken Apple mobile devices. AceDeceiver is the first iOS malware they have seen abusing certain design flaws[8]. This proves that even though Apple implement rigorous application vetting process, malware creators have found ways to infect the iOS.

As Apple 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 0.2% of the total mobile malware detected.

In this Project, there is only one (1) iOS malware detected which is iOS.Malware.XcodeGhost. Unlike earlier versions of the iOS threats, the XcodeGhost malware also does not require any iOS vulnerabilities or the iPhone / iPad to be jail-broken in order to compromise the iOS device[9].

7 WEB THREAT

Mobile devices are used more than traditional computers for web browsing nowadays, as smartphones and tablets usage overtook desktop for the first time. In March 2017, StatCounter released their findings on the total internet usage across desktop, laptop, tablet and mobile which shows that the Android (37.93%) has overtaken Windows (37.91%)[10].

Referring to the following Figure 3, Samba becomes the main targeted with 77.4%. The number of Samba attack for the first half 2017 is almost doubled compared to the second half of 2016. Samba is an implementation of Server Message Block

(**SMB**) where it is the transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services. SMB operates over TCP ports 139 and 445[11]. The recent WannaCry ransomware takes advantage of this vulnerability to compromise Windows machines, load malware, and propagate to other machines in the network. The attack uses SMB version 1 and TCP port 445 to propagate.

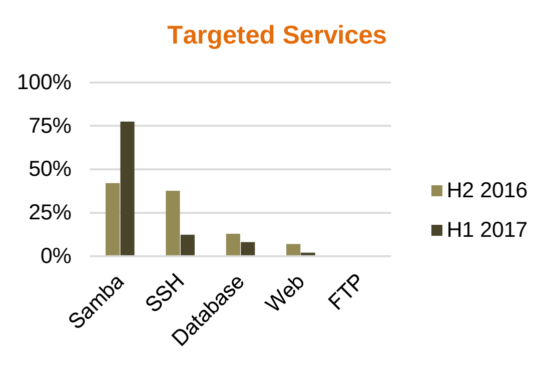


Figure 3 : Overview of targeted services

The Secure Shell (**SSH**), which is the cryptographic network protocol for operating network services securely over an unsecured network, becomes the second target with 12.3%. The best-known example for a SSH usage is for remote login to computer systems by users.

Web services apparently placed fourth with 2% where the malware is targeted specifically to the web services. By referring to Figure 4, 33.3% 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. On the malware or attacker 26.7% is attempting to compromise phpMyAdmin web application using CVE-2009-4605 vulnerability and 33.5% 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.

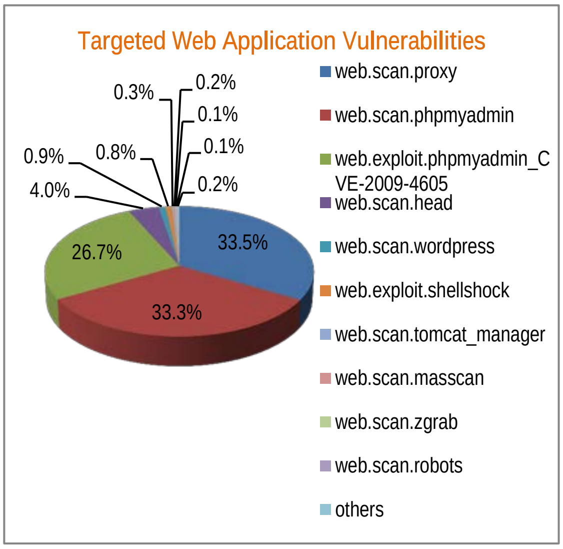


Figure 4 : Overview of the targeted web application vulnerabilities

The ease of use and wide availability of web attack toolkits are feeding the number of web malware threats.

Table 6 lists the web threats detected by this Project. Browser exploitation is the highest ranked web malware contributing to 45.65% of the web threats detected. The Browser Exploitation Framework (**BeEF**) is a penetration testing tool that focuses on web browsers. BeEF is a framework similar to Metasploit. BeEf uses a javascript named ‘hook.js’ which when executed by a browser, gives a hook to BeEF. This malware is able to view cookies, browser history to the more sophisticated attacks of getting a shell.

The BeEF launches a BeEF instance which is a combination of the user interface (**UI**) server (the UI which is used to launch attacks and shows the various exploits) and the communication server. This server coordinates and communicates with the hooked browsers. These 2 servers in collaboration makes BeEF work.

Ranking	Malware	%
1	Exploit.BeEF.Framework	45.65%
2	Exploit.Kit.MagnitudeRedirect	34.06%
3	Exploit.Kit.Magnitude	6.16%
4	Exploit.Kit.TDS	6.16%
5	Exploit.Kit.Rig	2.17%
6	Exploit.Kit.Malvertisement	1.81%
7	Exploit.HTML.IframeRef.AA	1.09%
8	Exploit.JSIframe.Psyme	1.09%
9	Exploit.Kit.Terror	0.72%
10	Exploit.Kit.Neptune	0.36%
11	Exploit.Kit.Sundown	0.36%
12	Exploit.Kit.Terror.Redirect	0.36%

Table 6 : Web threats captured - Exploit Kits

The BeEF allows professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exportability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

8 RANSOMWARE

Practicing safe web browsing should become a habit for all Internet users. Ransomware 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. Table 7 illustrates new ransomware detected globally as reported by Symantec in 2016[12].

No	Malware
1	Cerber
2	CryptXXX
3	Locky

Table 7 : New ransomware detected.

Ransomware attacks are now not only used to gain credit card information, but it is very much about the money. By exploiting system vulnerabilities that are difficult to patch, the attacker used the vulnerabilities to encrypt data and demands ransom for data decryption key. In recent attacks, WannaCry and NotPetya, the malware targeting computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency[13].

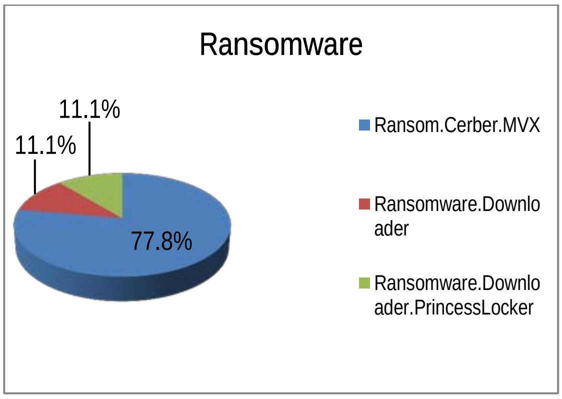
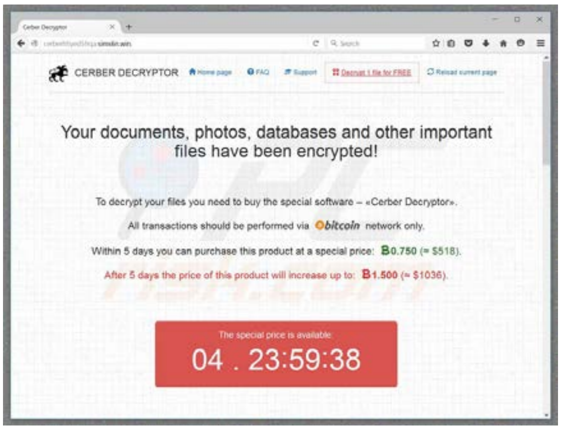


Figure 5 Regional ransomware

Figure 5 shows the three ransomwares detected in this Project i.e. Cerber, Downloader and DownloaderPrincess Locker. Cerber is clearly the prominent ransomware making up 77.8% of the total ransomware detected during the first half of 2017. The ransom payments are at approximately 1.24 to 2.48 bitcoins (equivalent to US $3,428.60 to $6,857.20 – July 2016 rates).



Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via bitcoin network only.

Within 5 days you can purchase this product at a special price: B0.750 (≈ $518).

After 5 days the price of this product will increase up to: B1.500 (≈ $1036).

The special price is available:

04 . 23:59:38

Figure 5 : Cerber ransomware screenshot

Figure 5 shows a snapshot of the Cerber ransomware. According to Margaret Rouse, Cerber ransomware virus is a destructive computer virus that encrypts victim's files with sophisticated encoding algorithm[14].

In April 2017, researchers identified new mutations in the distribution of this virus. The Cerber project is targeting vulnerabilities in the Apache Struts 2 on Windows servers, which the platform is free and open-source framework for creating Java web applications[15]. The researcher found out that malware distributors have been attacking systems running programs created with Apache Struts and setting up backdoors, enrolling devices into Distributed Denial of Service (**DDoS**) bot network, placing cryptocurrency miners and of course, malicious viruses like ransomware on compromised machines.

The vulnerability in Apache Struts software allowed criminals to target servers instead of individual computers, providing them with chances to reach potential victims that surely have money and most likely are willing to pay up just to get the control of the data back.

9 CONCLUSION

Mobile devices are rapidly overtaking home devices in the number of users. Research estimates that there will be more than six billion smartphone users by 2022[16]. These devices are replacing personal computers at home and in the workplace for everything from web surfing to ecommerce transactions to online banking.

Mobile devices are likely to be the main the target because application data, and the presence of a microphone, camera, text history, call history, and more, make smartphones a device where most sensitive data are located. Sophisticated exploits are becoming more prevalent, and malicious actors of all types have reasons to target these enterprise devices. Securing these devices should be a top priority both in business and personal use.

In combatting cyber threats which exist in various platforms, information sharing is an inexpensive and good approach. In order to achieve the information sharing objectives, removing barriers to information sharing is important. A lot of effort must be done to establish the trust, information sharing facilitation and multi-directional sharing of information. In other words, there need to be a clear framework for how organisations, both in the public and private sectors, can voluntarily share cyber threat and vulnerability information effectively.

10 REFERENCES

[1] GReAT, “WannaCry ransomware used in widespread attacks all over the world,” Kaspersky Lab, 2017.

[2] McAfee, “Threat Intelligence Sharing.” [Online]. Available: https://www.mcafee.com/us/security-awareness/threat-intelligence-sharing.aspx. [Accessed: 10-Jul-2017].

[3] K. Chandrasekar, G. Cleary, O. Cox, H. Lau, B. Nahorney, and B. O. Gorman, “Internet Security Threat Report,” Mountain View, CA, 2017.

[4] Radware, “DDoS Attack Definitions - DDoSPedia.” [Online]. Available: https://security.radware.com/ddos-knowledge-center/ddospedia/command-and-control-server/. [Accessed: 10-Jul-2017].

[5] Statista, “Global operating systems market share for desktop PCs, from January 2012 to July 2016,” 2017. [Online]. Available: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/. [Accessed: 10-Jul-2017].

[6] Statista, “Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 1st quarter 2017,” 2017. [Online]. Available: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. [Accessed: 10-Jul-2017].

[7] J. Minor, “Mobile Threat Monday: By the Book,” 2015. [Online]. Available: http://uk.pcmag.com/malwarebytes-anti-malware-for-android/70737/feature/mobile-threat-monday-by-the-book. [Accessed: 10-Jul-2017].

[8] Palo Alto Networks, “AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device,” 2016. [Online]. Available: https://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/. [Accessed: 19-Jul-2017].

[9] C. Xiao, “Update: XcodeGhost Attacker Can Phish Passwords and Open URLs through Infected Apps - Palo Alto Networks Blog,” 2015. [Online]. Available: https://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/. [Accessed: 10-Jul-2017].

[10] StatCounter, “Android overtakes Windows for first time,” 2017. [Online]. Available: http://gs.statcounter.com/press/android-overtakes-windows-for-first-time. [Accessed: 10-Jul-2017].

[11] A. Islam, N. Oppenheim, and W. Thomas, “SMB Exploited: WannaCry Use of &quot;EternalBlue&quot;,” FireEye Inc, 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html. [Accessed: 10-Jul-2017].

[12] Asim Rab et al., “An ISTR Special Report: Ransonware and Businesses 2016,” 2016.

[13] A. Raj, “Wanna Cry.. The Ransomware Attack,” 2017. [Online]. Available: http://www.cybervaultsec.com/2017/06/19/wanna-cry-ransomware-attack/. [Accessed: 10-Jul-2017].

[14] Margaret Rouse. Advanced Encryption Standard (AES). SearchSecurity. Information Security information, news and tips. http://searchsecurity.techtarget.com[Accessed: 10-Jul-2017].

[15] S. Sahu, “CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution,” 2017. [Online]. Available: http://blog.trendmicro.com/trendlabs-security- intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/. [Accessed: 10-Jul-2017].

[16] Ericsson, “Ericsson Mobility Report,” Stockholm, Sweden, 2016

11 APPENDICES

11.1 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:

MALAYSIA	Universiti Teknikal Malaysia Melaka Universiti Putra Malaysia Telekom Malaysia AIMS Universiti Malaya
INDONESIA	Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center (ID-SIRTII)
BRUNEI	Brunei Computer Emergency Response Team (BruCERT)
FRANCE	Alliacom
AUSTRALIA	Australia Computer Emergency Response Team (AusCERT)
JAPAN	Japan Computer Emergency Response Team / Coordination Center (JPCERT/CC)
TAIWAN	Taiwan National Computer Emergency Response Team (TWNCERT)

11.2 B : Threat Categories

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 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 follows.

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

11.3 C : Data Source

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