CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 42 - (1/2017)

Incident Trend Analysis for 2016

Cryptocurrencies 102 and the Dark side of the web

Ransomware WannaCry Attack! Are you at risk?

"Cybersecurity is a shared responsibility, and it boils down to this : In cybersecurity, the more systems we secure, the more secure we all are"

Jeh Johnson

ISSN 1985-1995

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia, an agency under Malaysia's Ministry of Science, Technology and Innovation was set up to be the national cyber security specialist centre. Its role is to achieve a safe and secure cyberspace environment by reducing the vulnerability of ICT systems and networks while nurturing a culture of cyber security. Feel secure in cyberspace with CyberSecurity Malaysia.

www.cybersecurity.my

Cyber999 Help Centre | My CyberSecurity Clinic | Professional Development (Training & Certification) | Product Evaluation & Certification (MyCC) | Information Security Management System Audit and Certification (CSM27001) | Malaysia Trustmark | Security Assurance | Digital Forensic & Data Recovery | Malaysia Computer Emergency Response Team (MyCERT) | Security Management & Best Practices | Cyber Security Research | CyberSAFE (Cyber Security Awareness for Everyone)

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

T: +603 8992 6888
F: +603 8992 6841
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

An agency under

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,

The opportunity of travelling from one continent to another, delivering speeches, participate in international conferences, and have the opportunities to meet people with relevant knowledge in the arena of cyber security landscape, one consistent theme I encounter, is that people are eager to hear the latest threats and case studies affecting that particular nation and how the organization counters those issues. People are interested to hear the “expert opinion” and what solutions may be offered and exchanged amongst the collaborating countries.

It gives me great pleasure to showcase 21 terrific articles in this first publication for e-Security Bulletin for 2017. You will be enlightened from the shared articles as well as will be kept abreast with the current and relevant issues on cyber and technologies landscape.

I believe that many of you are aware of the recent Ransomware Wannacry attack, whereby more than 200,000 machines in 150 countries worldwide have been infected. The threat has become the most severe and menacing cyber incident in the history of the Internet, after the DYN DDoS attack in October 2016. The article entitled “Ransomware WannaCry Attack! Are you at risk?” will provide you with a better grasp on the threat plus how to shield yourself from being a fallen victim. In addition, another article to be highlighted is the “Incident Trend Analysis for 2016” that could give you with more insights on the particular subject matter.

On that note, I would like to convey my utmost appreciation to all contributors for their nobility of sharing invaluable knowledge and also for their continuous support towards our goal of enhancing online safety.

We hope our readers will be more informed and equip with relevant knowledge on countering such threats.

Thank you and warmest regards.

Dato' Dr. Haji Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

Chief Editor
Dr. Zahri bin Yunos

Editor
Lt. Col Mustaffa bin Ahmad (Retired)

Internal Reviewers
1. Mohd Shamil bin Mohd Yusoff
2. Ramona Susanty binti Ab Hamid
3. Nur Arafah binti Atan
4. Jazannul Azriq bin Aripin

Designer & Illustrator
1. Zaihasrul bin Ariffin
2. Nurul Ain binti Zakariah

READERS' ENQUIRY
Outreach and Corporate Communications, Level 5, Sapura@Mines, No.7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia,
Level 5, Sapura@Mines,
No. 7 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

TABLE OF CONTENTS

1. 5 Common Social Engineering Tactics 1
2. Embryonic Cyber Security Products 3
3. Malware Trend Report H2|2016 6
4. Incident Trend Analysis for 2016 17
5. Cryptocurrencies 102 and the Dark side of the web 20
6. Social Networking Security and Privacy 26
7. Blockchain Implementation (Proof-of-Concept) 30
8. Email Security Threats and Trends 34
9. Cyberbalkanization/Splinternet 37
10. Going for Digital Detox 40
11. CyberSAFE Tips for Parents 'Educate your Child! Say No to Cyber-Bullying' 43
12. Zooming In Cyber Security Market Development 45
13. Approved Cryptographic Algorithms in ISO/IEC Standards 49
14. Approved Cryptographic Algorithm in NCA[1] Projects 55
15. Cryptography and Virus 60
16. Lightweight Cryptography in Internet of Things 63
17. Ransomware WannaCry Attack! Are you at risk? 68
18. Mobile Security: Android OS vs iOS 70
19. CyberSecurity Malaysia New Building at Cyberjaya 75
20. Certificate vs Certification 76
21. Cyber Security Terms That We Should Alert 77

5 Common Social Engineering Tactics

By | Nur Sharifah Idayu binti Mat Roh & Noraziah Anini binti Mohd Rashid

A social engineer is someone who uses techniques of deception, persuasion, and influence to obtain information that would otherwise be unavailable. Social engineering is different from hacking in the aspect of obtaining information, whereby social engineers get access to confidential information with the victim's consent. Basically, they are con artists who are good at convincing you to give your information outright by manipulating you into thinking they are a trusted party. In other words, it is not about being a good liar; it is about being an ordinary person who finds extraordinary ways to manipulate people to their advantage. By using a variety of media, including phone calls and social media, these hackers trick people into offering access to sensitive information. Social engineers use a variety of techniques to achieve their goals. However, this article will focus on five common types of attacks that social engineers normally use to target people:

1. Phishing
2. Baiting
3. Pretexting
4. Quid Pro Quo
5. Tailgating.

#1. Phishing

Phishing is a type of social engineering attack that is usually delivered in the form of e-mails, chats, web advertisements or sites designed to impersonate real systems or organizations. Phishing messages are designed to convey a sense of urgency or fear with the end goal of capturing sensitive end-user data. Phishing messages may come from banks, the government or major corporations. Phishing scams may be the most common type of social engineering attack used today. Most phishing scams exhibit the following characteristics:

1. Attempts to obtain personal information, such as name, address and social security number.
2. Use link shorteners or embedded links that direct users to suspicious URL websites that look legitimate.
3. Combine the threat with fear and a sense of urgency in order to manipulate a user into immediate action.
4. A phishing message may come from a bank, the government or a large corporation.
   - Call for different actions. Some ask the person to "verify" their account login information, and include a login mock-up page complete with a logo and brand to appear legitimate.
   - Some claim the person is the "winner" of a prize or lottery and request bank account details to deliver the prize.
5. Submit phishing e-mails to users after they installed the crack to a Google Play APK file that is pre-loaded with malware. This particular phishing campaign shows how malware attacks are usually paired with phishing attacks in an attempt to steal users' information.

#2. Baiting

Baiting is similar to phishing, in that it involves offering an item or good that hackers use to attract victims. The "bait" comes in many forms, either digital, such as peer-to-peer music or movie downloads, or physical. Baiting attacks are not limited only to the online scheme. Hackers can also focus on exploiting human curiosity through the use of physical media. For example:

1. Baiters can offer users a free music or movie download when they submit their login credentials to a specific website.
2. Hackers infect USBs with a Trojan virus and disperse them throughout an organization's parking area. Out of curiosity, many workers will take the USB and plug it into their computers, thus automatically enabling a keylogger and providing hackers access to certain employee login credentials.

#3. Pretexting

Pretexting is the human equivalent of phishing. Pretexting is defined as the practice of presenting

© CyberSecurity Malaysia 2017 - All Rights Reserved

oneself as another and creating good reasons or scenarios designed to obtain personal information. One of the most important aspects of social engineering is trust. A solid ground is an essential part of building trust. Examples of pretexting include:

1. An e-mail to employees from what appears to be the Head of IT support, or chat messages from an investigator claiming to conduct corporate audits.
2. Posing as external IT service staff auditors and manipulating the physical company security to allow them into the building.

#4. Quid Pro Quo

Much like baiting, quid pro quo attacks involve hackers asking for critical data or login credentials in exchange for services. For example:

1. Fraudsters posing as IT services, spam calling direct numbers of end users to offer free help or IT technology improvement in exchange for login details.
2. Posing as researchers, requesting access to the company network as part of an experiment in exchange for a certain amount of money. If an offer sounds too good to be true, it is probably a quid pro quo attack.

As real-world examples show, some office workers are more than willing to give their passwords for treats of a meal or chocolate bar.

#5. Tailgating/Piggybacking

Last but not least, another type of social engineering attack is tailgating, which is also known as piggybacking. The attack involves someone who does not have proper authentication but follows workers to access protected system areas. For example:

1. Someone asks to borrow an employee's laptop for a few minutes, when the hacker is able to quickly install any malicious software on the laptop.
2. A hacker can strike up a conversation with an employee and use some sorts of presentation or persuasion skills to make it past the front desk.
3. Hackers request workers to hold the door open for them as they claim having forgotten their employee access cards.

Conclusion

All employees should be aware of the various forms of recent social engineering to ensure that corporate cyber security is preserved. Attending security awareness training is one way to reduce the risk of being hacked, which can simply equip employees with security knowledge and security best practices. Another method is for the organization to carry out breach exercises on the organization's physical access using social engineering techniques. This can be very helpful for employees to understand how people can be easily manipulated and persuaded by others. Thus, it is more likely they can prevent attacks before sensitive information gets exposed and the organization can also identify which employees need further awareness.

References

1. http://searchsecurity.techtarget.com/definition/social-engineering

2. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

3. http://www.social-engineer.org/framework/influencing-others/pretexting/principles-planning/

4. http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

5. http://www.informit.com/articles/article.aspx?p=1350956&seqNum=11

© CyberSecurity Malaysia 2017 - All Rights Reserved

Embryonic Cyber Security Products

By | Nazahan bin Nazri

Developing a secure ICT product obviously requires it is designed, built and operated by people who understand the threats, know the security requirements and also have general skills.

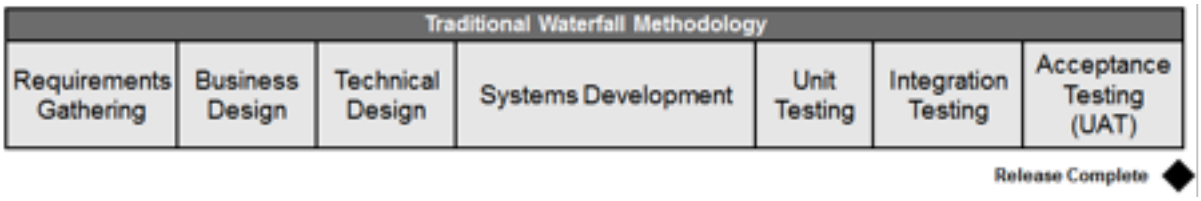
Most products fail due to problems relating to the development process. The inability to coordinate different teams, resolve personal conflicts, or respond effectively to unforeseen technical difficulties are all common problems. Without an adequate process in place to respond to any concern, products can get lost or side-tracked, and stall or fail to meet even basic requirements.

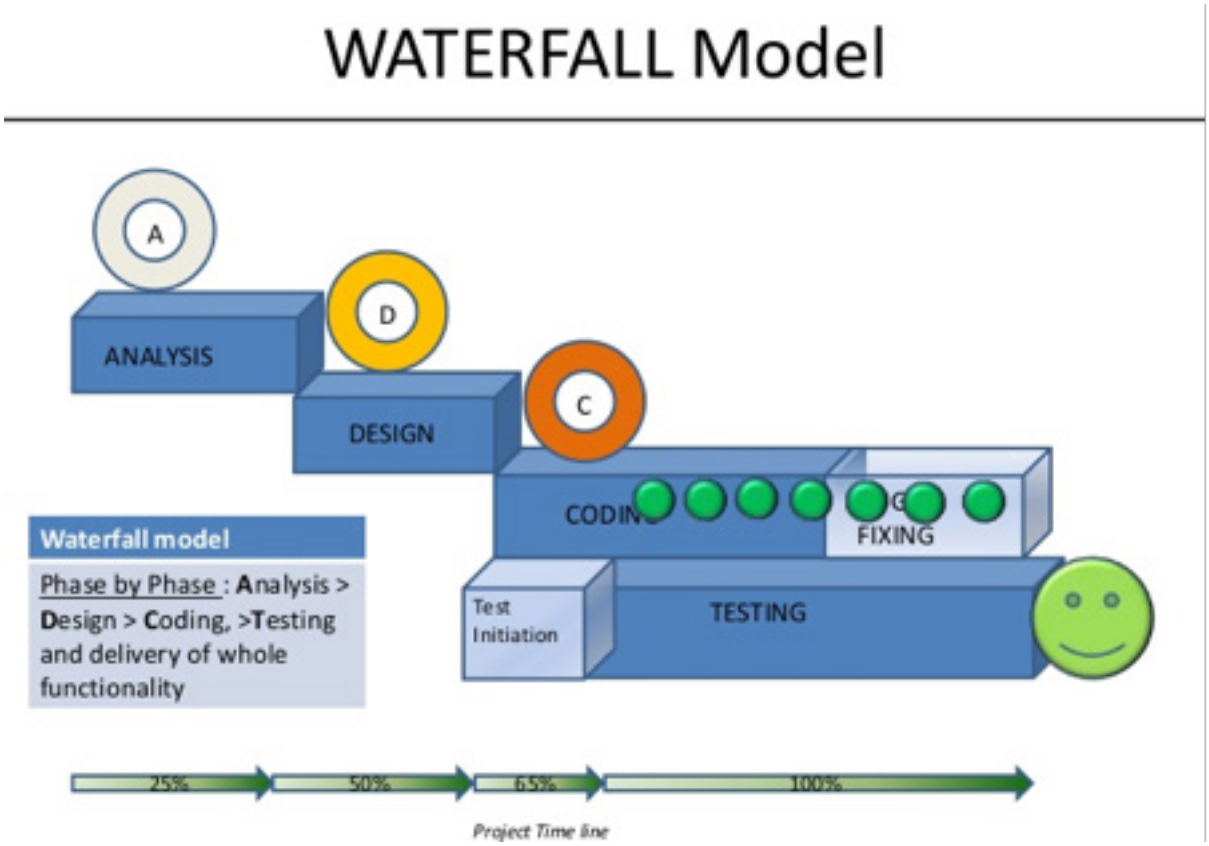
The Embryonic Process

Most organizations utilize a hybrid iterative-waterfall methodology to facilitate quicker development cycles and the ability to adapt to changes through the process.

The waterfall model is a sequential product development process, whereby progress is considered to be flowing steadily downwards (like a waterfall) through the phases of requirement gathering, analysis, design, development, unit testing, integration testing, acceptance testing and release.

This model is best applied when the requirements have been determined, clear, and fixed, the product definition is stable, and the technology is well-understood. In addition, the product will have no ambiguous requirements, and sufficient resources with the required expertise will be accessible.

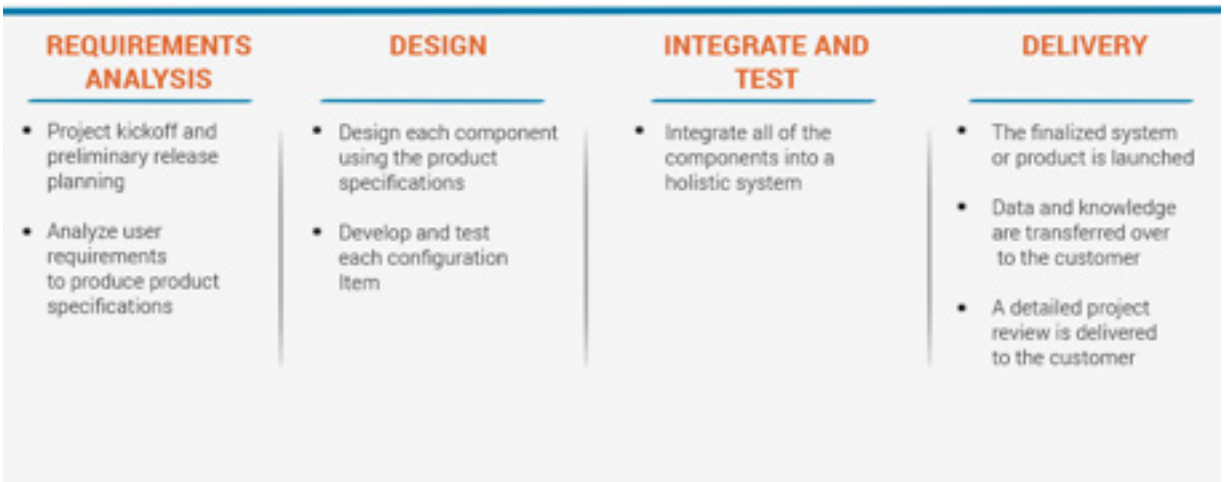




© CyberSecurity Malaysia 2017 - All Rights Reserved

The waterfall development model originated in the manufacturing and construction industries for highly structured physical environments, where **after-the-fact changes are prohibitively costly,** if not impossible. Since no formal software development methodologies existed at the time, this hardware-oriented model was simply adapted for software development.

The main advantage of using the waterfall approach is that time spent **early in the software lifecycle** can lead to **enhanced economy** in later stages. For example, a bug found in the early stages (e.g. requirement specification or design) is cheaper in terms of money, effort, and time to fix than the same bug found later on, once development has started.



Requirement Analysis

To develop a successful product, a clear understanding of what the client needs and is planning to use the product for is necessary. The product must also be able meet all of the client's expectations and do exactly what the client wants.

The very first step is to analyse the user requirements. The functional requirements of the product are analysed and ways to meet those requirements are examined.

Tensions may erupt between various departments within a firm. To alleviate any stress and avoid conflict it is possible to create an integrated product team with one point person to represent each interest. In this phase, frequent meetings are held to ensure everyone's concerns and needs are met and considered.

Understanding the requirements and allocating resources efficiently can drastically reduce development time as well as potential errors, technical glitches and miscommunication. These are major reasons for attempting to lower cost and save time.

Design & Implementation

In the next phase, the product specs are put into action to develop and test each configuration item. Each item is designed and built according to the specifications established in the initial phase. With a clear understanding of the end requirements, the design and development process flows more smoothly and easily.

Integration & Testing

After building and testing the configuration items, or discrete components, separately, they are integrated into a holistic system to ensure they work together harmoniously. Since there is already a requirement-based plan for integration and testing, this phase becomes cost and time-efficient.

Delivery

All the mentioned steps lead up to the final moment: product or system delivery, ready for use. However, delivery processes have different degrees of metrics that involve product deployment. Moreover, the value chain stream depends on client requirements.

© CyberSecurity Malaysia 2017 - All Rights Reserved

Conclusion

The model is simple, and easy to understand and use in the product development phase. The model is also easy to manage due to its rigidity – each phase contains specific deliverables and a process review. With this model, phases are processed and completed one at a time, so the phases do not overlap. Ultimately, the waterfall model works well for projects if the requirements are very well-understood.

References

1. Product Methologies; https://www.inflectra.com/Methodologies/Waterfall.aspx

2. Waterfall Model; http://istqbexamcertification.com/what-is-waterfall-model-advantages-disadvantages-and-when-to-use-it/

3. Cybersecurity challenge; http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge

4. Cybersecurity product thru secure development; http://folk.uio.no/josang/papers/JOO2015-WISE.pdf

© CyberSecurity Malaysia 2017 - All Rights Reserved

Malware Trend Report H2|2016

By | OIC-CERT Permanent Secretariat

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.

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.

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.

© CyberSecurity Malaysia 2017 - All Rights Reserved

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.

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.

Target Audience

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

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.

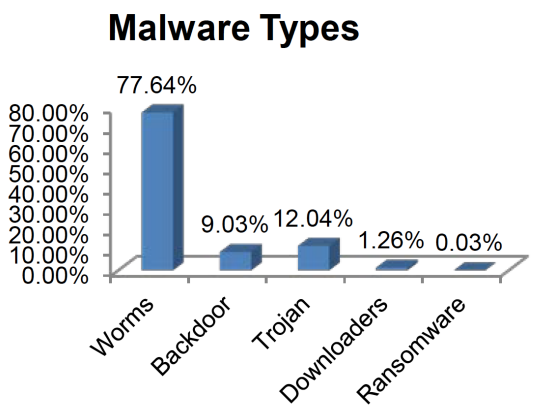


Figure 1 Captured malware types, H2 2016

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

© CyberSecurity Malaysia 2017 - All Rights Reserved

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.

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.

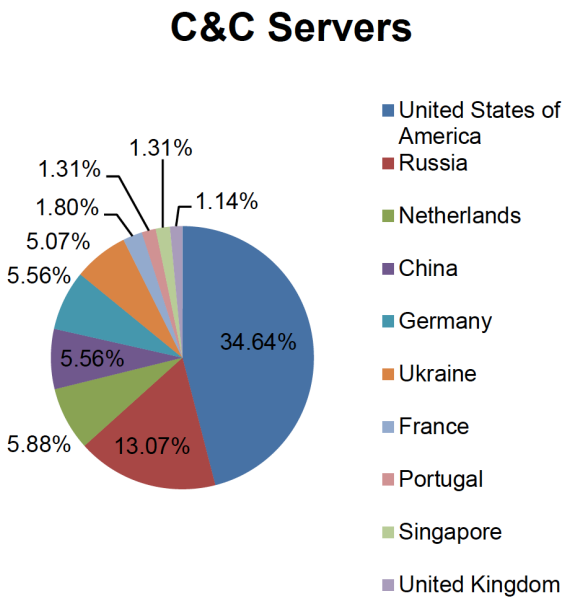


Figure 2 C&C servers distribution

© CyberSecurity Malaysia 2017 - All Rights Reserved

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 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

© CyberSecurity Malaysia 2017 - All Rights Reserved

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.

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].

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.

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

© CyberSecurity Malaysia 2017 - All Rights Reserved

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 (APKs) 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.

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].

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].

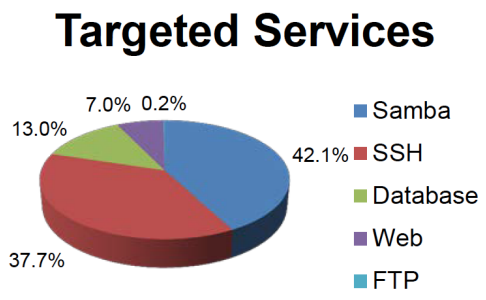


Figure 3 Overview of targeted services

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.

© CyberSecurity Malaysia 2017 - All Rights Reserved

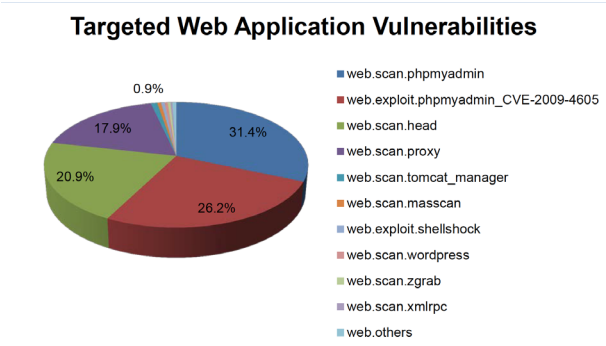


Figure 4 Overview of the targeted web application vulnerabilities

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.

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].

© CyberSecurity Malaysia 2017 - All Rights Reserved

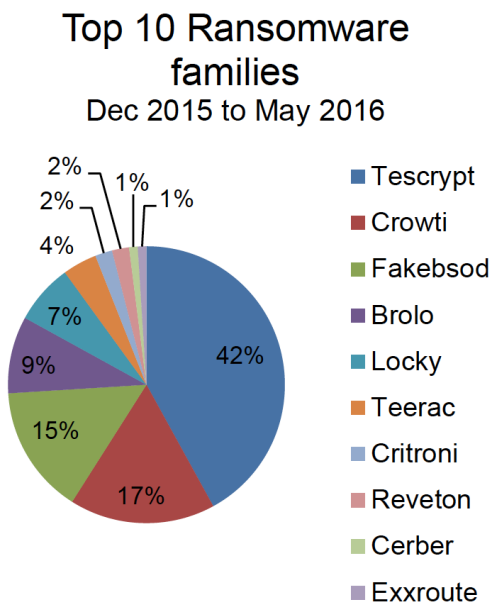


Figure 5 Prevalent ransomware – Global

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.

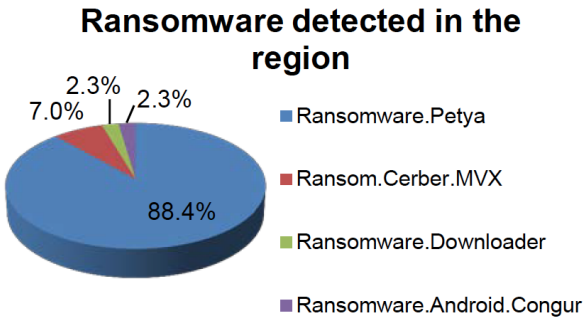


Figure 6 Regional ransomware

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].

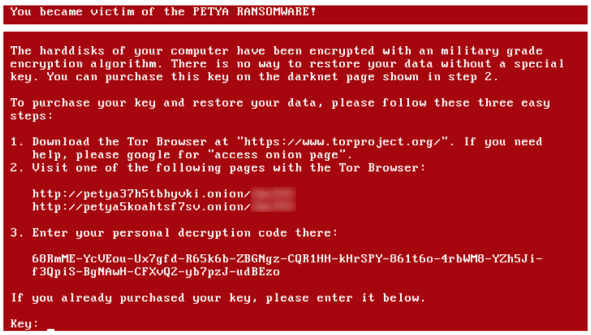


Figure 7 Petya ransomware screenshot

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.

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

© CyberSecurity Malaysia 2017 - All Rights Reserved

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].

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:

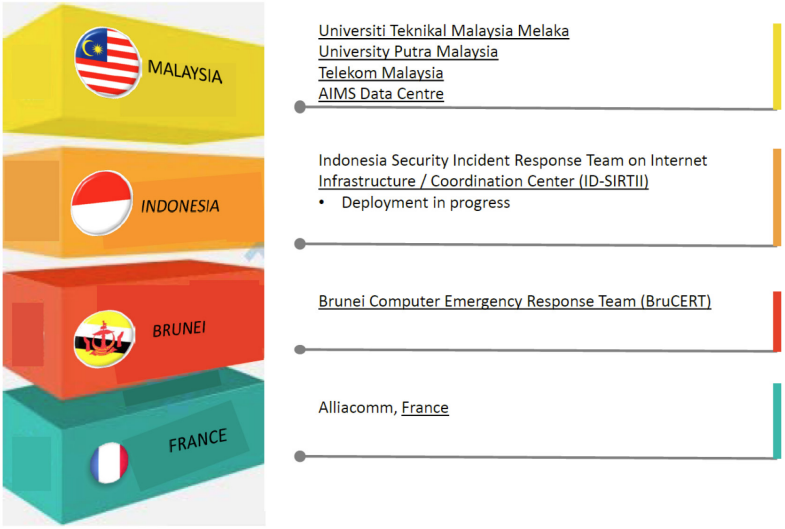


Figure 8 Participants for the Project

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.

© CyberSecurity Malaysia 2017 - All Rights Reserved

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

© CyberSecurity Malaysia 2017 - All Rights Reserved

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:

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

© CyberSecurity Malaysia 2017 - All Rights Reserved

Incident Trend Analysis for 2016

By | Syarifah Roziah Mohd Kassim & Kilausuria Abdullah

Introduction

This 2016 trend analysis provides an overview and analysis of the year in terms of incidents. The report is based on data obtained from MyCERT's incident reports. Data confidentiality is preserved throughout the report to ensure the public and organizations are well-protected. Emerging trends are identified and analysed in comparison with 2015. Some of the present analysis findings include:

- Whether the cyberattack trend is on the increase or decline
- Common modes or techniques used in cyberattacks
- Latest cyberattacks
- Social media continues to be an avenue for cyberattacks
- More attacks are becoming money-motivated

MyCERT currently operates the Cyber999 computer security incident handling and response help centre as well as the Cybersecurity Malaysia Malware Research Centre.

MyCERT works closely with law enforcement agencies, such as the Royal Malaysian Police, Securities Commission, and Bank Negara Malaysia. MyCERT also has close collaborations with Internet Service Providers (ISP), computer security incident response teams and various computer security initiatives worldwide.

MyCERT responds to nine categories of incidents:

a. Content-related
b. Cyber harassment
c. Denial-of-Service (DoS) attacks
d. Fraud
e. Intrusions
f. Intrusion attempts
g. Malware
h. Spam
i. Vulnerability reports

Incident reports were obtained through the following channels:

a. Hotline number
b. Email
c. Fax
d. SMS
e. Online report form
f. Mobile phone app – Cyber999 App
g. 24x7 on-call reporting
h. Walk-in

Total incidents for 2015 and 2016

Category	2015	2016
Content-Related	33	50
Cyber Harassment	442	529
DoS	38	66
Frauds	3257	3921
Intrusions	1714	2476
Intrusion Attempts	303	277
Malicious Codes	567	435
Spam	3539	545
Vulnerability Reports	22	35
Total	9915	8334

Incidents that Increased in 2016

Category	2015	2016	Percentage
Content-Related	33	50	51.52%
Cyber Harassment	442	529	19.68%
DoS	38	66	73.68%
Fraud	3257	3921	20.39%
Intrusions	1714	2476	44.46%
Vulnerability Reports	22	35	59.10%

© CyberSecurity Malaysia 2017 - All Rights Reserved

Incidents that Decreased in 2016

Category	2015	2016	Percentage
Intrusion Attempts	303	277	-8.6%
Malicious Codes	567	435	-23.3%
Spam	3539	545	-84.6%

Trend Analysis for 2016

Fraud

Fraud incidents continue to be one of the major threats in our constituency. As fraud incidents have increased to 20.39% in 2016 compared to 2015, Internet users are advised to be vigilant of fraud activities. Fraudsters are always up to date with new techniques and modus operandi to prey on potential victims. Common fraud activities reported are the Love Scam, Lottery Scam, Fraud Purchase, Phishing, and Impersonation.

A key finding regarding fraud activities is that fraudsters are targeting small-medium corporate companies more than individuals with scam activities to maximize impact and increase monetary gains. This move has actually contributed to the increasing number of commercial fraud incidents.

Type of Fraud	2016	2015
Love Scam	44	22
Purchase Fraud	110	155
Lottery Scam	35	78
Impersonation	79	60

Some of the fraud incidents we have handled that are worth highlighting for public awareness and precaution, should the public encounter such emails or websites, are:

- Impersonation of Portal Rasmi Jabatan Imigresen Malaysia (JIM)
- Phishing emails impersonating Ketua Akauntan Negara regarding unclaimed money.
- Loan frauds that use the name Koperasi 1Malaysia Berhad via WhatsApp.
- Phishing website of Kementerian Kewangan Malaysia

Web Defacement Intrusion

Intrusion incidents reported in 2016 increased by 44.46% compared to 2015. Such incidents reported to Cyber999 consist of account compromises and web defacements. Account compromises, including email, social media and server accounts, continued to be reported in 2016. Web defacement means that the web content hosted on a web server has been modified or altered illegally, but it may not indicate a full system compromise. The majority of web defacements reported to Cyber999 involved the private sector as well as other sectors, with the majority of web defacements reported related to the private sector.

Most web defacements reported mainly exploited known vulnerabilities, for instance in the Content Management System or CMS that runs on web servers such as Joomla or Word Press. To keep attackers away, System Administrators need to apply security patches, keep their servers/applications up to date with current patches and follow best practices for web application.

Based on the present findings, the most popular hack modes used by attackers to deface websites are SQL injection and the exploitation of known vulnerabilities in a server.

The hack modes used in web defacement activities in 2016 are as follows:

- Brute force attacks
- Cross-site scripting
- Known vulnerabilities (e.g. unpatched system)
- Other web application bugs
- SQL injection
- Web server intrusion

Based on observations over the past two years, most targeted domains are .com and .com.my corporate websites belonging to the private sector. Platforms like Apache and IIS web servers were targeted most, followed by nginx and LiteSpeed web servers.

Cyber Harassment and Content-Related Incidents

Content-related incidents increased in 2016 from 2015 by 51.52%. Most incidents were related to intellectual property and involved trademark infringement, such as from local/

© CyberSecurity Malaysia 2017 - All Rights Reserved

foreign service providers and home users.

Hoax emails were also observed, which contained some elements of false content. Examples of such emails are:

- False notifications of a National Power Electricity Interruption on 18 December 2016
- Hoax tsunami warning emails

Cyber harassment incidents increased in 2016 from 2015 by 19.68%. The trends observed are:

- Cyber bullying, such as creating fake profiles of victims, cyber-blackmailing victims with money, humiliation and making victims' personal photos go viral on the net.
- Posting personal profiles belonging to victims (naked/nude photos/videos) on websites without the victims' knowledge
- Cyber stalking, such as threatening, and sending unsolicited sexual photos and inappropriate texts.
- Religious incidents, such as websites posting defamatory and misleading information about Islam.

Distributed-Denial-of-Service (DDoS) attacks

DDoS incidents increased by 73.68% in 2016 compared to 2015. Some of the DDoS incidents observed are:

- DDoS amplification attacks
- Log triggers from several DDoS mitigation providers, as more companies are subscribing to DDoS mitigation services

The DYN cyberattack on October 21, 2016 that involved multiple distributed denial-of-service (DDoS) attacks targeting systems operated by Domain Name System (DNS) provider DYN contributed to the increase in DDoS incidents. Many source IPs or agents of this DDoS attack originated from Malaysian IP addresses.

Malicious Codes

Even though malicious code incidents were fewer in 2016 than in 2015, incidents related to botnets, bots, and malware hosting continued to be reported to Cyber999. Incidents related to ransomware also continued to be reported to Cyber999, with a total of 82 incident reports in 2016. Cyber 999 also received reports of Mirai botnet infection incidents originating from Malaysian IP addresses that took part in the DYN DDoS attack in October 2016.

Conclusion

Based on the incident trend for 2016, it can be concluded that techniques used in cyberattacks continue to grow in sophistication and method. The sophistication sometimes outgrows the defence mechanisms, which means that enterprises must improve their defence. Cyberattacks are also becoming sophisticated in their ability to evade detection by security appliances and law enforcement tracers. Social media is gaining popularity among Internet users, but not adhering to security requirements properly and lack of awareness of security can lead to various cyberattacks ranging from account compromise, identity theft and cyber blackmail. If not secured properly, social media, mobile computing and interconnected devices can become the perfect avenue for attackers to execute specially crafted, highly sophisticated and difficult to detect attacks.

© CyberSecurity Malaysia 2017 - All Rights Reserved

Cryptocurrencies 102 and the Dark side of the web

By | Engku Azlan Engku Habib & Ikmal Halim Jahaya

Initially, Bitcoin and most other cryptocurrencies were made with *bona fide* intention and as the main reason. However, criminals are very creative but on the wrong side of the law and will use whatever means to get the upper hand.

Over 1010 cryptocurrencies exist in the Internet ecosystem [1], as mentioned in a previous article (Cryptocurrencies 101). Of these, only 94 types of cryptocurrencies have a market capital exceeding USD 1M in value. Meanwhile, cryptocurrencies ranking 186 to 1010 have market capital below USD 100k. These are huge sums of wealth being created that attracting people to wish for some slices of the cake.

History in Malaysia

It appears that the current de-facto cryptocurrency (Bitcoin) was first accepted and discussed in Malaysia around 2012, and possibly even earlier. Bitcoin was first accepted and used globally by the public in 2009.

Bitcoinmalaysia.com, a leading, claimed to be the first website to promote and discuss Bitcoin in Malaysia, has been hosted since 24 August 2012[2]. Any offline or informal discussions could have begun earlier still.

As of 28 May 2017[3], Bank Negara Malaysia, the controlling body for finances in Malaysia, declared the following about Bitcoin (and other Cryptocurrencies):

> The Bitcoin is not recognised as legal tender in Malaysia. The Central Bank does not regulate the operations of Bitcoin. The public is therefore advised to be cautious of the risks associated with the usage of such digital currency.
>
> **Bank Negara Malaysia**
> **2 January 2014**

Whereas at the international level, cryptocurrencies are received with mixed reactions. Thailand was the first country to officially ban the usage of Bitcoin in the Kingdom [4]. China was the second country to ban Bitcoin [5].

In contrast, an international entrepot hub, Singapore views cryptocurrency from another perspective. It allowed the usage of Bitcoin in 2014[6] and has a nearly complete explanation of the definition of cryptocurrencies and the taxation of transactions using cryptocurrencies.

Meanwhile, Japan officially legalized the usage of Bitcoin as a legal method of payment on 1st April 2017[7]. Under this law, Bitcoin Exchange is under the anti-money laundering regulation, and at same time Bitcoin is categorized as a prepayment instrument.

To ensure that usage is controllable and to avoid uncertainties, Bitcoin Exchange is to strengthen their IT infrastructure (to avoid the Mt. Gox intrusion incident from recurring) and conduct operational stipulation. From the management side, the Exchange is needed to conduct employee training programs and to submit annual reports to legislators for audit purposes.

The unintended relation between cryptocurrencies and the Deep Web is discussed in the next subtopics as case studies. Under no circumstance is the usage of cryptocurrencies either promoted or prohibited.

What is the Deep Web?

The Dark web, a subset of the Deep Web, is a notorious meeting ground for hardcore criminals, from human traffickers to hired assassins. To cover their tracks, they will use any method that provides advantages against law enforcement agencies (LEA).

The Deep Web is much bigger than the Surface Web that already has more than 555 million registered domains. Websites (or subdomains) that are not catalogued fall into the Deep Web

© CyberSecurity Malaysia 2017 - All Rights Reserved

category. Some sites are purposely hidden, while others appear hidden because search engine crawlers cannot find/index and catalogue them. It is estimated that the Deep Web is an exorbitant 400-500 times bigger than the Surface Web. Data incompatibilities and technical problems can complicate indexing efforts. There are Web sites that require login passwords before users can access the content. Crawlers cannot penetrate data that requires keyword searches on a single specific Web site. There are also timed access sites that no longer allow public views after a certain time limit. These challenges and others thus make it much harder for search engines to find and index data.

The aforementioned technical descriptions of the Deep Web address both good and bad websites. For the sake of this article, only purposely built and hosted websites with *mala fide* intention are mentioned.

The characteristics for *mala fide* websites are generally as follows:

a. Can only be accessed on the TOR network

   Intended users need to use the TOR browser bundle to access content. A normal browser cannot work even if the user employs TOR software or is behind a proxy. This is because the dedicated TOR browser has a built-in 'interpreter' that is able to open Deep Web content.

b. Employ a different URL naming convention (do not end with .com, .net and others, but mostly end with .onion).

   (e.g. http://kpvz7ki2v5agw5.onion/wiki/index.php/Main_Page)

Contrary to popular belief, the Dark Web is not the Deep Web, but is only part of it. The Dark Web relies on darknets or networks where connections are made between trusted peers. Examples of Dark Web systems include TOR, Freenet, and the Invisible Internet Project (I2P) [8].

Most services or products on the Dark Web only accept Bitcoin as payment method. This is done to hide money trails, as Bitcoin (and other cryptocurrencies) is not regulated by the government or any central entity or agency.

Examples of illegal services or products advertised on the Dark Web that accept cryptocurrencies for payment are listed below. The URLs are not shared for security reasons; besides, URLs do not usually last long, as another means of evading identification.

i. Drug Trafficking

Figure 1: Peoples Drug Store sells heroin, cocaine, ecstasy, and more; gives Bitcoin a commission for promoting the website and being the payment method

ii. Gun trade

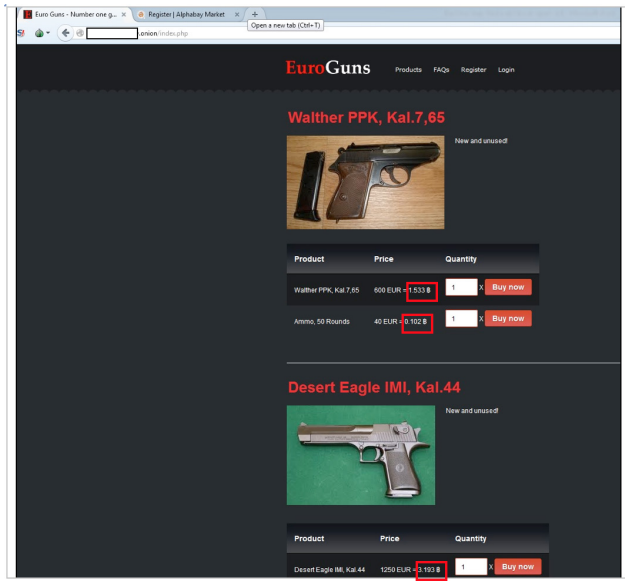


Figure 2: Handguns being sold on the Deep Web. Note the .onion URL and the price in Bitcoins in red.

© CyberSecurity Malaysia 2017 - All Rights Reserved

iii. Ransomware

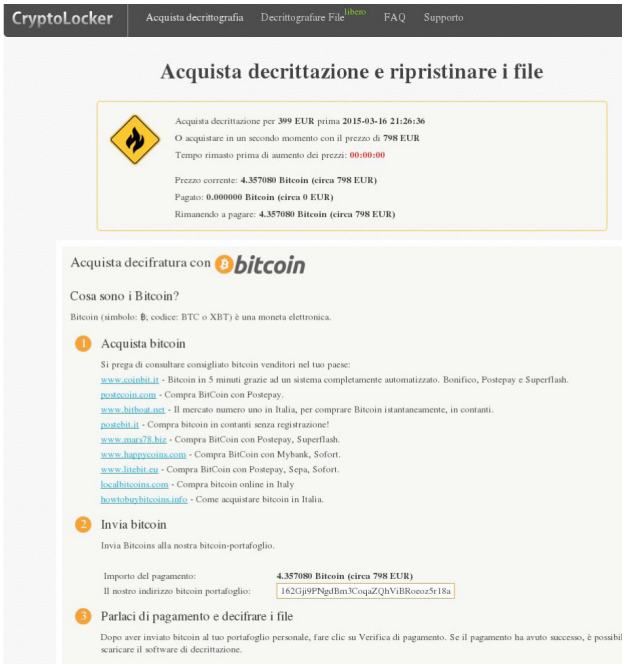


Figure 3: Ransomware demanding payment via Bitcoin in Italian language (auto detected based on the victim's profile – e.g. language used on the computer)

iv. Fake Documents (credit cards)

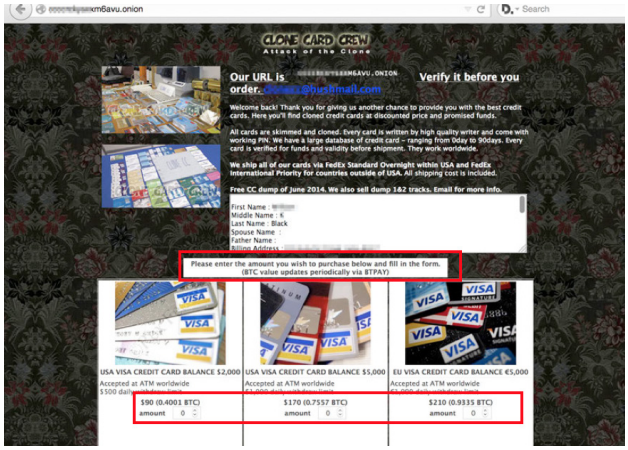


Figure 4: Fake credit cards with stolen details for sale on the Dark Web with Bitcoin as the payment method accepted

v. Fake Documents (US passport)

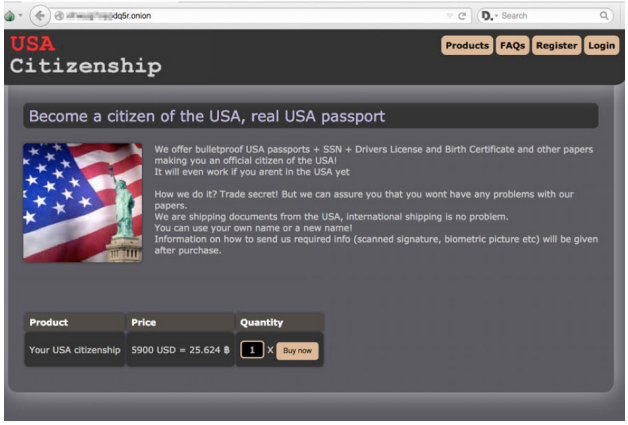


Figure 5: Fake USA passport up for sale for USD 5,900 @ BTC 25.624

vi. Money laundering.

Although Bitcoin is fairly anonymous, there exists aservice that is mostly used for money laundering to secure transactions by adding more anonymity. This is generally achieved by "mixing" the user's Bitcoins—transferring them through a spidery network of microtransactions before returning them to the user. In the process, the user will end up with the same amount of money (minus a small handling fee), but the transactions become substantially harder to track.

Ultimately, Bitcoin users will wish to extract money from the system and turn it into cash or other types of traditional payment means. Several anonymous services exist in the Deep Web for this purpose. These allow users to exchange Bitcoins for money via PayPal, Automated Clearing House (ACH), Western Union, or even send cash directly via mail.

For security reasons, the websites and methodology of this service are not discussed in detail in this article.

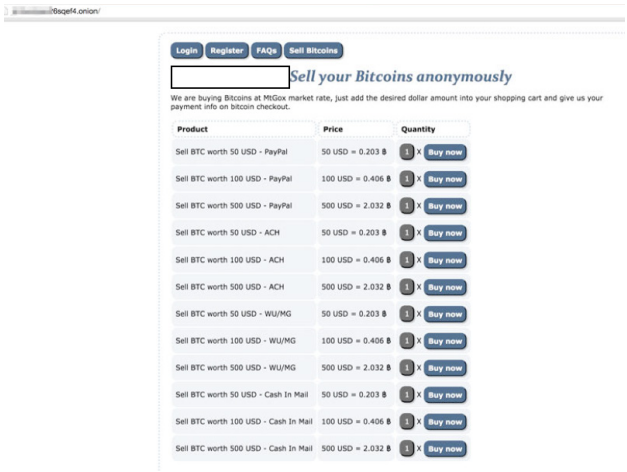


Figure 6: Service of exchanging cash or offering electronic Bitcoin payment

© CyberSecurity Malaysia 2017 - All Rights Reserved

vii. Online pharmacy for illegal/ prescription medicine on the Deep Web

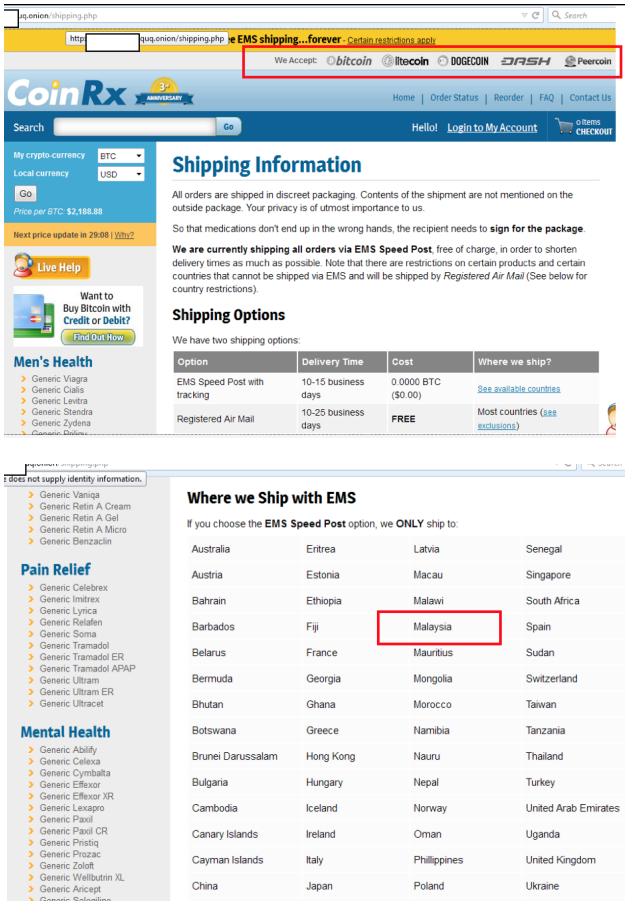


Figure 7: Online pharmacy that accepts Bitcoins and other popular cryptocurrencies as payment and delivers to Malaysia. Note the .onion URL.

viii. Hacker for hire

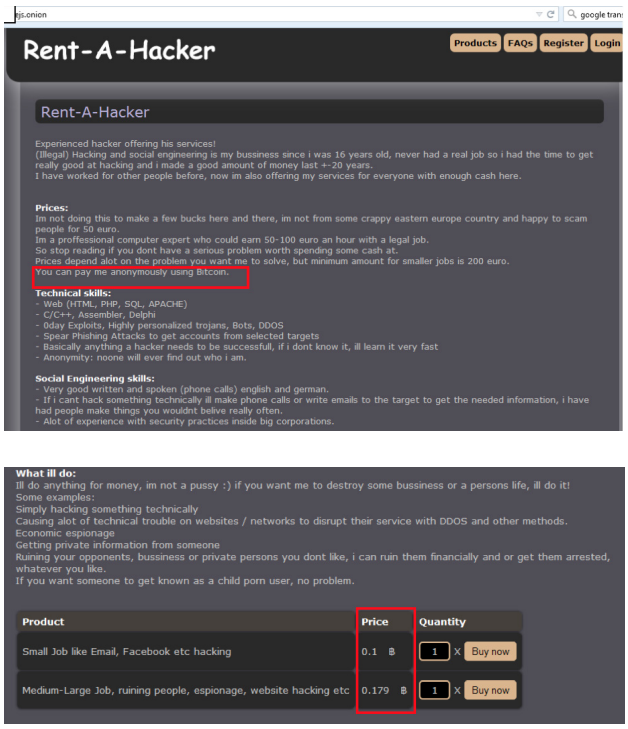


Figure 8: Hacker offering his services for Bitcoin prices

Based on research by scientists from Trend Micro, some statistics on products sold on the Deep Web were compiled [8].

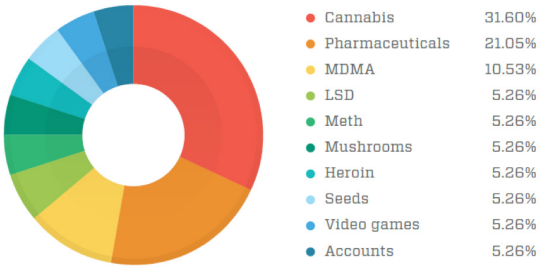


Figure 9: Vendor breakdown [8].

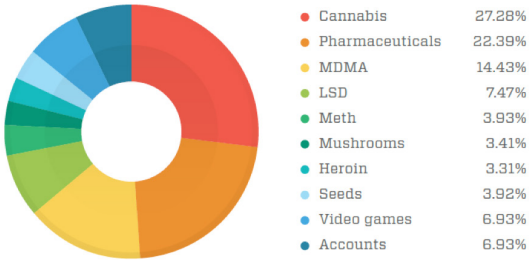


Figure 10: Buyer breakdown [8].

Apart from typical WWW (http or https) used for the Deep Web, other methods of communication or data distribution are also used.

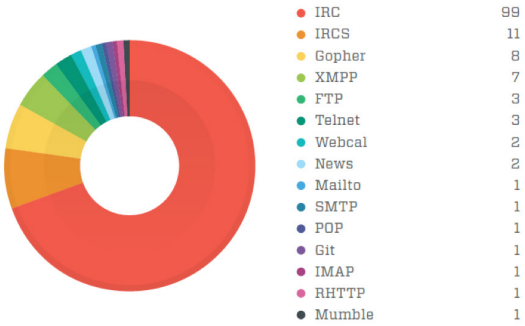


Figure 11: Protocols used on the Deep Web (excluding http/ https) [8]

Searching The Deep Web

Unlike for the Surface Web, the term 'googling' would be dreadfully incorrect. The Deep Web involves utilizing other methods and search engines to find interesting and controversial websites. The Deep Web has a search engine comparable to wiki with the same function as the Surface Web cousin but with focus only on searching and archiving materials in the Deep Web.

© CyberSecurity Malaysia 2017 - All Rights Reserved

For security reasons, the full URLs are not listed:

Search Engine	
DuckDuckGo	More focus on anonymous searches but not on Deep Web searches
Grams	Search engine with focus on the drug trade
Not Evil	Tor search engine that only indexes hidden services on Tor.
Torch	Tor search engine claimed to have indexed around 1.1 million pages.

Wiki

Wiki	
The Uncensored Hidden Wiki	Wiki sites on materials that are illegal on the Surface Web
Harry71's Onion Spider -	A hybrid of a search engine and Wiki. It is a spider robot for finding known .onion sites. It does not list onions that are down.

Figure 12: Torch search engine. Note the illegal services advertised on the website

Figure 13: The Uncensored Hidden Wiki main page

Figure 14: Harry71 Onion Spider website. A simple website that lists various Deep Web services.

Challenges To Law Enforcement

Since TOR was designed for whistle-blowers to use and for anonymity in the first place, its creation has become a huge stumbling block for LEA in determining who uses the Deep Web for criminal purposes. Besides hurdles with Surface Web investigation, officials investigating the Deep Web face the following challenges as well:

i. **Encryption:** Contents in the Deep or Dark Web are encrypted in case of Lawful Interception. This would deter normal investigation from being carried out and investigators need to be inside the Deep Web itself to obtain data almost manually and possibly act as other forum members and try to buy products or obtain services.

ii. **Categorization:** It is very difficult to categorize sites on the Deep Web, since all sites end with .onion domains and are not categorized as usual Surface Web sites (.com, .gov, .org). Any .onion site can host anything from grey-area crime (e.g. porn or free speech, which may be legal in certain countries and not in others) to definite crime (e.g. assassins, paedophiles).

iii. **High-pace activities:** The Deep Web is a very dynamic place. A site can be at a specific URL one day and offline in just a day or two. The URL of the same site on the Deep Web also changes frequently.

Any information obtained by investigators 10 days ago may no longer be relevant today and can thus seriously affect prosecution.

Prospect Of The Deep Web

Cryptocurrencies like Bitcoin coexist with the Deep Web and complement each other to achieve the maximum user anonymity possible. Bitcoin

© CyberSecurity Malaysia 2017 - All Rights Reserved

or other new currencies have new methods of obscuring transactions. The Federal Bureau of Investigation (FBI) forecasted that Bitcoin will only become more popular, as it will be used to fund illegal organizations, including hacker or terrorist group because money trails are very hard to trace [9].

With this highly lucrative and yet untapped illegal market, there are always prospective sellers entering the Deep Web to offer products and services. Hence, law enforcement will only have more cases to resolve.

A resolute and concise cyber law that can be implemented in all or most countries in the world is needed to combat crime, especially on the Deep Web. So far, criminals can move to countries that have no serious laws on cybercrime or the jurisdiction does not really understand the cyber situation since it is not the same as in the physical world.

Whilst convenient, cloud services can also be used by criminals hosting malware in reputable cloud service providers where the traffic is less likely to be blocked. An estimated 16% of malware and cyberattacks come from Amazon cloud services [10].

Conclusion

What was originally created as a tool for secret communication has evolved into a prominent underground domain: a display of human nature, improvisation and evolution. However, this domain is an obstacle for LEA and government investigators to identify lawbreakers, but it should not be so. To start, LEA and investigators may be taken aback by the Deep Web & Bitcoin aficionados, but with proper study and research they should be able to fully understand and be in a proper position to eradicate the nuisance caused by underground lawbreakers.
Moreover, proper laws and an understanding of current laws and judiciaries pertaining to the Deep Web ecosystem besides the normal Surface Web, are important to bring perpetrators to justice.

References

1. *http://coinmarketcap.com/all/views/all/*
2. *http://bitcoinmalaysia.com/page/24/*
3. *http://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement&ac=49&lang=en*
4. *http://www.cnbc.com/id/100923551*
5. *https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions*
6. *http://coinrepublic.com/singapore-tax-authorities-iras-recognize-bitcoin-and-gives-guidance/*
7. *http://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/*
8. *Trend Micro's Below the Surface: Exploring the Deep Web, Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler, June 2015.*
9. *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.*
10. *The Dark Web Revealed, Marc Goodman, Popular Science, April 2015*

© CyberSecurity Malaysia 2017 - All Rights Reserved

Social Networking Security and Privacy

By | Nor Zarina binti Zamri

Abstract - Social networking sites have become very popular for communication and information sharing. As people are moving more towards social networking, personal security, privacy and data are at higher risk. This article examines risks and security measures to be adopted for more secure use of social networking.

Keywords— Security, Privacy, Facebook, Twitter, Website.

Introduction

Social networking has become very important, if not compulsory in daily life. By definition, the term 'social networking' comes from 'social network,' which represents relationships and flows between people, groups, organizations, computers or other information/knowledge processing entities. In general, social networking sites are platforms that provide virtual communities for people with the same interests or to simply socialize [1].

The history of existing social networking is illustrated below.

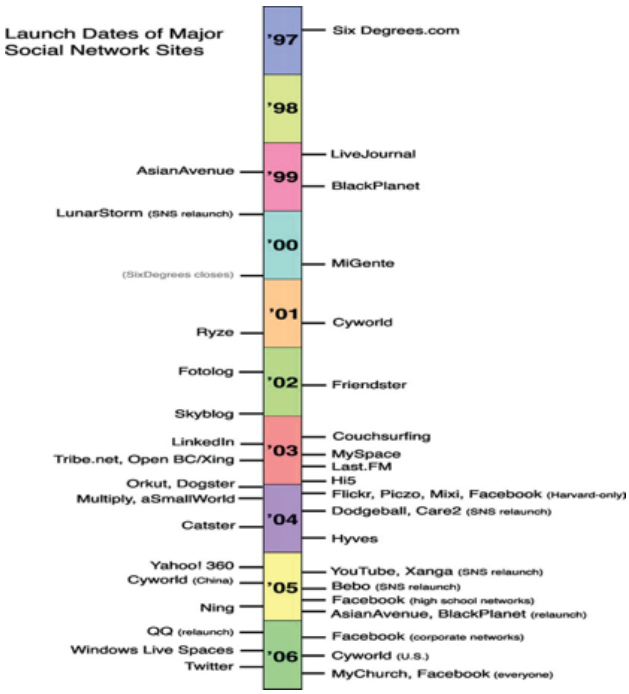


Figure 1 Timeline of the launch dates of many major SNSs and dates when community sites were re-launched with SNS features [2]

As the importance and need for social networking websites rise, the risks involved in protecting and securing personal data and communication devices/systems also increase. This article mainly concentrates on various possible risks, and their impact and security mechanisms necessary for protecting ourselves and the devices involved in communication.

Some of the most widely accessed social networking websites will be emphasized (e.g. Facebook, Twitter) along with the security and privacy concerns involved, as well as security measures to follow/adopt to protect our personal data and communication devices.

Security And Privacy In Social Networking

Failure to observe and ignoring security and privacy in social networks results in a number of problems, as discussed below [3].

Social applications offer easy access to attackers.

Almost all social applications require access to private user data [3]. Attackers have started inventing applications to deceive users for attackers' own benefit. Users do not realize they are exposed to attacks while adding friends to their lists without filtering friends' profiles. This can lead to Trojans on phishing pages. A spambot can be added silently to the vulnerable user's account, which will send the user informal messages followed by links.

Welfare hoaxes

It is well-known that social networking sites are typical platforms for users to communicate and interact with each other. It is proven that social networking sites are a good medium for intermediaries to collect charity for disaster victims, such as earthquakes and floods, but not all people have pure intentions to help. Many fake pages and groups are created by scammers intending to take advantage of disasters. Such irresponsible scammers will collect user credit card information by sending links for users to make donations to disaster victims, but sadly,

© CyberSecurity Malaysia 2017 - All Rights Reserved

all the money donated by the user will be credited to the scammer's bank account. This type of scam is frequent these days, and it is also happening regularly on social networking sites.

Phishing attacks on user credentials

Phishing is a form of stealing user account data, such as usernames and passwords, by presenting users with a fake login page. In this case, after a user has logged in to the fake page, the information will be sent to the attacker, who may use the victim's account wrongly. There are many effects of phishing, identity theft and stealing personal user information that prevent users from accessing their own accounts and allow power abuse at the corporate level, for example changing the system flow like bypassing the budget approval process. There are new and dangerous phishing threats that lead users to install unused plug-ins containing malware that will infect users' computers. Moreover, this malware will spread to other machines that are connected to the affected computer. Pharming is a very dangerous form of phishing. Such attack will modify the domain name resolution system and redirect users to false web pages. Attackers will wait for the user to visit the target site rather than produce links, thus making the attack more effective. Nonetheless, there are various ways to evade phishing attacks. For example, be careful with all email received by checking the sender's email domain name and check if the visited page is trusted before filling in any personal data. It is advisable not to open suspicious links, and if required, forward the email to the network administrator for further action.

Malware

Over the last five years, an abundance of spam has been dispersed through social networking sites. In an easy but effective way, attackers use phished social accounts to post inappropriate messages that will link the users to malware. All such messages get posted on the victim's friends' profiles or accounts. This technique is used to create confidence in the user to click, rather than posting by spambots. This threat is known as "Koobface," which is one of the most popular malware that uses Facebook as a platform for spreading. Figure 2 presents the lifecycle of Koobface, which starts when the user's account begins sending the malware link to friends, who directly open it without authenticating it first. As the link is opened, it will lead the victim to a similar looking page like a You Tube video and request them to download some plug-in in order to watch the video. Once the user downloads the plug-in, the malware will affect them as it is being transferred from other infected machines. This newly infected machine will act as a host to store a copy of the malware.

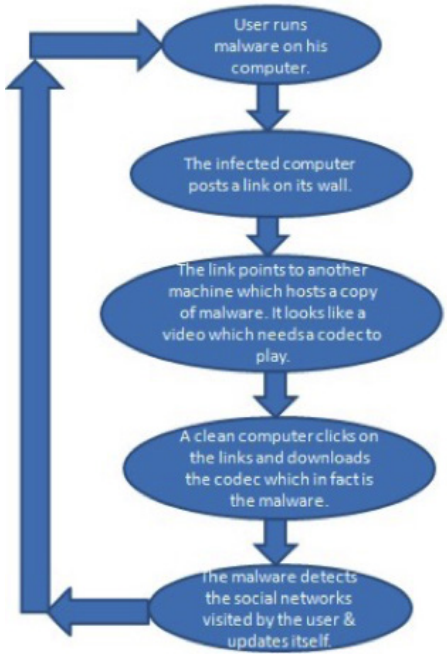


Figure 2. Lifecycle of Koobface (a kind of malware) [3]

Social Networking Website: Facebook

Facebook was developed by Mark Zuckerberg and friends in 2003. Facebook is the most widely used social networking website that is accessed globally. Facebook offers various languages on the interface [4]. According to research, Facebook ranks as the second most widely accessed website after Google. This shows how addicted and dependent people are on this social networking website. It is a domain space where data is shared/exchanged/accessed by various people. Potential attackers concentrate on this website to obtain people's personal data and any other information required for attacks. Additionally, Facebook has numerous applications and games that users are able to access. These applications are also a potential risk factor for malware infection.

Even though Facebook provides Privacy and Security settings through which it is possible to protect and secure our accounts and information, most of us do not even bother with using these. A basic security recommendation is to apply all possible security to applications, block access to all areas and then provide access only to the required areas of application.

© CyberSecurity Malaysia 2017 - All Rights Reserved

Similarly, Facebook needs to block access to all possible application areas and allow users decide on what to access [5].

Security and Privacy concerns

- User Profile: Users normally provide actual and correct data on their Facebook profiles. This is not actually required, unless it is sure that we will provide access to our profile to reliable friends. All others should not have access to our profile.
- Adding Friends/Groups: Users need to be very careful when adding friends or groups. Only reliable and known friends/groups should be added or given profile access.
- Shared Data: Data we are sharing represents personal areas of interest and indirectly helps assessments of our personal life. We need to be careful with sharing data by only sharing with related or reliable friends and not everyone on Facebook.
- Privacy/Security Settings: It is necessary to change the privacy settings to secure our profile and other actions. Facebook provides these settings to make accounts and access more secure and it is recommended to use these settings. These settings allow deciding who can contact us and who can have access to our profile.
- Login Notifications: Enable login notifications in the Facebook security settings, so that notifications will be sent to your email or mobile. This way, it is possible to trace and take immediate action if unauthorized users try to access our account.

Facebook is the most accessed and popular social networking website. This does not mean it is the most secure application. Facebook provides many security and privacy features that facilitate better security of our accounts and access levels. It all depends on the individual whether to follow these security and privacy features to make life peaceful and happy or to accept the risks and face the consequences.

Social Networking Website: Twitter

Twitter is the most widely utilized professional-social networking website. Twitter is used to send and read short messages known as tweets. Only registered users can send messages and unregistered users can read messages. Twitter shares public user information with other registered account holders for personal identification.

Twitter is the most widely employed professional connectivity social network and also the mostly frequently attacked social networking website. One way to become stable and more secure to avoid attacks like phishing is to use the security and privacy settings [1].

Security and Privacy concerns

- User Information: Do not share personal or critical information while tweeting. All tweets are public and there is an option to secure your tweets so only selected people who are following you can view your tweets. Even then, sharing critical information, such as personal data, bank information and identification numbers is not recommended for security purposes.
- Following: Following on Twitter has a critical role in protecting user security and privacy. Unless you know a person well, do not follow them or their tweets. The best way to facilitate attacks is to follow users and get relevant information through their tweets. Do not follow anybody unless you know them well, and even then, do not share critical personal information.
- Location Update: The Geo Tagging feature in Twitter allows other users to know your current location. This is not always safe. Unless it is really required, do not enable this service, because there is no need for people to know your current location. Location may alert attackers and burglars who are waiting for the correct time to attack you or your property.
- Blocking: If you feel that some users in your following list are not trusted, block them immediately. By doing so, they will not know anything regarding your actions and location.
- Monitor your Kids: Kids are not mature enough to use social networking websites, which may have serious mental impact or may even result in physical attacks on kids. An example of mental impact on children is triggered feelings of envy when they see other peoples' tweets, and this can also lead to depression. Physical attacks, such as kidnapping and sexual abuse can easily happen to kids when attackers can predict the child's location or personal information like school and home location. If required,

© CyberSecurity Malaysia 2017 - All Rights Reserved

at least take into account some of the things mentioned below for their safety.

- Remove your kids' personal information from Twitter. Children are not mature enough to use this website. Ensure the child's personal information is not available.
- Turn off the tweeter location option. It will help kids be safe by not giving attackers the chance to find the child's location easily for physical attacks. It can also prevent mental disturbances when people retweet the child's status and make negative comments about the tweet.
- Frequently check your child's account for unnecessary postings.

- Login Information: Always choose complex passwords for your Twitter account to make it harder for attackers to crack and misuse your account.

Even though Twitter is more secure compared to other social networking websites, it all depends on how we share information.

Conclusion

Social networking sites have become potential targets for attackers due to the availability of sensitive information as well as the large user base. Therefore, privacy and security concerns with online social networks are increasing. Privacy is one of the main concerns, since many social network users are not careful about what they expose on their social network space. The second problem is identity theft, whereby attackers make use of social network accounts to steal victims' identities. Third is the spam problem. Attackers use social networks to increase spam through the click rate, which is more effective than the traditional email spam. The forth concern is with malware. Attackers use social networks as a channel to spread malware, since it can spread very fast due to the high connectivity among users. Social networking sites are always facing new types of malware. Lastly, physical threats were addressed, which are the most harmful. Such threats are enabled by social network features like location-based services that make it easier for criminals to track and approach victims.

Social networking sites attempt to implement various security mechanisms to prevent such matters and to protect their users. But attackers will always find new methods to break through these defences. Therefore, social network users should be aware of all potential threats and be more careful when using social networking.

References

1. *E. Aïmeur, S. Gambs, and A. Ho, "Towards a Privacy-Enhanced Social Networking Site," 2010 Int. Conf. Availability, Reliab. Secur., no. 3, pp. 172–179, Feb. 2010.*

2. *D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," J. Comput. Commun., vol. 13, no. 1, pp. 210–230, Oct. 2007.*

3. *G. Bamnote, G. Patil, and a Shejole, "Social networking - Another breach in the wall," Int. Conf. Methods Model. Sci. Technol., vol. 1324, pp. 151–153, 2010.*

4. *L. Bilge, T. Strufe, D. Balzarotti, E. Kirda, and S. Antipolis, "All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks," Www 2009, pp. 551–560, 2009.*

5. *A. Albesher, "Privacy and Security Issues in Social Networks : An Evaluation of Facebook," pp. 7–10, 2013.*

6. *C. Perez, B. Birregah, R. Layton, M. Lemercier, and P. Watters, "REPLOT : REtrieving Profile Links On Twitter for suspicious networks detection," pp. 1307–1314, 2013.*

© CyberSecurity Malaysia 2017 - All Rights Reserved

Blockchain Implementation (Proof-of-Concept)

By | Abdul Alif bin Zakaria

Introduction

What is blockchain? A blockchain is a public ledger of all Bitcoin transactions ever executed. It is constantly growing as 'completed' blocks with new sets of recordings are added to the blockchain in linear, chronological order. Each node (computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the Bitcoin network. The blockchain has complete information about the addresses and balances right from the genesis block to the most recently completed block.

Blockchain establishes a system of distributed consensus in the digital online world that combines existing technology, such as the database system, P2P network, and cryptography, as shown in Figure 1. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It paves the way for developing a democratic, open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun.

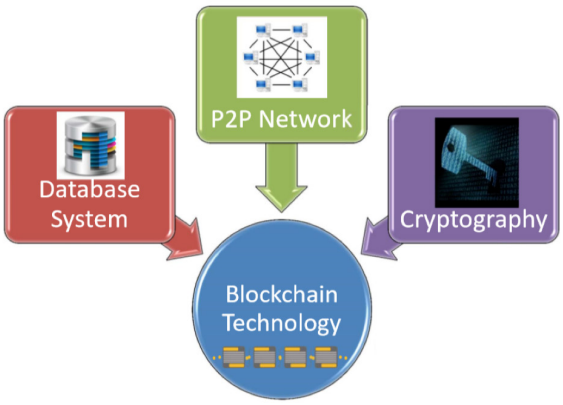


Figure 1: Blockchain Technology

This article presents the possible implementation of blockchain technology in coming years and how the blockchain system can be applied in various areas. It is evident that the future and opportunities of blockchain are growing, as this fundamental technology is all set to revolutionize our digital world.

Asset Tagging

LuxTag [1] is the first ever digitized certificate of authenticity for products (or machines, vehicles, etc.) on a blockchain. It is updatable and can have messages attached, whose conjoint ownership can be flexibly transferred. It re-invents certificates of authenticity using NEM blockchain technology. In LuxTag, the certificates are fully-fledged accounts in the blockchain. These digital token accounts are used to track the status of an item throughout its life and to further provide companies with post-sale big data, to which they currently have no access. The Blockchain records these events and appends them to a notarization account, which represents the tokenized luxury item. Blockchain implementation in this system stops product counterfeiting, as only genuine products are recognized because the origin of the products is recorded and verified in prior.

Land Registry

Landstead [2] uses NEM [3] blockchain technology to offer a registry of land and properties, allowing governments and citizens to co-create open blockchain systems that can be trusted and consulted by interested parties. Built in a secure blockchain environment, the Landstead platform puts security first with NEM at its core. Users can review any transaction and registration in the NEM blockchain, providing transparency and veracity. Governments are the axis of the platform, managing user privileges as well as land and property data. Through notaries and government servants, they manage veracity via the blockchain.

Recruitment Industry

ChronoBank.io [4] is an ambitious and wide-ranging blockchain project, aimed at disrupting

© CyberSecurity Malaysia 2017 - All Rights Reserved

the HR, recruitment, and finance industries similar to how Uber disrupted the taxi business. The goal is to make a difference in the way people find work and are rewarded for their labour – doing so within a decentralized framework and without the involvement of traditional financial institutions. Another goal is to create a revolution in short-term recruitment within key professions. This alternative is a new generation of time-based currencies utilizing the latest developments in blockchain technology.

Diamond Certification

Everledger [5] is a fraud detection system that overlays big data from closed sources like insurers and law enforcement. It is a permanent ledger for diamond certification and related transaction history, verification for insurance companies, owners, claimants and law enforcement. Everledger is built on both public and private blockchains to achieve a hybrid model. It enables tracking any asset that carries a Unique Identifier, which is difficult to destroy or replicate. Custom client solutions are built on IBM's cloud-based blockchain solution, which is underpinned by LinuxONE [6] to ensure the highest level of security for clients' assets.

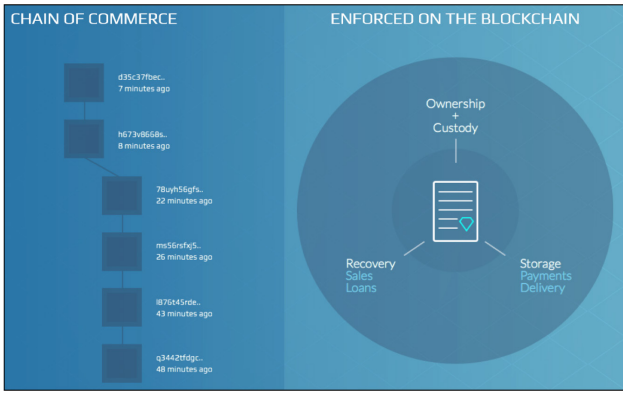


Figure 2: Smart Contract for Diamond Certification and Transaction

Gold Trading

DinarDirham [7] is a decentralized gold trading platform combining the stability of gold price with the technological security of the blockchain network. By employing blockchain technology and robust trading platforms, DinarDirham allows quick and transparent access to the bullion markets for small investors. The smart contracts and transactions issued to users via the blockchain are transparent. All assets issued in DinarDirham are bridged completely transparently to the liquidity provider using the blockchain infrastructure to ensure decentralization. The DinarDirham Wallet also uses the latest technology in web security to keep assets safe and secure.

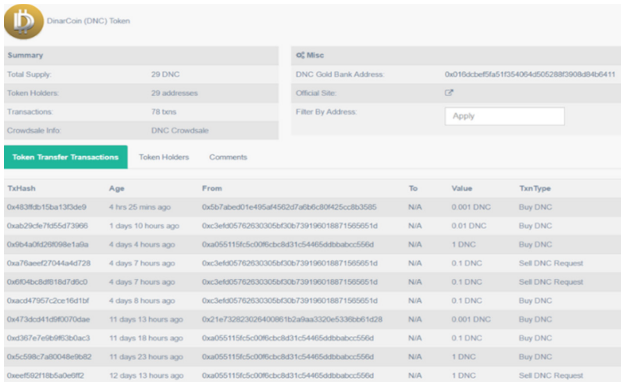


Figure 3: Decentralized Gold Trading Platform

Digital Passport

ShoCard [8] is a digital identity for protecting consumer privacy and is as easy to use as showing a driver's license. It is optimized for mobile use and is so secure that even banks can rely on it. Blockchain start-up ShoCard has developed a proof-of-concept focused on digital identity in partnership with a major IT firm that works with the airline industry. Focus was on creating an innovative, mobile identity management solution using BlockCypher's blockchain infrastructure.

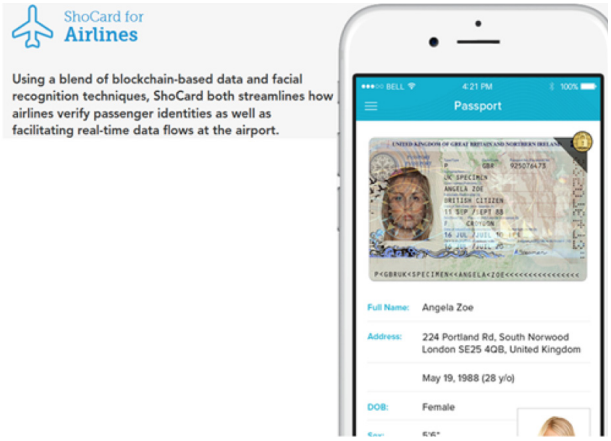


Figure 4: Identity for a Mobile World

Product Verification

Blockverify [9] is a transparent supply chain that employs blockchain technology to improve anti-counterfeit measures in different industries

© CyberSecurity Malaysia 2017 - All Rights Reserved

and has a significant, positive social impact. Blockverify facilitates verifying a product that is already in possession but seems to be counterfeit. The system can identify if a product was diverted from its original destination. It can also easily trace and locate stolen merchandise. Blockverify can track fraudulent transactions of any type throughout the system.

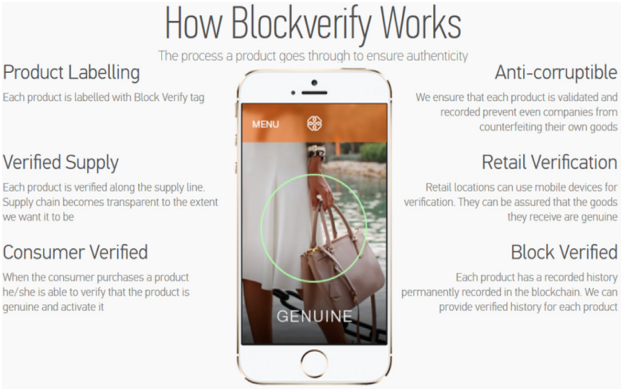


Figure 5: Blockchain-Based Anti-Counterfeit Solution

Healthcare

Blockchain technology addresses the trade-off between personalized care and operational costs by connecting the ecosystem to universal infrastructure. Shared infrastructure allows creating global standards without compromising privacy and security. Gem [10] partnered with industry leaders to identify problems they want to solve with their network, after which a federated blockchain was spun out to support the pilot running on GemOS. Access to resources is regulated by permission control across multiple organizations, to which patients, providers, hospitals, devices, and other identity types can refer regarding blockchain applications.

Figure 6: Bringing the Blockchain to Healthcare

Voting System

VoteWatcher [11] aims to offer complete transparency to the modern electoral system and empower every voice by providing a reliable and secure voting mechanism. Detailed election records are posted online and on the blockchain, and every step in the process is highly auditable. Custom generated ballots contain unique (non-identifying) tokens in the form of QR codes to prevent the same ballot from being scanned twice. The tokens also serve to unlock a "vote unit" once scanned by the voting machine, which is transferred to the choice candidate on a blockchain. This way, votes are recorded and tallied in real time. In the event of a recount, the blockchain data can be used to expose tampering with the ballots themselves and vice-versa.

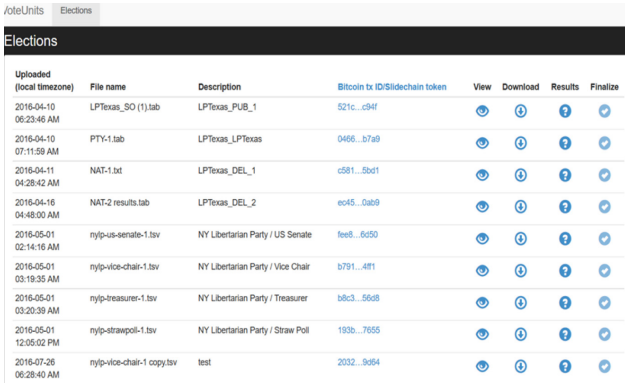


Figure 7: Innovative Blockchain Voting System

Music Royalty

MUSE [12] is a ledger for keeping track of Smart Contracts and three different types of cryptographic tokens: Core Units, Smartcoins and User-Created Tokens. It also serves as an On-Blockchain Exchange, allowing users to trade all three types of crypto-tokens without needing to exit the ecosystem and trusting a third party to hold their funds. MUSE's open, transparent and permanent nature makes it possible for anybody (artists, labels, publishers, royalty collecting organizations, etc.) to plug in for free and start building on top of this stable and solid infrastructure. Artists or entrepreneurs can plug into MUSE and benefit immediately from it all while offloading the costs of maintaining their databases to the Blockchain.

© CyberSecurity Malaysia 2017 - All Rights Reserved

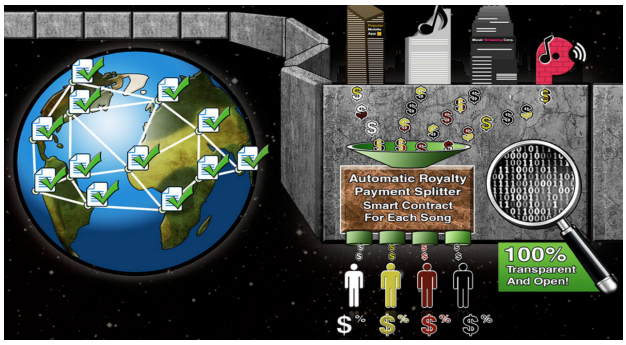


Figure 8: A Blockchain Specifically Tailored for the Music Industry

IP Protection

Blockai [13] is a copyright platform that helps artists claim their copyrights and protects them for free in four steps. Firstly, create a piece of digital art, photo or anything that can be copyrighted. Then register your copyright on the blockchain, a public ledger powered by Bitcoin. The record is permanent and immutable. Next, receive a registration certificate with cryptographic evidence that protects your copyright. You own the certificate forever. Finally, share your creation with peace of mind. You have proof of publication that protects your copyright and copyright monitoring that alerts you when people are using your work.

Conclusion

2017 is a pivotal year for blockchain technology. Many of the start-ups in the space will either begin generating revenue by providing products that the market demands, or they will vaporize by running out of cash. This should be the year when product implementation utilizing blockchain technology will grow. This is a crucial step in the larger adoption of blockchain technology, as it will allow sceptics to see the functionality rather than just hear of its promise.

References

1. LuxTag: Maintain Tokenized Assets on the Blockchain. Retrieved from http://luxtag.io/

2. Home - Landstead - Atraura Blockchain. Retrieved from http://landstead.atraurablockchain.com/#!/

3. NEM - Distributed Ledger Technology (Blockchain). Retrieved from https://www.nem.io/index.html

4. Chronobank.io. Retrieved from https://chronobank.io/

5. Everledger A Digital Global Ledger. Retrieved from https://www.everledger.io/

6. IBM LinuxONE. Retrieved from http://www-03.ibm.com/systems/linuxone/

7. DinarDirham.com - Innovation Creates Future. Retrieved from https://www.dinardirham.com/#

8. ShoCard Identity for a Mobile World. Retrieved from https://shocard.com/

9. Block Verify. Retrieved from http://www.blockverify.io/

10. Introducing GemOS, your blockchain operating system. Retrieved from https://gem.co/

11. VoteWatcher - The World's Most Transparent Voting Machine. Retrieved from http://votewatcher.com/

12. Muse Blockchain. Retrieved from http://museblockchain.com/

13. Binded: Copyright made simple. Retrieved from https://blockai.com/

© CyberSecurity Malaysia 2017 - All Rights Reserved

Email Security Threats and Trends

By | Kilausuria binti Abdullah & Sarah binti Abdul Rauf

Introduction

Email is an extremely popular method of communication. The ease of use and speed of communication via email make it attractive for business and personal use. Based on Wikipedia, email, or electronic mail, refers to a method of exchanging digital messages between people using digital devices such as computers and mobile phones.

In general, Internet email messages consist of two major sections, which are the message header and the message body. The email header is structured into fields such as From, To, CC, Subject, Date, and other information about the email. Simple Mail Transfer Protocol (SMTP) is a protocol used in the process of transporting email messages between systems by using message header fields.

Email Security

The popularity of email has made it a target of abuse by some people for their own benefit. Examples of email abuse are spam and phishing emails. When using email, users need to be aware there are threats involved. To avoid being scammed, users are advised to always apply best practices when using email and to become knowledgeable of newer issues with email.

Email Incident Statistics

Based from Cyber999 incident records, 657 incidents were reported regarding account compromise intrusions from 2012 to 2017(Q1). Below are the statistics on account compromise incidents reported for 2012-2017(Q1)

Year	Total Incidents by Year
2012	50
2013	153
2014	139
2015	119
2016	149
2017(Q1)	47

Table 1: Account compromise intrusions from 2012 to 2017(Q1)

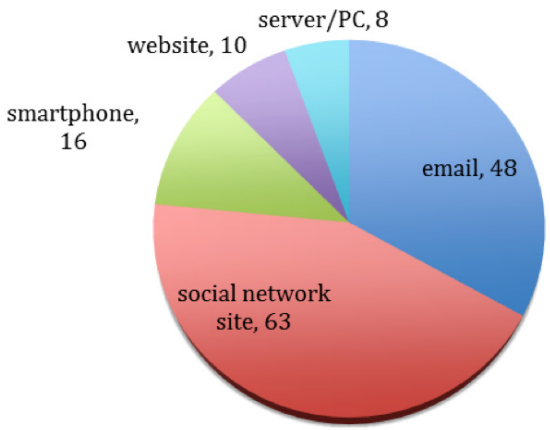


Figure 1: Account compromise intrusions in 2016 based on media used

Email Incident Trends

1. Spam Messages

Spam email is the most common threat involving email. One of the spam messages trends is email-marketing campaigns. Email marketing campaigns are used because they deliver outstanding results for businesses. Spam email can also be used as a distribution mechanism for malware.

2. Email Phishing and Spear Phishing

Besides phishing emails that target banks, phishers have also created phishing emails and websites for other famous applications, organizations and email providers, such as PayPal, iTunes, Gmail, etc.

© CyberSecurity Malaysia 2017 - All Rights Reserved

3. Scam Emails by Social Engineering

Hackers use victims' compromised email accounts to send scam emails to friends on the list of the compromised accounts. Scam emails can contain requests for help and money, claiming someone is supposedly in trouble.

From: [redacted]@gmail.com>
Date: [redacted]
Subject: URGENT ASSISTANCE!!!
To:

I really hope you get this fast. I could not inform anyone about our trip, because it was impromptu. we had to be in Johannesburg, South Africa for a program. The program was successful, but our journey has turned sour. we misplaced our wallet and cell phone on our way back to the hotel we lodge in after we went for sight seeing. The wallet contained all the valuables we had. Now, our passport is in custody of the hotel management pending when we make payment.

I am sorry if i am inconveniencing you, but i have only very few people to run to now. i will be indeed very grateful if i can get a loan of $2,850 from you. this will enable me sort our hotel bills and get my sorry self back home. I will really appreciate whatever you can afford in assisting me with. I promise to refund it in full as soon as I return. let me know if you can be of any assistance. Please, let me know soonest. Thanks so much..

Figure 2: Example of scam email

4. Spreading Malware

Another trend that is gaining momentum is email containing malware. The malware can spread via emails that contain links to infected sites or attachments that are infected with malware. When the user clicks on the link or opens the email attachment, the user's machine will be infected with malware. Some ransomware employs this method to spread. Ransomware is a type of malware that can lock users' computers or encrypt user files until ransom is paid.

5. Business Email Compromise (BEC)

Another common trend is Business Email Compromise (BEC). A variation of this is known as CEO fraud. In CEO fraud, cybercriminals might use hacked CEO emails to send impersonation emails to the finance manager or an employee in the finance department. This compromised email account is then used to trick the employee to transfer funds to an account controlled by the scammers.

Commercial Fraud is another BEC scheme that uses compromised email accounts to manipulate customers or suppliers to send funds to a fraudulent account. The most common method applied by cybercriminals to commit BEC fraud is email spoofing by social engineering (similar email address and similar domain).

I need your help, pls urgently wire USD [redacted] to another of my supplier in Indonesia today.
He needs the money as to send my containers papers so my goods can be cleared from port before Friday.
I am currently not disposed to make transaction because am out of my station.
I will send USD [redacted] to you next week as soon as am back before you finish production of my order.
please pay through bank with their account information below for immediate receiver via this info

Account Name: [redacted]

Account No.: [redacted]

Bank Name: [redacted]

Figure 3: Sample of commercial fraud email

6. Data Leakage and Business Disruption

Disgruntled ex-employees who previously managed the company email account may intentionally change the admin email username and password. The organization cannot directly reset the email account because that ex-employee who is the only one that knows the email server settings previously created it.

This type of threat can be minimized if the company has proper policies on staff termination and security procedures for handling company email.

Email Security Threat Mitigation

End-user email security best practices

- Never open attachments or click on links in email messages from unknown senders.
- Change passwords periodically and use best practices for creating strong passwords.
- Never share passwords with anyone, including co-workers.
- Try to send as little sensitive information as possible via email, and only send sensitive information to recipients who require it.
- Use spam filters and anti-virus software.
- When working remotely or on a personal device, use VPN software to access corporate email.
- Avoid accessing company email via public Wi-Fi connections.

By educating employees on email security and implementing proper measures to protect email, enterprises can mitigate many of the risks that come with email usage and prevent sensitive data loss or malware infections via email.

Enterprise Email Security Best Practices

There are multiple ways to secure email accounts. For enterprises, it is a two-pronged approach, encompassing employee education and comprehensive security protocols. Best practices for email security include:

- Engage employees in ongoing security education around email security risks and how to avoid falling victim to phishing attacks over email.

© CyberSecurity Malaysia 2017 - All Rights Reserved

- Require employees to use strong passwords and mandate password changes periodically.
- Utilise email encryption to protect both email content and attachments.
- Implement security best practices for BYOD if your company allows employees to access corporate email on personal devices.
- Ensure that webmail applications are able to secure logins and use encryption.
- Implement scanners and other tools to scan messages and block emails containing malware or other malicious files before they reach your end users.
- Implement a data protection solution to identify sensitive data and prevent it from being lost via email.

Implementing defensive technology is important, but defending against attacks requires ongoing user awareness, training and proactively. For example, finance staff needs to be proactive when dealing with payments. They need to check email addresses carefully and if the request is suspicious, they should check via phone call with the person or institution that supposedly sent the email.

Another proactive measure is to use email encryption. Email encryption keeps messages and attachments illegible to unauthorized users. Be sure to deploy a solution that is not only secure but also easy to use. The easier the email encryption is for senders and recipients, the more likely it is to keep email secure.

In order to combat ransomware that spreads via email, employers need to educate employees on ransomware threats and the potential security risks affiliated with suspicious links and attachments. Employees must not click on unfamiliar links, especially shortened links, like bit.ly or owl.ly. Frequent and complete back-ups are also an important safeguard.

Conclusion

The best way to prevent private data from falling into the wrong hands is to take proactive action. Encryption is the best bet, keeping data safe even if your account is hacked or if your password simply falls into the wrong hands.

If the company refuses or has constraints with using encryption, some email protection can help against advanced email threats. It can protect against ransomware, business email compromise, spoofing, and phishing. Despite the best tools available to protect your company and you, users need to have basic knowledge about email security and understand the best email practices.

References

1. *https://en.wikipedia.org/wiki/Email*
2. *http://write.flossmanuals.net/basic-internet-security/introduction-to-e-mail-safety/*
3. *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/infosec-guide-email-threats*
4. *http://www.focus.net.nz/blog/category/general/email-security-best-practices*
5. *https://www.cambridgenetwork.co.uk/news/huge-rise-in-cyber-attacks-as-criminals-start-to-target-smal3964/?*
6. *https://www.zixcorp.com/resources/blog/january-2017/email-security-threats-to-watch-in-2017*
7. *http://library.ahima.org/doc?oid=99319#.WQA6RR0lFn4*

© CyberSecurity Malaysia 2017 - All Rights Reserved

Cyberbalkanization/Splinternet

By | Mohd Rizal bin Abu Bakar

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." - John Perry Barlow, Declaration of the Independence of Cyberspace (February 8th,1996)[1]

John Perry Barlow's above declaration calling for the continued independence of cyberspace was made over 20 years ago. He disapproved of the US government's proposal of the Communications Decency Act crafted to protect society, especially children, from sexually graphic material transmitted through the Internet. However, Barlow's declaration was not only intended specifically for the proposed legislation. He saw it as a gateway tool for governments to control what Internet users can see or do, thus violating human rights to the access to information and free speech.

Fast forward to today, in the post-Snowden era, the declaration has often been used as a call to arms by governments of the world instead; to use the Internet as a 'shield' from the outside world; and to protect the nation(s) from foreign influences deemed threats to national security.

In recent years, the Internet has attracted the main attention for cyber-related crimes involving political events, corporate and critical infrastructure hacking, fake news, child pornography and trafficking, terrorist recruitment and impersonation of celebrities, politicians and individuals. This proves that the Internet harbours uncontrollable information. With the invention of the Internet of Things, these crimes can soon spiral even more out of control.

With 3.3 billion users compared to 77 million when Barlow made the declaration, the number and variation of threats posed have increased exponentially. With VPN services readily available, users can still access foreign websites and obtain information. However, most of today's governments still do not have full control over the Internet.

Why? Because the Internet belongs to no one and everyone. It consists of layers upon layers of networks belonging to multiple companies and organizations with physical servers in various countries with diverse laws and regulations, making it extremely difficult to regulate the Internet as a whole.

The idea of splintering the World Wide Web into smaller fragments or a standalone Internet arose to counter these challenges faced by countries that hold different social, cultural, nationalist, religious and political views. Splintering the Internet (splinternet) or cyberbalkanization is a method necessitating legislature and technology to regulate the Internet without creating a new Internet infrastructure, which requires vast resources. There is no on-off switch. Cyberbalkanization combines the term "cyber" with Balkans, a political region in Southeast Europe with a history of partitioned cultures, languages and religions.[2]

From an economic perspective, fragmenting the Internet would be costly to countries, as its contribution to the world's Gross Domestic Product (GDP) in 2016 was a mind-blowing USD4.2 trillion. There are currently 3 to 4 billion people still offline, but those who are connected will be affected by such fragmentation due to censorship, laws that require local data storage, trade barriers and other regulations that limit the free flow of ideas, services and goods on the Internet.

The Great Firewall of China

The Cyberbalkanization of the Internet is nothing new. China has been cordoning the Internet after having passed the *Temporary Regulation for the Management of Computer Information Network International Connection* on January 23rd 1996, way before Barlow's declaration.[3]

China cyberbalkanized its Internet using censorship mainly due to social and political factors. In order to regulate the Internet domestically, China uses a combination of legislative and technological actions by way of the government to criminalize speech and activities, specific websites and search engine terms that are deemed to potentially damage the national interest. It also requires ISPs (both international and domestic) to store customer

© CyberSecurity Malaysia 2017 - All Rights Reserved

information within the country, thus slowing down cross-border Internet traffic.

What China calls the Golden Shield is actually a giant mechanism consisting of censorship and surveillance blocking major international social media platforms, such as Youtube, Facebook and Twitter, and replacing them with their own versions, such as Weibo and Baidu.

With almost 700 million Internet users from China, the country takes pride in its Internet sovereignty, mainly because the tech industry there is thriving. Beijing is a world leader in e-commerce and 4 of the top 10 Internet companies in the world originated there.[4]

Despite Western sceptics claiming that China's Great Firewall is oppressive due to its tight control and surveillance of the Internet, Beijing leaders of the Internet and tech communities claim that Beijing strikes the correct balance between "freedom and order" and "openness and autonomy.''

Only when Edward Snowden revealed the US government was spying on its citizens through its NSA programme did sceptics tone down criticism of Beijing's Golden Shield project.

Internet Splintering

Cyberbalkanization is not entirely new in other countries actually. In 2011, President of Egypt Hosni Mubarak ordered all ISPs to black out the Internet during the Egyptian revolution. The Internet blackout was done by interfering with routing protocols. As a result, Egypt basically dropped off the face of the Internet. Even though it was a temporary blockage, the move successfully blocked all communications to and from Egypt with the outside world, specifically targeting social media. This opened the eyes of Internet communities and governments to realize that the blockage was a form of Internet weaponization.

Internet censorship is a step forward in the direction of cyberbalkanization, as is the case in Brazil. In 2016, Marcel Maia, a Brazilian judge in Sergipe, northeast of the country ordered telecommunication providers in the country to block WhatsApp for 72 hours after the company refused to disclose messages sent between drug traffickers. The ban, however, was later overturned by a higher court.[5]

In March that year, the same judge imprisoned Diego Dzodan, Facebook's Vice President for Latin America for "repeated non-compliance" with the court's requests for WhatsApp chat logs.

Like Brazil, the Germans, who do not look too kindly upon government spying, took action after Snowden. They started investigating the construction of an "Internetz," a German-only network, with the possibility of expanding to the rest of the European Union. The current state of this project is unclear.

Cyberbalkanization/splinternet is even more apparent in conflict-ridden countries. In North Korea, only 4% of the population have Internet access, with all websites under government control. Burma filters e-mails and blocks access to groups exposing human rights violations.

In Cuba, the Internet is only available at government-controlled locations. Online activities are monitored through IP blocking, keyword filters and browsing history.

In Vietnam, he Communist Party requires Yahoo, Google and Microsoft to divulge data on all bloggers who use their platforms. It blocks websites that criticize the government, as well as those that advocate democracy, human rights and religious freedom.

In Turkmenistan, the only Internet service provider is the government, and Gmail, Yahoo and Hotmail are monitored and access to many websites is blocked.

Even America jumped on the bandwagon. Donald Trump has campaigned to "close" the Internet in areas where the U.S. has enemies, despite the fact that a large number of Internet service and social media providers dominate the social media industry and originated there.[6]

Recently, the UAE, Saudi Arabia, Yemen, the Maldives and Bahrain have cut their diplomatic relations with Qatar over its alleged support of terrorism. With Qatari nationals in UAE given 2 weeks to leave, airlines such as Emirates and Etihad suspended their flights to Qatar, leaving a big question mark of what would occur in the following week. Will countries like the UAE, Yemen and Maldives hold a blockade on their Internet too, for fear of protests on social media?

© CyberSecurity Malaysia 2017 - All Rights Reserved

Conclusion

Though the dream of original Internet pioneers was a completely open, non-hierarchical Internet, over the years barriers have been created to restrict this freedom. Slowly, the Internet is becoming more cordoned off, heading in the direction where it all started in the first place: secure military communications and defence purposes.

Even the four distinct reasons for Internet fragmentation, i.e. political, ethical, commercial, and security, all lead to the same conclusion: the map of the political world should become the map of cyberspace. This strongly suggests that the days of an open, universal Internet are numbered.

Who will fully cyberbalkanize their Internet first remains an open-ended question. Will it be China? Europe? Or even the United States? We are so used to an open and global Internet, it is difficult to imagine what a world of fragmented, national Internets might look like. What we do know is that the World Wide Web is coming to an end. When it does, it will be another nail in the coffin of globalisation.

References

1. *https://www.eff.org/cyberspace-independence*
2. *https://en.m.wikipedia.org/wiki/Splinternet*
3. *https://en.wikipedia.org/wiki/Great_Firewall*
4. *https://www.wired.com/1997/06/china-3/*
5. *https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/*
6. *http://thegrio.com/2017/01/27/donald-trump-wants-to-close-up-the-internet/*

© CyberSecurity Malaysia 2017 - All Rights Reserved

Going for Digital Detox

By | Yuzida bin Md Yazid & Nur Athirah bin Abdullah

Do you find yourself replying to WhatsApp messages and Facebook comments almost in real time? Do you spend more time looking at your gadget than chatting with your family and friends? Are you constantly checking your smartphone every few minutes for new chats, emails, 'Likes' or retweets? If the answer is YES, you are most probably close to digital stress! Information technology has changed the way we live and work. Most companies are even providing their employees smartphones with Internet connection to ensure they are contactable around the clock. Smartphones have now become a technology leash, or digital leash. With the flood of incoming texts, emails, calls, and push notifications, it is unlikely our screens will stay dark for more than a moment. There is an expectation to respond to all forms of communication as soon as possible.

Many people out there are on the brink of technology burnout but do not realize their condition. Those who already notice the symptoms may proceed on to treatment. Going on a digital detox might be one of the best options.

What is Digital Detox?

Digital detox refers to a period of time during which a person refrains from using electronic connecting devices, such as smartphones and computers. It is regarded as an opportunity to reduce stress or focus on social interaction in the physical world. Digital detox means switching off all mobiles, smartphones, tablets, laptops and computers for a certain length of time not answering emails, text messages and even staying clear of your laptop, and spending screen-free time doing whatever it is you enjoy. A digital detox gives you a chance to rest your brain and recharge your spirit.

Do you need a digital detox?

The value of face-to-face interactions with people around us is always emphasized. However, mobile phones can be a major distraction from such interactions. When was the last time you unplugged for 24 hours? If you answered "I can't remember" and if you feel that your phone is taking over your live, you definitely need a digital detox.

You need a digital detox, if....

- You aren't getting as much done as you'd like each day
- You have a hard time sleeping
- Your spouse or partner thinks you're always "on call" even when you're at home and outside office hours
- You obsessively check your social media feeds
- You have a habit of jumping on your phone at the dinner table
- The thought of going without a cell phone for 24 hours gives you anxiety

Disconnect and reconnect

Here are some ways to digitally detox yourself:

- Delete accounts that you no longer use such as your old Myspace, Friendster, Line or WeChat accounts.
- Give yourself space. Take time out from tweeting and Instagramming. This is 'me time.' If something is so funny and too interesting that you can't resist sharing, try to delay. Don't tweet it, don't forward it! Tell it to your family over dinner or call up a friend and have a real conversation. Start appreciating the people around you.
- Set your accounts as private. It's surprising and scary at the same time how many

© CyberSecurity Malaysia 2017 - All Rights Reserved

people have access to your personal stuff (pictures, thoughts, check-ins, activities, and videos) with just a click of a button. Posting everything online is like allowing a stranger to read your diary and getting very personal insight into your life. Just imagine, your pictures could be saved on almost anyone's phone or laptop in the entire world.

- Challenge yourself. What's the first thing you do in the morning? Check Twitter, WhatsApp and Instagram? Try to refrain yourself from doing this! If you still (or accidentally) do this, penalize yourself by donating RM1 to your 'Digital Detox' coin box.
- Stay off ALL your social media accounts for 24 hours. Ignore the persistently blinking light on your phone. It's difficult to imagine not being connected at all, but if you make it past 24 hours, you'll realise that it is actually possible. You can surely make it through your day without seeing another picture of a plate of nasi lemak or reading a friend's grammatically incorrect rant on FB.
- Take short technology breaks throughout the day. Or, you could take longer breaks — a few hours or more — each day. Start with half-hour breaks, then 1 hour breaks and gradually increase the period once you managed to stay away longer from your devices.

- Tell family, friends and colleagues when you're unreachable. Tell them that you will get in touch with them when you are back online.
- Inform important people on how to reach you, for example while you are on digital detox, they can reach you by phone call in case of emergency rather than text. You should still be reachable by very important people in your life.
- Pick a dedicated place to keep your phone while you're taking a break from technology. Putting your phone away shows family and friends that you are paying attention to them and they are more important than incoming messages.
- Don't go to bed with your phone even if it serves as your alarm clock. You'll tend to wake up and cannot resist checking for any messages or notifications.
- Charge your phone far away from you. For example, if you are watching TV with your family in the living room, you can charge your phone in your bedroom. It is better if your room is located upstairs, as you will be lazier to get up and check on it frequently.
- Don't use your phone to listen to music while working out at the gym or jogging. Although music is a good workout buddy, stopping mid-interval to answer a text or like a Facebook photo is not productive to burning calories. Before you exercise, turn your phone to airplane mode or do not disturb. By doing so, there is no temptation to check on your device.
- Spend longer hours on activities that will detach you from your device, such as swimming, hiking, rock climbing, cooking, and of course praying. These activities will not allow you to keep glancing at your phone every second.
- When you're in the office, turn off your phone's push notifications for social media apps including Facebook, Instagram, Pinterest, news sites — anything that sends an alert when someone contacts you or likes a post.
- Set a specific time in the day to check and a time limit for how long you will spend on a site, such as 20 minutes. This way, you're not going offline entirely but rather choosing when to access social media sites and networks
- If your boss includes you in a WhatsApp group, be smart with filtering messages. Only reply to important messages and consider their priority. A WhatsApp group for office matters is not always a good idea, as people will feel obliged to reply even if the matter can wait till tomorrow.

© CyberSecurity Malaysia 2017 - All Rights Reserved

Positive side effects of a digital detox

- You will strengthen your relationships
- You will boost your productivity
- You will increase your attention span
- You will be happier
- You will sleep better
- You will start appreciating other things in life
- You will feel calm and relaxed

However, if your nature of work requires being connected at all times, you can stay plugged in and detox at the same time. This will help you feel more fulfilled, calm, and connected to the things that really matter. If you are planning to have a digital detox retreat, be sure to leave out-of-office notices and inform your boss. Most importantly, have a co-worker be your backup for any urgent matters.

We need to realize that at the end of the day technology does not nourish us. Instead, we experience 'fear of missing out (FoMO)' and miss the 'joy of missing out (JoMO).' We need to take an honest look at what it means to be connected to technology 24/7. Only then will it become easier to make healthier choices in every aspect of our life and live to the fullest.

References

1. Wikipedia https://en.wikipedia.org/wiki/Digital_detox

2. 8 Steps for Doing a Digital Detox Without FOMO http://www.shape.com/lifestyle/mind-and-body/8-steps-doing-digital-detox-without-fomo

3. 12 Signs You Need a Digital Detox. http://www.thealternativedaily.com/12-signs-you-need-a-digital-detox/

4. Do You Need a Digital Detox? https://resources.buffiniandcompany.com/do-you-need-a-digital-detox/

5. The Center for Internet Addiction http://netaddiction.com/

© CyberSecurity Malaysia 2017 - All Rights Reserved

CyberSAFE Tips for Parents 'Educate your Child! Say No to Cyber-Bullying'

By | Elina Mubin

According to the ESET Asia Cyber Savviness Report 2015, Malaysians are the most cyber-savvy nation in the Asian region, ahead of Singapore, India, Thailand, Hong Kong and Indonesia. The study categorizes cyber-savviness based on several factors, such as the ability to understand activities likely to make users vulnerable online, risky behaviours while surfing the web, and steps users take to protect themselves online.

However, being cyber-savvy does not necessarily mean that Internet users take the right precautions or that they are even fully aware of cyber security risks posed by common online activities. For instance, users in India and Indonesia take the greatest precaution despite having the lowest level of cyber security awareness.

In light of prevailing concerns with disturbing paedophilia acts like Richard Huckle's case, preying on children on the Internet and the on-going negative social media influence changing the scale and form of child sexual abuse and exploitation, CyberSecurity Malaysia implemented the CyberSAFE Program module on Cyber Parenting. The aim was particularly to talk about how we should Educate Ourselves and Safeguard our Children's Cyber World, and Be a WISE Cyber Parents!

Top five tips on how to parent your child on cyber-bullying!

1. Recognize and Educate Your Child about the Problem

The first step in dealing with cyber bullying is to educate your children. Tell your kids about the behaviour and how to look out for warning signs. Once they are aware of the problem and what to look for, it can be prevented.

2. Assure Your Child's Trust so they will to be Open to You

If you overact and lose your temper with kids that are cyberbullying your child, he/she will find it hard to confide in you again. This causes the child to be further picked on and can even escalate the situation. Stay calm and rational. Allow your child to confide in you and support them.

3. Find support for Cyber Bullying... locally if possible

Look out for support groups and quickly put your kid in touch with others who are suffering from similar problems. This is a great way for your child to relieve of some of their hurt. Meeting others that have a similar problem can help minimize the emotional burden.

4. Reach out to friends and networks

If you discover who happens to be bullying your child, reach out to their family. This might do the trick, but at the same time, it may somewhat pose a difficult situation. If they are not reasonable people, it is best to leave it alone. If they are, perhaps speaking with them can ease the problem. You must be careful about this because some parents will never admit their child is wrong.

© CyberSecurity Malaysia 2017 - All Rights Reserved

5. Screen Shot and Save Bullying Messages and Get Help When Needed

Never erase messages of when your child is being cyberbullied. If it continues or feel it is threatening, you will benefit greatly from having proof in printed form to show the police or school. Most importantly, explain to your kid that it is not their fault. Kids need to know that bullying is a real and painful thing on the Internet as well as the school yard and you will always be there to help. Never let them feel alone. GET HELP WHEN NEEDED. If you would like to know more about how to safeguard your home computing, check out an Internet Safety Specialist or contact CYBER999.

We know that all the parenting tips in the world cannot take away the sting of finding out that your child is the victim of cyber bullying. Still, we hope that these tips will help you better cope with it!

© CyberSecurity Malaysia 2017 - All Rights Reserved

Zooming In Cyber Security Market Development

By | Nazahan bin Nazri & Mohd Affan bin Mohd Rajib

Cyber Security products and services are rising fast in an aggressive trade that helps all protect data, assets and businesses. It is also a multifarious industry with a wide range of offerings equalling the diverse needs and technologies.

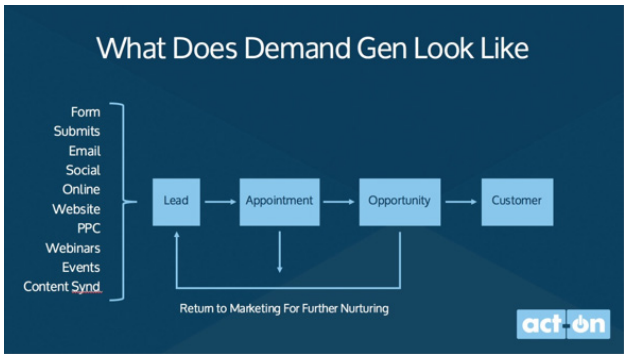
In this new digital era, wars as we know them are no longer common only on the battleground. The new playing field is the vast cyberspace, full of irony, where no one can see you, which means anyone can be anybody.

Nowadays, computer keyboards can be weapons of mass destruction whilst sensitive information can be used to hold hostage for ransom, which often leads to causalities and severe devastation. The increasing need for better cyber security has grown for years now, with major organizations at the receiving end of attacks.

Data breaches have become far more common and it is becoming harder and harder for organisations to prevent them without assistance. Placing stringent policies with the right tools and systems can mitigate the risk. Thus, cyber security business is expected to grow tremendously in the coming years.

Demand Generations

This predicament is certainly becoming a huge dilemma. However, for cyber security companies, this signifies ultimately massive demand generations. More than ever before, cyber security has now grown into a significant part of operating organisations, particularly those working in real-time and with online transactions.



Leveraging on the high-rising demand, cyber security companies need to take this opportunity to launch marketing efforts this dire instant and take advantage of the huge market segments. Let's take a closer look at those opportunities and zoom in on what is on the plate.

IoT Cyber Risk

One of the greatest apprehensions in the tech world is undeniably the massive impact that the newbie sensational awesomeness of the *Internet of Things* (IoT) will have on cyber security.

Easily hackable, Internet connected devices have already been used for *distributed-denial-of-service* (DDoS) attacks, and videos are popping up of how easy they are to break into by a skilled hacker. In years to come, cyber security companies will have plenty of tools to play while focusing on creating and marketing cyber security options not only to IoT companies but also appliance and product companies that are likely to consider creating connected devices in the future. This is a huge prospect for cyber security companies that have ICT Product Security Assessment expertise.

SPA & VAPT

In this brave new world, hackers are portrayed

© CyberSecurity Malaysia 2017 - All Rights Reserved

as super villain criminals of the cyberspace. The damage done by these hackers is beyond imagination, from retrieving sensitive government information to crashing stock markets. In contrast, as more people are learning how to hack, more cyber security companies may find they can actually hire these hackers. But finding a hacker who actually wants to work with Cyber Security companies is the tricky part.

Companies can employ hackers to expose potential vulnerabilities in potential clients' systems and prove cyber security needs by hacking (with permission) into the servers and data of potential clients. After all, B2B companies in all industries often need to prove they will be valuable to the customer. Openly proving they can hack customers' data is eventually going to be one of the most successful ways to prove that cyber security is necessary.

Another resolution is to train Cyber Security company employees to become certified pen testers, learning from the best in the field. Nowadays, numerous companies adhere to a compliance policy that requires the organisation to carry out a *Security Posture Assessment* (SPA).

Cyber Security Market Development

Cyber security market development also involves defining what cyber security actually means. There is a tendency to focus on security as a form of crime prevention. However, many companies, especially those with large IT departments, or those believing they do not have too much sensitive data are not necessarily going to suspect they are about to be the victim of a crime. Thus, cyber security companies can be expected to reframe their products not just as a form of crime prevention but also a form of consultation.

First of all, companies that utilize cyber security must be able to avoid the negative publicity that comes with a hack or data leakage. Second, those companies should also market themselves as being far more secure. If a competitor has been hacked, the companies can easily reel in potential customers. For those in highly competitive industries, this can be incredibly valuable.

SME

Cyber security firms often focus on bigger companies that can afford more expensive services. But with so many small medium enterprises (SMEs) now also holding personal data and so many more of them storing data online, this is an opportunity for cyber security companies to create a service or device with the "cyber security light" option. This would accommodate smaller businesses for far less

© CyberSecurity Malaysia 2017 - All Rights Reserved

of a cost, providing some degree of protection but not necessarily as comprehensive as larger organisations.

Old hack strategies

Cyber security trends are likely to increase in coming years. Some conventional strategies may go out of date, for example organisations that have already been hacked or sensitive information that has been compromised. This is known as predatory sales, which means waiting for an atrocious incident to happen. However, there are organisations that require digital forensic investigation in order to mitigate future risk. But these days, many companies are finding that the vulnerability and negative publicity that occur after a hack are causing them to respond poorly to this type of cold calling/active sales strategy.

Cyber security companies have targeted IT staff using language that is highly technical in nature. However, the decision makers on many forms of cyber security are not IT savvy. They are often C-level executives with little understanding of technical jargon but who still know they may need protection. We can expect to see this tendency of catering more towards those who understand the technical nature of hacking is to be phased out in favour of more plain language solutions. There are an abundance of market analyses for determining the trends of cyber security market development. Let's take a look at Porter's 5 forces analysis.

The 5 Forces Analysis that shapes the attractiveness of market development

After analysing the current and potential future state of the five competitive forces, it is possible to search for options that can influence these forces in their organization's interest. Although industry-specific business models will limit options, their own strategy can change the impact of competitive forces on the organization. The objective is to reduce the power of competitive forces.

The following figure provides some examples. They are of general nature. Hence, they have to be adjusted to each organization's specific situation. The options of an organization are determined not only by the external market environment, but also by its own internal resources, competences and objectives.

© CyberSecurity Malaysia 2017 - All Rights Reserved

1. Reducing the Bargaining Power of Suppliers

- Partnering
- Supply chain management
- Supply chain training
- Increase dependency
- Build knowledge of supplier costs and methods
- Take over a supplier

2. Reducing the Bargaining Power of Customers

- Partnering
- Supply chain management
- Increase loyalty
- Increase incentives and value added
- Move purchase decision away from price
- Cut out powerful intermediaries (go directly to customer)

3. Reducing the Threat of New Entrants

- Increase minimum efficient scales of operations
- Create a marketing/brand image (loyalty as a barrier)
- Patents, protection of intellectual property
- Alliances with linked products/services
- Tie up with suppliers
- Tie up with distributors
- Retaliation tactics

4. Reducing the Threat of Substitutes

- Legal actions
- Increase switching costs
- Alliances
- Customer surveys to learn about their preferences
- Enter substitute market and influence from within
- Accentuate differences (real or perceived)

5. Reducing the Competitive Rivalry between Existing Players

- Avoid price competition
- Differentiate your product
- Buy out competition
- Reduce industry over-capacity
- Focus on different segments
- Communicate with competitors

Conclusion

Using well-thought out strategies may assist cyber security companies to identify potential gaps while at the same time improve market shares. It seems every day there are reports of new hacks, and every day the need for cyber security grows. It is in the best interest of cyber security companies to continually look at new security marketing trends and do whatever it takes to reach a new, broader audience with their products and services.

References

1. http://cybersecurityventures.com/cybersecurity-market-report/

2. http://www.cgma.org/resources/tools/essential-tools/porters-five-forces.html

3. http://www.information-age.com/11-trends-will-dominate-cyber-security-2016-123460617/

4. http://www.indigocube.co.za/cyber-security/cyber-security-development

© CyberSecurity Malaysia 2017 - All Rights Reserved

Approved Cryptographic Algorithms in ISO/IEC Standards.

By | Nik Azura binti Nik Abdullah, Norul Hidayah binti Lot Ahmad Zawawi, Liyana Chew binti Nizam Chew, Nor Azeala binti Mohd Yusof

When developing a cryptographic devices, or implementing cryptography in any sectors such as payment industry, banking, smartcards, and Internet of Things (IoT), it is vital to know which cryptographic algorithms are suitable to be used. Usage of approved cryptographic algorithms listed in international standards, which are recognize all over the world, will provide assurance of product's or implementation's security and at the same will boost user's confidence in choosing a safe solution. Such cryptographic algorithms have been tested, evaluated and cryptanalyzed to ensure that it meets its intended functionality. Most standards are being reviewed and updated regularly in a periodic manner. Therefore, it can be assured that the cryptographic implementations are according to current trends.

The following organizations / groups developed well-known and most widely used international standards with regards to cryptographic algorithms:-

- International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC)
- National Institute of Standards and Technology (NIST) – FIPS standards
- Institute of Electrical and Electronics Engineers (IEE)
- American National Standards Institute (ANSI)
- European Telecommunications Standards Institute (ETSI)
- Internet Engineering Task Force (IETF) – RFC standards
- RSA Security LLC – PKCS standards.
- In this article, we will provide lists of approved cryptographic algorithm recorded by ISO/IEC.

ISO/IEC

ISO/IEC JTC 1 is a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its purpose is to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT). The developments of the ISO/IEC standard are done by subcommittees (SCs) and most of these subcommittees have several working groups (WGs), special working groups (SWGs), and study groups (SGs). The technical committee for JTC 1, within the field of IT Security techniques is ISO/IEC JTC 1/SC 27. This technical committee comprises of five WGs and two SWGs:

- ISO/IEC JTC 1/SC 27/WG 1: Information security management systems
- ISO/IEC JTC 1/SC 27/WG 2: Cryptography and security mechanism
- ISO/IEC JTC 1/SC 27/WG 3: Security evaluation, testing and specification
- ISO/IEC JTC 1/SC 27/WG 4: Security controls and services
- ISO/IEC JTC 1/SC 27/WG 5: Identity management and privacy technologies
- ISO/IEC JTC 1/SC 27/SWG-M: Management
- ISO/IEC JTC 1/SC 27/SWG-T: Transversal items

One of the aspects which ISO/IEC JTC 1/SC 27 addresses is the cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information. The ISO/IEC JTC 1/SC 27/WG 2 is responsible for the technical development of this scope.

1. ISO/IEC 18033 Standards

Approved encryption algorithms are as in ISO/IEC 18033: Information technology -- Security techniques -- Encryption algorithms standards.

ISO/IEC 18033-2: 2006 Part 2: Asymmetric ciphers

This standard specifies asymmetric encryption algorithms for the purpose of data confidentiality. It also specifies the functional interface of such

© CyberSecurity Malaysia 2017 - All Rights Reserved

a scheme, and in addition specifies a number of particular schemes that appear to be secure against chosen ciphertext attack. The different schemes offer different trade-offs between security properties and efficiency. Algorithms that are allowed in this part of ISO/IEC 18033 are:

- El-Gamal based Key Encapsulation Mechanism:
  - ECIES -KEM
  - PSEC-KEM (Provably Secure Elliptic Curve encryption – Key encapsulation Mechanism)
  - ACE-KEM (Advanced Cryptographic Engine–Key Encapsulation Mechanism)
- RSA-based Key Encapsulation Mechanism (RSA-KEM):
  - REM1 – RSA encoding mechanism
  - RSAES – bounded-plaintext-length asymmetric ciphers
- Data Encapsulation Mechanism (DEM):
  - DEM 1 - data encapsulation mechanism
  - DEM 2 - fixed-label-length data encapsulation mechanism
  - DEM 3 – fixed-plaintext-length
- Cipher based on modular squaring
  - HIME
  - HIME (R) – bounded-plaintext-length asymmetric ciphers

ISO/IEC 18033-3: 2010 Part 3: Block ciphers

This standard specifies block cipher symmetric encryption algorithms for the purpose of data confidentiality. Algorithms that are allowed in this part of ISO/IEC 18033 are:

Block length	Algorithm name	Key length
64 bits	Triple Data Encryption Algorithm (TDEA)	128 or 192 bits
	MISTY1	128 bits
	CAST-128	
	HIGHT	
128 bits	AES	128, 192 or 256 bits
	Camelia	
	SEED	128 bits

ISO/IEC 18033-4: 2011 Part 4: Stream ciphers

This standard specifies stream cipher symmetric encryption algorithms that produce keystream to combine with plaintext, keystream generators for producing keystream, and object identifiers assigned to dedicated keystream generators in accordance with ISO/IEC 9834. Algorithms that are allowed in this part of ISO/IEC 18033 are:

Algorithm Name	Key Length
MUGI	128 bits
SNOW 2.0	128 or 256 bits
Rabbit	128 bits
Decimv2	80 bits
KCipher-2 (K2)	128 bits

ISO/IEC 18033-5: 2015 Part 5: Identity-based ciphers

This standard specifies identity-based encryption mechanisms. Algorithms that are allowed in this part of ISO/IEC 18033 are:

- BF ID-based encryption mechanism
- SK ID-based key encapsulation mechanism
- BB1 ID-based key encapsulation mechanism

ISO/IEC CD 18033-6 Part 6: Homomorphic encryption

This standard is still under development. However, it specifies homomorphic encryption that supports one operation, sometimes referred to as “partially homomorphic” as opposed to “fully homomorphic” encryption that support universal computations in the encrypted domain, is powerful enough to secure a wide range of applications in the cloud computing sector.

2. ISO/IEC 10118 Standards

Approved cryptographic hash function algorithms are as in ISO/IEC 10118: Information technology -- Security techniques -- Hash-functions standards.

ISO/IEC 10118-2: 2010 Part 2: Hash-functions using an *n*-bit block cipher

This standard specifies hash-functions which makes use of n-bit block cipher algorithms. Algorithms that are allowed in this part of ISO/

© CyberSecurity Malaysia 2017 - All Rights Reserved

IEC 10118 are:

Hash-function type	Hash-code length (*n* is the block length of the algorithm)		
	L_1	L_2	L_H
Hash-function 1	$=n$	$=n$	$\leq n$
Hash-function 2	$=n$	$=2n$	$\leq 2n$
Hash-function 3	$=4n$	$=8n$	$= 2n$
Hash-function 4	$=3n$	$=9n$	$= 3n$

ISO/IEC 10118-3: 2004 Part 3: Dedicated hash-functions

This standard specifies the round-function that consists of a sequence of sub-functions, the padding method, initializing values, parameters, constants, and the object identifier as normative information, and also specifies several computation examples as informative information. Algorithms that are allowed in this part of ISO/IEC 10118 are:

Hash-function type	Hash-code length (*n* is the block length of the algorithm)		
	L_1	L_2	L_H
RIPEMD-160	512	160	Up to 160
RIPEMD-128	512	128	Up to 128
SHA-1	512	160	Up to 160
SHA-256	512	256	Up to 256
SHA-512	1,024	512	Up to 512
SHA-384	1,024	512	384
WHIRLPOOL	512	512	Up to 512

ISO/IEC 10118-4: 1998 Part 4: Hash-functions using modular arithmetic

This standard specifies two hash-functions which make use of modular arithmetic. Algorithms that are allowed in this part of ISO/IEC 10118 are:

- MASH-1
- MASH-2

3. ISO/IEC 29192 Standards

Approved cryptographic lightweight algorithms are as in ISO/IEC 29192: Information technology -- Security techniques -- Lightweight cryptography standards.

ISO/IEC 29192-2: 2012 Part 2: Block ciphers

This standard specifies two block ciphers suitable for lightweight cryptography. Algorithms that are allowed in this part of ISO/IEC 29192 are:

Block length	Algorithm name	Key length
64 bits	PRESENT	80 or 128 bits
128 bits	CLEFIA	128, 192 or 256 bits
512	160	Up to 160

© CyberSecurity Malaysia 2017 - All Rights Reserved

ISO/IEC 29192-3: 2012 Part 3: Stream ciphers

This standard specifies two dedicated keystream generators for lightweight stream ciphers. Algorithms that are allowed in this part of ISO/IEC 29192 are:

Algorithm name	Key length
Enocoro	80 or 128 bits
Trivium	80 bits

ISO/IEC 29192-4: 2013 Part 4: Mechanism using asymmetric techniques

This standard specifies three lightweight mechanism using asymmetric techniques. Algorithms that are allowed in this part of ISO/IEC 29192 are:

- a unilateral authentication mechanism based on discrete logarithms on elliptic curves;
- an authenticated lightweight key exchange (ALIKE) mechanism for unilateral authentication and establishment of a session key;
- an identity-based signature mechanism.

ISO/IEC 29192-5: 2016 Part 5: Hash-functions

This standard specifies three hash-functions suitable for applications requiring lightweight cryptographic implementation. Algorithms that are allowed in this part of ISO/IEC 29192 are:

Algorithm name	Permutation size	Hash-code length
PHOTON	100, 144, 196, 256 and 288 bits	80, 128, 10, 224 and 256 bits
SPONGENT	88, 136, 176, 240 and 272 bits	88, 128, 160, 224 and 256 bits
Lesamnta-LW	384 bits	256 bits

ISO/IEC NP 29192-6: Part 6: Message authentication codes (MACs)

This standard is still under development.

4. ISO/IEC 9796 Standards

Approved digital signature schemes are as in ISO/IEC 9796: Information technology -- Security techniques -- digital signature schemes giving message recovery standards.

ISO/IEC 9796-2: 2010: Integer factorization based mechanism
This standard specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. Algorithms that are allowed in this part of ISO/IEC 9796 are:

a. MAC Algorithm 1

Dedicated Hash-Function	The MDx-MAC algorithm is also known as
Dedicated Hash-function 1	RIPEMD-160-MAC
Dedicated Hash-function 2	RIPEMD-128-MAC
Dedicated Hash-function 3	SHA-1-MAC
Dedicated Hash-function 4	SHA-256-MAC
Dedicated Hash-function 5	SHA-512-MAC

© CyberSecurity Malaysia 2017 - All Rights Reserved

Dedicated Hash-function 6	SHA-384-MAC
Dedicated Hash-function 8	SHA-224-MAC

MAC Algorithm 1 requires five steps: key expansion, modification of the constant and the IV, hashing operation, output transformation, and truncation.

b. MAC Algorithm 2

Dedicated Hash-Function	The MDx-MAC algorithm is also know as
Dedicated Hash-function 1	RIPEMD-160-MAC
Dedicated Hash-function 2	RIPEMD-128-MAC
Dedicated Hash-function 3	SHA-1-MAC
Dedicated Hash-function 4	SHA-256-MAC
Dedicated Hash-function 5	SHA-512-MAC
Dedicated Hash-function 6	SHA-384-MAC
Dedicated Hash-function 7	WHIRLPOOL-MAC
Dedicated Hash-function 8	SHA-224-MAC

MAC Algorithm 2 requires four steps: key expansion, hashing operation, output transformation, and truncation.

c. MAC Algorithm 3

Dedicated Hash-Function	The MDx-MAC algorithm is also know as
Dedicated Hash-function 1	RIPEMD-160-MAC
Dedicated Hash-function 2	RIPEMD-128-MAC
Dedicated Hash-function 3	SHA-1-MAC
Dedicated Hash-function 4	SHA-256-MAC
Dedicated Hash-function 5	SHA-512-MAC
Dedicated Hash-function 6	SHA-384-MAC
Dedicated Hash-function 8	SHA-224-MAC

MAC Algorithm 3 requires five steps: key expansion, modification of the round function, padding, application of the round-function, and truncation.

ISO/IEC 9796-3: 2006: Discrete logarithm based mechanism

This standard specifies digital signature mechanisms giving partial or total message recovery aiming at reducing storage and transmission overhead. Algorithms that are allowed in this part of ISO/IEC 9796 are NR defined on prime field and ECNR, ECMR, ECAO, ECPV, and ECKNR defined on an elliptic curve over a finite field.

5. ISO/IEC 10116: 2006 Standards

Approved modes of operation are as in ISO/IEC 10116: Information technology -- Security techniques – Modes of operation for an n-bit block cipher. This standard specifies modes of operation for an n-bit block cipher. These modes only provide protection of data confidentiality. Protection of data integrity and requirements for padding the data are not within the scope of this standard. Five modes of operations that are allowed in this part of ISO/IEC 10116 are Electronic Codebook (ECB), Cipher Block Chaining (CBC) with optional interleaving, Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR).

© CyberSecurity Malaysia 2017 - All Rights Reserved

References

1. *ISO/IEC JTC 1/SC 27 IT Security techniques https://www.iso.org/committee/45306.html*

2. *List of International Organization for Standardization standards https://en.wikipedia.org/wiki/List_of_International_Organization_for_Standardization_standards*

3. *ISO/IEC 18033-2: 2006 Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers.*

4. *ISO/IEC 18033-3: 2010 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*

5. *ISO/IEC 18033-4: 2011 Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers*

6. *ISO/IEC 18033-5: 2015 Information technology -- Security techniques -- Encryption algorithms -- Part 5: Identity-based ciphers*

7. *ISO/IEC CD 18033-6: Information technology -- Security techniques -- Encryption algorithms -- Part 6: Homomorphic encryption*

8. *ISO/IEC 10118-2: 2010 Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher*

9. *ISO/IEC 10118-3: 2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions*

10. *ISO/IEC 10118-4: 1998 Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functios using modular arithmetic*

11. *ISO/IEC 29192-2: 2012: Information technology -- Security techniques -- Lightweight cryptography standards -- Part 2: Block ciphers*

12. *ISO/IEC 29192-3: 2012: Information technology -- Security techniques -- Lightweight cryptography standards -- Part 3: Stream ciphers*

13. *ISO/IEC 29192-4: 2013: Information technology -- Security techniques -- Lightweight cryptography standards -- Part 4: Mechanism using asymmetric techniques*

14. *ISO/IEC 29192-5: 2016: Information technology -- Security techniques -- Lightweight cryptography standards -- Part 5: Hash-functions*

15. *ISO/IEC 29192-6: Information technology -- Security techniques -- Lightweight cryptography standards -- Part 6: Message authentication codes (MACs)*

16. *ISO/IEC 9796-2: 2010 Information technology -- Security techniques -- digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanism*

17. *ISO/IEC 9796-3: 2006 Information technology -- Security techniques -- digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanism*

18. *ISO/IEC 10116: Information technology -- Security techniques – Modes of operation for an n-bit block cipher*

19. *https://www.cryptoexperts.com/services/standardization/*

© CyberSecurity Malaysia 2017 - All Rights Reserved

Approved Cryptographic Algorithm in NCA[1] Projects

By | Nik Azura Bt Nik Abdullah, Norul Hidayah Bt Lot Ahmad Zawawi, Liyana Chew Bt Nizam Chew, Nor Azeala Bt Mohd Yusof, Faridatul Akhma Binti Ishak

Strong cryptographic algorithms and secure protocol standards are essential tools that contribute to national security. A few countries have taken the initiative to develop a list of approved algorithms for their governments and commercial purposes. This article lists the approved algorithms for NCA projects in Europe, Japan, Australia, Canada and New Zealand.

EUROPE - NESSIE

1. NESSIE is the New European Schemes for Signatures, Integrity and Encryption.
2. NESSIE is a European research project to identify secure cryptographic primitives.
3. NESSIE is intended to identify and evaluate quality cryptographic designs in several categories.
4. From 42 submissions received, 12 were selected.
5. 5 publicly known algorithms but not explicitly submitted to the project were chosen as "selectees".
6. This project publicly announced that "no weaknesses were found in the selected designs".

Symmetric Cryptographic Algorithms
Block Cipher – AES, MISTY, Camellia, SHACAL-2

Asymmetric Cryptographic Algorithms
Encryption – PSEC-KEM, RSA-KEM, ACE-KEM

Hash Function Algorithms
SHA-256, SHA-384, SHA-512, Whirlpool

1. *NCA project = National Cryptographic Algorithms Project*

© CyberSecurity Malaysia 2017 - All Rights Reserved

JAPAN – CRYPTREC

1. CRYPTREC denotes the Cryptography Research and Evaluation Committee.
2. CRYPTREC is a project to evaluate and recommend cryptographic techniques for government and industry use.
3. CRYPTREC was set up by the Japanese Government, including members of the Japanese academia, industry and government.
4. This project combines the efforts of several agencies who are investigating methods and techniques of implementing 'e-Government' in Japan.
5. The CRYPTREC cipher list was divided into three categories: "e-Government Recommended Cipher List" (List 1), "Candidate Recommended Cipher List" (List 2) and "Monitored Cipher List".

Symmetric Cryptographic Algorithms

List 1 Block Ciphers - AES, TDEA
List 2 Block Ciphers - MISTY1, CLEFIA, CIPHERUNICORN-E, Hierocrypt-L1, CIPHERUNICORN-A, Hierocrypt-3, SC2000

List 1 Stream Ciphers - KCipher-2
List 2 Stream Ciphers - Enocoro-128 v2, MUGI , MULTI-S01

Asymmetric Cryptographic Algorithms

Digital Signature - Digital signature algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), RSA-PSS, RSASSA-PKCS1-V1.5

Encryption - PSEC-KEM, RSA-OAEP

Key Exchange - Diffie-Hellman (DH), Elliptic curve Diffie–Hellman (ECDH)

Hash Function Algorithms

List 1 - SHA-256, SHA-384, SHA-512
List 2 - SHAKE256, SHA-512/256, SHA-256, SHA-384, SHA-512

© CyberSecurity Malaysia 2017 - All Rights Reserved

Australia - DSD

1. DSD is the Defence Signals Directorate.
2. DSD explicitly approved and detailed the use of Suite B algorithms to protect information classified as CONFIDENTIAL and above.
3. Agencies must use products endorsed by DSD in order to protect information classified as CONFIDENTIAL and above.

Symmetric Cryptographic Algorithm
Block Cipher - AES

Asymmetric Cryptographic Algorithms

Digital Signature - RSA Digital Signature Algorithm (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA)

Key Exchange - Diffie-Hellman (DH), Elliptic curve Diffie-Hellman (ECDH), RSA

Hash Function Algorithms
SHA-256, SHA-384 (For top secret)

© CyberSecurity Malaysia 2017 - All Rights Reserved

CANADA - CSE

1. CSE is the abbreviation of Communications Security Establishment.
2. CSE is the Canadian government's national cryptologic agency administered under the Department of National Defence (DND).
3. CSE's mission is to provide and protect information of national interest through leading-edge technology in synergy with their partners.
4. CSE's vision is safeguarding Canada's security through information superiority.
5. CSE employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign signals intelligence services.
6. CSE also provides technical and operational assistance to the Royal Canadian Mounted Police and federal law enforcement and security agencies.

Symmetric Cryptographic Algorithms
Block Cipher - AES, TDEA (3-key option & 2-key option), CAST-128

Asymmetric Cryptographic Algorithms

Digital Signature - Digital signature algorithm (DSA), RSA Digital Signature Algorithm (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA)

Key Establishment Schemes - RSA, Diffie-Hellman and Menezes-Qu-Vanstone, Elliptic Curve Cryptography Cofactor Diffie-Hellman and Menezes-Qu-Vanstone

Hash Function Algorithms
SHA-1, SHA-2, SHA-3

© CyberSecurity Malaysia 2017 - All Rights Reserved

New Zealand - GCSB

1. GCSB stands for the Government Communications Security Bureau.
2. GCSB contributes to New Zealand's national security by providing:
   - Information assurance and cyber security to the New Zealand Government and critical infrastructure organisations.
   - Foreign intelligence to government decision-makers.
   - Cooperation and assistance to other New Zealand government agencies.

Symmetric Cryptographic Algorithm
Block Cipher – AES-256, TDEA

Asymmetric Cryptographic Algorithms

Digital Signature - Elliptic Curve Digital Signature Algorithm (ECDSA)

Key Exchange - Diffie-Hellman, Elliptic curve Diffie-Hellman (ECDH)

Hash Function Algorithms
SHA-1, SHA-256, SHA-384, SHA-512

© CyberSecurity Malaysia 2017 - All Rights Reserved

Cryptography and Virus

By | Isma Norshahila binti Mohammad, Abdul Alif bin Zakaria

Introduction

Cryptology is an art and science of hidden and secret writing. It has two main components, which are cryptography and cryptanalysis. Cryptography is the practice and study of modifying information so that it becomes unintelligible. It is used to provide secrecy and integrity to data, and both authentication and anonymity to communications. Cryptanalysis is the practice and study of breaking codes to evaluate the strength and relevance of the current algorithm.

There are two categories of cryptography, namely symmetric and asymmetric key cryptography. Symmetric key cryptography, also known as secret key cryptography, is a form of cryptography that allows users to communicate securely by using a single key. Both sender and receiver share the same key. Asymmetric key cryptography allows users to communicate securely by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically. The private key is kept secret while the public key may be widely distributed.

Traditionally, cryptography has been used for defence purposes. Ciphers defend against passive eavesdroppers; digital signature algorithms defend against forgers; pseudorandom bit generators defend against next bit predictors, and so on. In 1996, a new area of cryptology with focus on cryptography and viruses was invented, which is called cryptovirology. Cryptovirology extends beyond finding protocol failures and design vulnerabilities. This forward engineering discipline can be used for attacking rather than defending.

Cryptovirology

Cryptovirology is the study of the applications of cryptography to malicious software. It employs public key cryptography to mount attacks on computer systems, which shows that cryptography also has negative usage. The combination of virus science and cryptography is cryptovirology. Cryptovirology attacks have been categorized as:

"give malware-enhanced privacy and be more robust against reverse engineering, secondly give the attacker enhanced anonymity while communicating with deployed malware"

The first cryptovirology attack is called "cryptoviral extortion." It was invented by Adam L. Young and Moti Yung and was presented at the 1996 IEEE Security & Privacy Conference [1]. In this attack, a cryptovirus, cryptoworm, or cryptotrojan that contains the attacker's public key encrypts the victim's file and asks for payment in exchange for the decryption key. If there is no backup, the victim must pay to get the file back. The authors predicted that cryptoviral extortion attackers would have demanded e-money long before bitcoin even existed. Many years later, the media re-labeled cryptoviral extortion as ransomware.

Viruses

In computer science, there are several types of viruses, such as viruses, trojans, worms, spyware and adware [2]. A virus is a malicious piece of code that copies itself and infects a computer without the user's permission or knowledge, while a trojan is a type of computer software that camouflages as regular software, such as utilities, games and sometimes even antivirus programs. A worm is a self-replicating computer program that uses a network to send copies of itself to other nodes. Spyware is a computer software that gets installed on a personal computer to intercept or take partial control of the user's interaction with the computer, without the user's informed consent. Adware is an advertising-supported software that spies on users to know about their likes and dislikes.

Cryptovirus

A cryptovirus is defined as a computer virus that contains and uses a public key. Usually, the public key belongs to the author of the virus, but there are other possibilities as well. For instance, a virus or worm may generate and use its key pair at runtime. Cryptoviruses may utilize secret sharing to hide information and may communicate by reading posts from public bulletin boards. Cryptotrojans and cryptoworms

© CyberSecurity Malaysia 2017 - All Rights Reserved

are the same as cryptoviruses, except they are trojan horses and worms, respectively. Note that under this definition, a virus that uses a symmetric key and not a public key is not a cryptovirus. A virus that contains and uses a symmetric key to encrypt and decrypt its code is called a polymorphic virus [4].

Typical Cryptoviral Attack

This attack is done in a few steps. First, the cryptovirus attaches itself to some data, which it will encrypt by using a symmetric key. Subsequently, the symmetric key and the data will be encrypted using the author's public key. The author will then put the data up for ransom. The victim may choose to either pay the ransom money or lose the data.

Cryptoviruses, or ransomware, have evolved rapidly since 2013. CryptoLocker is a malicious cyber threat that was spotted in 2013. It propagates via infected email attachments, encrypting files on a local computer hard drive or mounted network drive using RSA public key cryptography with the private key stored only on its control server. Once it is loaded, the user will receive a message telling them they must pay in Bitcoins or with a prepaid voucher by a specific deadline to get access to the locked files. It will threaten to delete the private key if the deadline passes. CryptoLocker was taken down in an international operation in 2014. However, the scammers still got away with some $3 million.

In 2016, the ransomware continued to wreak havoc. Attacks and ransom demands went up. Payments were frequently made using Bitcoins. One of the attacks was in San Francisco, when cyber criminals breached San Francisco's light rail network systems [8]. However, the victim avoided paying because its system had a backup. Another attack that happened in 2016 was at a Hollywood hospital, which forced a payment of $17,000 in bitcoins to retrieve the data [9].

Wannacry Ransomware

A global cyberattack underway since May 2017 has affected more than 200,000 organizations in 150 countries [10]. The "WannaCry" ransomware appears to have used a flaw in Microsoft's software, discovered by the National Security Agency and leaked by hackers, to spread rapidly across networks locking away files. For cybercriminals to gain access to the system, they need to download a type of malicious software onto a device within the network. This is often done by getting a victim to click on a link or download it by mistake.

Ransomware often demands between 0.3 and 1 Bitcoins (£400 - £1,375) but can demand a payment denominated in dollars made via Bitcoin. This digital currency is popular among cybercriminals because it is decentralized, unregulated and practically impossible to trace. It demands payment in Bitcoins, gives instructions on how to buy them, and provides a Bitcoin sending address.

A young cyber expert managed to stop the spread of the attack by accidentally triggering a "kill switch" when he bought a web domain for less than £10. When the WannaCry program infects a new computer, it contacts the web address. It is programmed to terminate itself if it manages to get through. When the 22-year-old researcher bought the domain, the ransomware was connected and he therefore stopped this attack.

Countermeasures For Cryptoviruses

Several measures can be taken to significantly reduce the risk of being infected by a cryptovirus. The possible countermeasures are as follows:

1. Perform regular backups of critical information to limit the impact of data or system loss and to help expedite the recovery process. Keep this data on a separate device, and backups should be stored offline
2. Maintain up-to-date antivirus and antispyware software
3. Keep the operating system and software up-to-date regularly with the latest patches
4. Encrypt important data
5. Do not follow unsolicited web links in email
6. Be extra careful when opening email attachments
7. Follow best and safe practices when browsing the web

© CyberSecurity Malaysia 2017 - All Rights Reserved

Conclusion

Cryptography has been traditionally used for defence purposes, but cryptovirology uses cryptography for attacking rather than defending. Cybersecurity companies have developed sophisticated defences against cyberattacks, including machines that fight back when they spot hackers in a system. Cryptovirology is a proactive anticipation of the opponent's next move and suggests that certain safeguards should be developed and put into place.

References

1. *Young, A., & Yung, M. (1996). Cryptovirology: extortion-based security threats and countermeasures. Security and Privacy, 1996. Proceedings.*
2. *http://www.computerhope.com*
3. *https://security4web.org*
4. *https://www.bankvaultonline.com/knowledge-base/explainers/viruses-polymorphic-code-2/*
5. *http://en.wikipedia.org/wiki/Cryptovirology*
6. *http://www.cryptovirology.com/*
7. *Young, A., & Yung, M. (2004). Malicious cryptography: Exposing cryptovirology. John Wiley & Sons.*
8. *http://www.cnbc.com/2016/11/29/why-transportation-networks-are-especially-vulnerable-to-ransomware.html*
9. *http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html*
10. *http://www.telegraph.co.uk/technology/0/ransomware-does-work/*

© CyberSecurity Malaysia 2017 - All Rights Reserved

Lightweight Cryptography in Internet of Things

By | Isma Norshahila binti Mohammad, Hazlin binti Abdul Rani

Internet Of Things And Lightweight Cryptography

The Internet of Things (IoT) refers to objects or devices that are able to interact and transfer data between them via Internet networks. The IoT evolution has led us to live in an environment that moves in all directions with an Internet connection. Today, most objects around us are connected and interact actively through the Internet.

IoT allows objects and people working together to produce and use various services to achieve common goals. Examples of IoT applications are smart cities (e.g. lighting, waste management and the environment), incident response (e.g. access control), retail (e.g. supply chain control and logistics) and home automation (e.g. intrusion detection and intelligent space).

While IoT provides new and exciting experiences for end users, it also opens up new avenues to hackers and organized crime. Three important things that should be emphasized in ensuring the security of smart devices are as follows:

1. The overhead of security solutions
   - Should be minimal due to the low-cost nature of smart devices, e.g. the gate count in hardware or the memory footprint in software
2. The power consumption of smart devices
   - Should be minimal because one of the features of smart devices is low-power
3. The performance of security solutions
   - Must be appropriate to support the needs of applications and end users

To address the above problem, a new study called lightweight cryptography was established to focus on designing cryptographic algorithms and protocols appropriate for use in a limited environment.

Lightweight cryptography is a subfield of cryptography aimed to provide solutions tailored for resource-constrained devices used in IoT, such as RFID tags, sensors, contactless smart cards, healthcare devices and so on. A number of lightweight primitives, including block ciphers, hash functions, message authentication codes and stream ciphers have been proposed to bring performance advantages over conventional cryptographic standards.

These primitives differ from conventional standards in the assumption that lightweight primitives are not intended for a wide range of applications.

In many conventional cryptographic standards, the trade-off between security, performance and resource requirements is optimized for desktop and server environments. This makes them difficult or impossible to implement in resource-constrained devices.

The idea of lightweight cryptography is to reach a better balance between security, performance and resource requirements (cost) for specific resource-constrained environments. Figure 1 shows the metrics and trade-offs of lightweight cryptography.

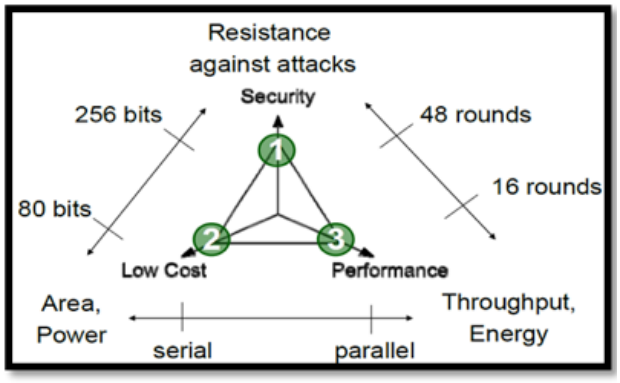


Figure 1: Metrics and Trade-offs of Lightweight Cryptography

Lightweight cryptography targets a wide variety of devices that can be implemented on a broad spectrum of hardware and software. The corresponding types of cryptography and devices are given in Table 1.

High end of device spectrum	Servers and Desktops	Conventional cryptography	
	Tablets and Smartphones		
Lower end of device spectrum	Embedded Systems	Lightweight cryptography	Highly constrained devices
	RFID and Sensor Networks		

Table 1: Corresponding types of cryptography and devices

© CyberSecurity Malaysia 2017 - All Rights Reserved

Lightweight Cryptographic Primitives

Generally, lightweight cryptographic primitives are divided into four categories, which are lightweight block ciphers, lightweight hash functions, lightweight message authentication codes and lightweight stream ciphers.

Lightweight Block Ciphers

Lightweight block ciphers are block ciphers that require less computing power. They are designed to fulfil the needs of constrained devices, such as RFID tags and sensor networks. A series of lightweight block ciphers have been proposed recently, including DESL, PRESENT, SIMON and SPECK. The performance benefits of lightweight block ciphers over conventional block ciphers achieved using lightweight design choices are as follows:

1. Smaller block sizes
   - Smaller sizes than AES are used to save memory.
2. Smaller key sizes
   - Small key sizes (less than 96 bits) are used for efficiency.
3. Simpler rounds
   - In lightweight designs, 4-bit S-boxes are preferred over 8-bit S-boxes. This size reduction results in significant area savings.
   - For hardware-oriented designs, bit permutations or recursive MDS matrices may be preferred over complex linear layers.
   - When rounds are simpler, they may need to be iterated more times to achieve security.
4. Simpler key schedule
   - Most lightweight block ciphers use simple key schedules that can generate sub-keys on the fly.
5. Minimal implementation
   - Implementing only the necessary cipher functions (e.g. encryption or decryption only) may require fewer resources than implementing the full cipher.

A list of examples of lightweight block ciphers and their implementation is given in Table 2.

No	Algorithm Name	Block size (bits)	Key Size (bits)	Implementation
1	CLEFIA	128	128, 192, 256	Both software and hardware implementation 1. Smart cards 2. Mobile devices
2	PRESENT	64	80. 128	1. RFID tags 2. Sensor networks
3	mCrypton	64	64, 96, 128	Low-cost RFID tags and sensors
4	Hight	64	128	1. Sensor in USN 2. RFID tag
5	Lee	64	128	Sensor network nodes
6	Katan/Ktantan	80	32, 48, 64	Low end devices - RFID tags
7	Klein	64	64, 80, 96	Resource-constrained devices especially for wireless sensor networks
8	PRINTcipher	48 96	80 160	Printed passive RFID tags

Table 2: Examples of lightweight block ciphers and their implementation

Lightweight Hash Functions

A hash function is a function that maps a bit sequence of arbitrary length to a fixed-length output. As a rule, there are three security requirements for a hash function. First, it should be preimage resistant: given an output (hash value), it should be hard to find an input (message) that would map to this output. Second, it should be second-preimage resistance: given a hash value and a corresponding message, it should be difficult to find another message

© CyberSecurity Malaysia 2017 - All Rights Reserved

with the same hash value. Finally, it should be collision resistant: it should be infeasible to find two messages with the same hash value.

Examples of typical applications for lightweight hash functions are lightweight signature schemes, RFID security protocols, random number generators and post-quantum signature schemes.

The expected usage of conventional and lightweight hash functions differs in various aspects, such as smaller internal state and output size, and smaller message size. Large output sizes are important for applications that require collision resistance of hash functions. For applications that do not require collision resistance, smaller internal and output sizes might be used.

Conventional hash functions are expected to support inputs with very large sizes (around 264 bits). In most target protocols for lightweight hash functions, typical input sizes are much smaller (e.g. at most 256 bits). Hash functions that are optimized for short messages may therefore be suitable for lightweight applications.

A list of examples of lightweight hash functions and their implementation is provided in Table 3.

No	Algorithm Name	Block size (bits)	Key Size (bits)	Implementation
1	Keccak/SHA-3	arbitrary	1600	Winner of NIST SHA-3 Competition
2	Armadillo	80, 128, 160, 192, 256	256, 384, 480, 576, 768	Hardware
3	Photon	80, 128, 160, 224, 256	100, 144, 196, 256, 288	Hardware
4	Spongent	80, 128, 160, 224, 256	88, 136, 176, 240, 272	ASIC Hardware
5	Quark	136, 176, 256	136, 176, 256	Hardware
6	Lesamnta-LW	256	256	NIST SHA-3 Competition candidate

Table 3: Examples of lightweight hash functions and their implementation

Lightweight Message Authentication Codes

Message authentication codes (MACs) are classically used for preventing unauthorized and corrupted messages from being forwarded in a network. A MAC generates a tag from a message and a secret key, which is used to verify the authenticity of the message. Recommended tag sizes for lightweight MACs are at least 64 bits for typical applications. Table 4 shows examples of lightweight message authentication codes and their descriptions.

No	Algorithm	Block size (bits)
1	Chaskey	▪ A permutation-based algorithm ▪ Takes 128-bit keys and processes 128-bit block messages using a 128-bit permutation ▪ Features: dedicated design for 32-bit microcontroller architecture, cross-platform versatility, resistance against timing attacks, key agility and patent-free.
2	TuLP	▪ Dedicated design for body sensor networks ▪ Based on PRESENT block cipher ▪ 64-bit output range ▪ TuLP-128 is a 128-bit variant that provides higher resistance against internal collisions ▪ Time and resource efficient on hardware-constrained devices
3	LightMAC	▪ Customized for energy-starved networks like Wireless Sensor Networks (WSNs). ▪ Based on lightweight hash function LOCHA. ▪ Security: Resilient to passive and active attacks.

Table 4: Examples of lightweight MACs and their descriptions

© CyberSecurity Malaysia 2017 - All Rights Reserved

Lightweight Stream Ciphers

Stream ciphers are also promising primitives for constrained environments. In 2004, the eSTREAM project was organized by the European Network of Excellence for Cryptology in order to identify new stream ciphers that may be suitable for widespread adoption. In the hardware category and aimed at devices with restricted resources, three ciphers are still part of the eSTREAM portfolio after the latest revision in 2012. The ciphers are Grain v1, MICKEY 2.0 and Trivium. Table 5 provides descriptions of these lightweight stream ciphers.

No	Algorithm	Block size (bits)
1	Grain v1	▪ Uses 80-bit keys, 64-bit IVs ▪ the authors do not explicitly limit the number of keystream bits that should be generated for each key/IV pair ▪ Widely analysed, provides implementation flexibility, and has a version that supports authentication.
2	MICKEY 2.0	▪ Uses 80-bit keys, IVs of variable length up to 80-bits. ▪ the maximum amount of keystream bits for each key/IV pair is 2^{40} ▪ Less analysed than Grain and Trivium, and its security mostly depends on the hardness of analysis.
3	Trivium	▪ uses 80-bit keys, 80-bit IVs ▪ at most 2^{64} keystream bits should be generated for each key/IV pair ▪ Widely analysed, elegant and flexible design; however, it only supports 80-bit keys.

Table 5: Descriptions of Lightweight Stream Ciphers.

NIST-Approved Cryptographic Primitives in Constrained Environments

Currently, there are two NIST-approved block cipher algorithms, namely AES and Triple DES (TDES). For lightweight cryptography purposes, the most suitable variant of the family is AES-128 due to the number of rounds and size of key schedule functions.

NIST-approved hash functions are specified in two FIPS standards: FIPS 180-4 and FIPS 202. FIPS 180-4 specifies SHA-1 and the SHA-2 family (i.e. SHA-224, SHA-256, SHA-384, SHA-512, SHA-512-224 and SHA-512/256) whilst FIPS 202 specifies the permutation-based SHA-3 family (i.e. SHA3-224, SHA3-256, SHA3-384 and SHA3-512). None of these approved hash functions are suitable for use in very constrained environments, mainly due their large internal-state size requirements.

Authenticated encryption provides performance and resource requirement advantages, because it simultaneously offers confidentiality and integrity protection of messages. NIST approves the CCM and GCM block cipher modes that provide authentication and encryption simultaneously. NIST also approves standalone MACs, CMAC, GMAC and HMAC to be used for generating and verifying message authentication.

Lightweight Cryptography Standards

There are three lightweight cryptography standards, namely ISO/IEC 29192 Lightweight Cryptography, ISO/IEC 29167 Automatic Identification and Data Capture Techniques, and Cryptography Research and Evaluation Committee (CRYPTREC).

ISO/IEC 29192 covers the essential symmetric key-based primitives (Block cipher, stream cipher, hash function, and MAC). The standards cover a relatively large range with regards to key size, block size, hash value, etc.

ISO/IEC 29167 Automatic Identification and Data Capture Techniques provides security services for RFID air interface communications. It describes the architecture, security features and requirements of security services for RFIS devices. Currently, seven suites have been published.

Cryptography Research and Evaluation Committee (CRYPTREC) is a project to evaluate and monitor the security of cryptographic techniques used in Japanese e-government systems. CRYPTREC publishes three types of cipher lists: e-Government Recommended Cipher List, Candidate Recommended Cipher List and Monitored Cipher List. The Lightweight

© CyberSecurity Malaysia 2017 - All Rights Reserved

Cryptography working group of CRYPTREC was established in 2013 with the aim to study and support appropriate lightweight cryptography solutions for e-government systems and any applications that necessitate lightweight solutions.

References

1. DRAFT NISTIR 8114 Report on Lightweight Cryptography

2. http://mathsci.ucd.ie/~gmg/ECC2007Talks/poschmann_LWC.pdf

3. X. Fan, K. Mandal and G. Gong. 2012. A Lightweight Stream Cipher for Resource-Constrained Smart Devices. CACR 2012-28 Technical Report.

4. https://www.cryptolux.org/index.php/Lightweight_Hash_Functions

5. https://en.wikipedia.org/wiki/SHA-3

6. N. Mouha, B. Mennink, A. V. Herrewege, D. Watanabe, B. Preneel and I. Verbauwhede. Chaskey: a Lightweight MAC Algorithm for Microcontrollers. http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session1-mouha-paper.pdf

7. A. R. Chowdhury and S. DasBit. LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network. http://itra.medialabasia.in/data/Documents/DISARM/publications/15.pdf

© CyberSecurity Malaysia 2017 - All Rights Reserved

Ransomware WannaCry Attack! Are you at risk?

By | Nur Shazwani binti Mohd Zakaria

Ransomware WannaCry attack is the latest cyber threat and the largest in the history of the Internet after the DYN DDoS attack on October 21, 2016. For a ransomware attack was announced Cyber Security Expert on May 12, 2017 ago, this ransomware attack is widely spread in several countries, such as Russia, Ukraine, and Taiwan. This malware also spread to other countries, including Malaysia and the list of countries affected by these attacks is growing to this day. As of now, the virus has infected more than 200,000 organizations in 150 countries.

What Is Ramsomware Wannacry?

Ransomware WannaCry is basically a malware that restricts users from accessing specific files and documents. It then asks the user to pay ransom money using bitcoins before the virus is withdrawn from the user's device. WannaCry generates a unique Bitcoin wallet address for each infected computer, but due to a rare condition bug, this code does not execute correctly. WannaCry then defaults to three hardcoded Bitcoin addresses for payment. The attackers are unable to identify which victims have paid using the hardcoded addresses, meaning that victims are unlikely to get their files decrypted.

Figure 1: Computer infected by ransomware WannaCry

```
<64-bit SIGNATURE>          - WANACRY!
<length of encrypted key> - 256 for 2048-bit keys, cannot
exceed 4096-bits
<encrypted key>             - 256 bytes if keys are 2048-bits
<32-bit value>              - unknown
<64 bit file size>          - return by GetFileSizeEx
<encrypted data>            - with custom AES-128 in CBC mode
```

Figure 2: Encryption format used

So far, this malware focuses on older Windows versions, which are not protected by any latest security. According to another report, the smartphone has not been infected, but please take precautions because it can be more active in future.

How Does Ransomware Wannacry Function?

Ransomware WannaCry spreads itself across an organization's networks by exploiting a vulnerability, which is the initial means of infection. It has the ability to spread itself within corporate networks without user interaction by exploiting known vulnerabilities in Microsoft Windows. Computers that do not have the latest Windows security updates applied are at risk of infection. The figure below describes how it works.

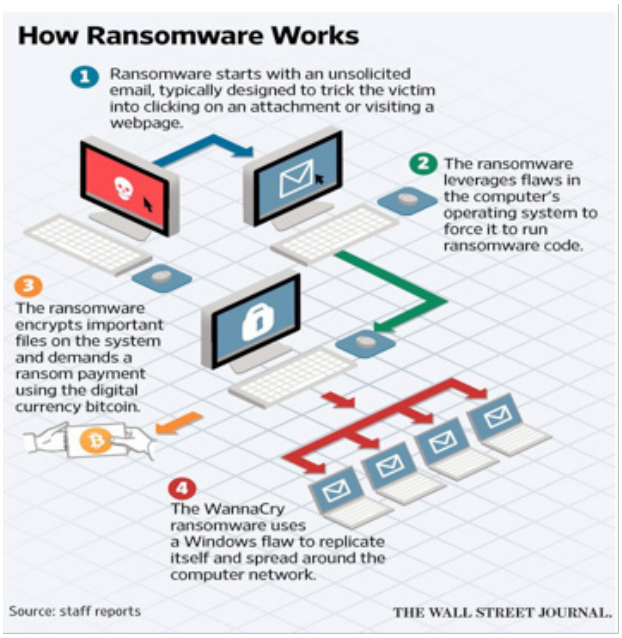


Figure 3: How ransomware WannaCry attacks your PC

© CyberSecurity Malaysia 2017 - All Rights Reserved

Can The Victim Recover The Encrypted Files Or Should They Pay The Ransomware Wannacry?

It is possible for files to be decrypted but not in most cases. Usually, if the victim pays the ransom money, it is not guaranteed the file will be decrypted again. So it is not recommended to pay the ransom money. However, the user can recover the file if the file has its own backup.

How To Protect Your Data From Ransomware

1. Please do not access any suspicious websites
   - Think before you click. Avoid websites that provide pirated material.
2. Do not click on any links from untrusted email senders
   - Do not open an email attachment from somebody or a company you do not know. Always hover over a link before you click to see where the link is really taking you.
3. Avoid downloading any data through the Internet
   - If you have to download a file from a suspicious website, an email, an FTP site or any file sharing service, please scan it before you run it.
4. Regularly do a backup to prevent data loss
   - The best thing you can do is to back up all your files. Ideally, you should have your files in at least three places: where you work on them, on a separate storage device and off-site. Keep your files on your computer, back them up to an external hard drive, and then back them up in a different location. You can use a backup service or simply get two external hard drives and keep one at work and one at home. It is more recommended to back up data using cloud services.
5. Please avoid using any OPEN Wifi.
   - When you are at the local coffee shop, library and especially the airport, please do not use the 'free' open (non-password, non-encrypted) Wifi.
6. Please install a trusted antivirus to secure your data and always update the patches.
   - Viruses and malware are created all the time. Please install a trusted antivirus and keep you antivirus software updated.
7. Regularly run the scheduled scan of your antivirus software
   - This may seem crazy, but many of us forget to do this. Kindly set up your software of choice to run at regular intervals. Once a week is preferred, but do not wait much longer between scans. Maybe it is difficult to work on your computer while your antivirus software is running. One solution is to run the software at night when you are not using your computer. Set your antivirus software to run on a specific night and always leave your computer running that day. Make sure it does not shut off automatically or go into hibernation mode.
8. Regularly update your operating system with the latest patches.
   - Whether you are using Windows, Mac OSX, Linux or any other OS, please keep it updated. OS developers are always issuing security patches that fix and plug security leaks. These patches will help to keep your system secure.
9. Use strong passwords to avoid brute force or any social engineering attacks.
   - Never use the same password especially for your bank account. Typically, the same email address or username is used for all accounts to remember passwords easily. These are easy to identify and steal. Your password must have lower case letters, upper case letters, numbers and symbols. Keep it easy to remember but difficult to guess.
10. Secure your network
    - Use WPA or WPA2 encryption. WEP is no longer strong enough as it can be bypassed in minutes by experts.

In conclusion, this ransomware does not stop here, it might attack again in future. Please keep in mind protecting your data regularly by following the above steps. PREVENTION IS BETTER THAN CURE!

© CyberSecurity Malaysia 2017 - All Rights Reserved

Mobile Security: Android OS vs iOS

By | Nur Fazila binti Selamat, Mohd Nor Akashah bin Mohd Kamal, Nurul 'Ain binti Zakariah

Abstract - At present, having a mobile device, especially a small mobile device such as a smartphone has become a necessity for everyone. Due to their small size, memory capability and ease of downloading or removing information, mobile devices pose a risk to an organization or person, particularly the risk of data leakage. Besides, with current technologies and increasing numbers of black-hat hackers, people and especially organizations must take extra precautions and be aware of current issues regarding mobile security. This article highlights mobile device protection, mainly for popular mobile operating systems (OS) Android OS and iOS. This article also provides an in-depth explanation of Android OS and iOS, statistics on Android OS and iOS, current issues with both OSs and how to mitigate and protect smartphones with both Android OS and iOS.

Keywords: mobile security, smartphone security, iOS, Android OS, mobile operating system.

Introduction

In this current Information Technology era, mobile devices like mobile phones, smartphones and tablets have become essential gadgets for everyone including organizations. However, without extra precautions and awareness of mobile security, personal or organizational data can be leaked and exposed easily, causing many unwanted consequences. Reflecting on the issue of data leakage, knowledge and awareness of mobile security are crucial for protecting data from being stolen and leaked. Mobile security, also known as wireless security, is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing [1]. The two most common smartphone operating systems (OS) are Android and iOS.

What is Android OS?

The Android operating system was developed by Google Inc. It provides an open-source platform and application environment for mobile devices [2]. Android runs on a wide range of devices from smartphones and tablets to set-top boxes [3].

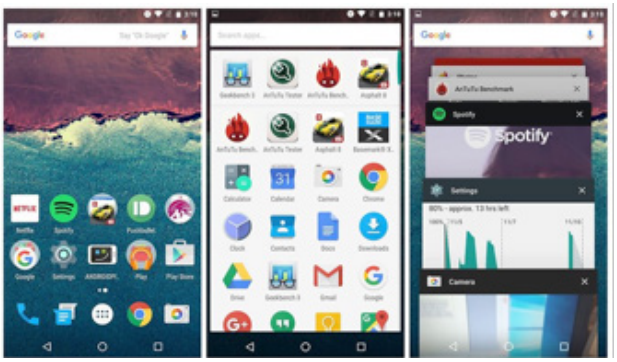


Fig. 1: Android OS user interface on smartphone.

Security Features

In terms of security, Android has built several security factors to ensure the device is well-protected, including [2][4]:

1. Automatic security: Android devices come with built-in software called "Verify Apps," which regularly checks to ensure all applications are running well on the device. If a harmful application is detected, "Verify Apps" will display an alert or block the application entirely.
2. Simplified security with Fingerprint API lets users unlock the device, securely sign in to applications, and check out on Android Pay and the Play Store, all with the tap of a finger.
3. Android updates: The Android update service delivers new capabilities and the latest security updates to selected Android devices, including updates through the web or over the air (OTA).
4. Android Device Manager: An integrated web application and Android application to locate lost or stolen devices.
5. SafetyNet: A privacy preserving intrusion detection system to assist Google tracking, mitigate known security threats and identify new security threats.
6. Application services: Frameworks that allow Android applications to use cloud

© CyberSecurity Malaysia 2017 - All Rights Reserved

capabilities, such as backing up application data and settings, and cloud-to-device messaging (C2DM) for push messaging.

In addition, Google provides a set of cloud-based services that are available to compatible Android devices with Google Mobile Services [2].

History of Android Versions

The Android mobile operating system began with the release of the Android beta in November 2007. The first commercial version, Android 1.0 (Alpha) was released in September 2008 [5]. Each major release is named in alphabetical order after a dessert or sugary treat.

Fig. 2: All Android versions.

Figure 2 shows the major Android releases in alphabetical order. The latest Android version is Nougat, which was released on August 22, 2016.

Code Name	Version No.	Initial Release Date
Alpha	1.0	September 23, 2008
Beta	1.1	February 9, 2009
Cupcake	1.5	April 27, 2009
Donut	1.6	September 15, 2009
Eclair	2.0-2.1	October 26, 2009
Froyo	2.2-2.2.3	May 20, 2010
Gingerbread	2.3-2.3.7	December 6, 2010
Honeycomb	3.0-3.2.6	February 22, 2011
Ice Cream Sandwich	4.0-4.0.4	October 18, 2011
Jelly Bean	4.1-4.3.1	July 9, 2012
KitKat	4.4-4.4.4	October 31, 2013
Lollipop	5.0-5.1.1	November 12, 2014
Marshmallow	6.0-6.0.1	October 5, 2015
Nougat	7.0-7.1.2	August 22, 2016

Table 1: Details of Android versions [6].

Table 1 presents details of the Android versions with the initial release on September 23, 2008, which was Android Alpha.

New Features of Android 7.1.2

For the latest version of Android 7.1.2 (Nougat) which was released on January 31, 2017, Google has improved several features [7][8]:

- Improved fingerprint scanner gestures – Users can drag down the notifications shade with a rear-mounted finger scanner. The user must enable this feature in the Moves section of the Settings menu, as this feature is not enabled by default. Google is also introducing the gestures to Nexus 5X and 6P smartphone owners.
- New multitasking view – This new multitasking view shows up to eight (8) cards in a grid-like view that is better suited for the tablet's display.
- Bluetooth Connectivity – Google has fixed the problem with Bluetooth connectivity randomly shutting down on users' devices.
- Updated boot screen – Shows the "Powered by Android" tagline on the boot splash screen.

What is iOS?

iOS (formerly known as iPhone OS) is a mobile operating system created and developed by Apple Inc. iOS runs on Apple devices such as iPhones and iPads. Basically, it is the main software that allows users to communicate using Apple phones or tablets.

Fig. 3: iOS user interface on iPhone.

iOS only allows users to install and run applications downloaded from the Apple App Store. Similar to Android OS, iOS offers notifications for any major or minor updates

© CyberSecurity Malaysia 2017 - All Rights Reserved

including operating system updates. Users can also check the iOS update manually by heading to Settings, and then "General," followed by "Software Update."

Security Features

Similar to Android, Apple also has their own security strategies to ensure both user and device are well-protected. Below are several security features provided by Apple for iPhone users [9]:

1. System Security: System security is designed to ensure both hardware and software are secure across all components of every iOS device, including boot-up process, software updates and Secure Enclave. The closed integration of hardware and software on iOS devices ensures that each system component is trusted, thus validating the system as a whole.
2. Encryption and data protection: Designed to protect user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it. Apple also provides a method of instant and complete remote wipe in case the device is stolen or lost. Users can automatically enable data protection by setting up a device passcode.
3. Application security: A system that enables apps to run securely and without compromising platform integrity.
4. Network security: Industry-standard networking protocols provide secure authentication and encryption of data in transmission. iOS uses and provides developer access to standard networking protocols for authenticated, authorized and encrypted communications. Both Wi-Fi and cellular data network connections have been integrated with proven technologies and the latest standards. iOS also supports Single Sign-On (SSO) features.
5. Apple Pay: Apple also provides features for secure payment. Users can use supported iOS devices and Apple Watch to pay in an easy, secure and private way in stores, apps and on the web in Safari.
6. Internet services: Set of services to help users get even more utility and productivity out of their devices including iMessage, FaceTime, Siri, Spotlight, Suggestions, iCloud, iCloud Backup and iCloud Keychain.
7. Device controls: Methods that allow iOS device management to prevent unauthorized users by enabling passcode protection and remote wipe if a device is lost or stolen.
8. Privacy controls: Capability of iOS to control access to Location Services and user data.

History of iOS Versions

In contrast to Android, Apple uses numerical order for iOS version sequence. Every year, Apple releases new updates with major feature improvements and bug fixes. The table below presents some information regarding the iOS versions:

iOS Version	Initial Release Date	End of Support (Year)
iPhone OS 1-1.1.2	March 6, 2008	2010
iPhone OS 2-2.2.1	July 11,2008	2011
iOS 3-3.2	June 17, 2009	2012
iOS 4-4.3.5	June 21, 2010	2013
iOS 5-5.1.1	October 12, 2011	2014
iOS 6-6.1.5	September 19, 2012	2015
iOS 7-7.1	September 18, 2013	-
iOS 8-8.4.1	September 17, 2014	-
iOS 9-9.3	September 16, 2015	-
iOS 10-10.3.2	September 13, 2016	-

Table 2: Details of iOS versions [10].

Security Concerns & Mitigation Strategies for Mobile Devices

The majority of attacks on mobile devices in 2015 focused on human exploitation, as found by the Proofpoint Human Factor Report [12]. Below are some of the best practices for ensuring data security on your mobile device.

1. Password Protection

It is highly recommended to protect your device with a password or personal identification number (PIN) and to enable the screen's auto-lock function. Avoid weak passwords and screen lock patterns that can be easily hacked.

© CyberSecurity Malaysia 2017 - All Rights Reserved

2. Not using Public Wi-Fi

Public Wi-Fi networks may be free but they are also a major security risk. Information sent over public Wi-Fi networks is visible to anyone on the network [13]. Do not transmit any sensitive or personal information such as online banking over public Wi-Fi. Use the secure transmission option like Virtual Private Network (VPN) or use your mobile data network.

3. Use Antivirus Software

Mobile antivirus software protects your device by detecting and stopping existing and emerging threats from malware, viruses and hackers. Many people do not realize that a smartphone is actually a computer and is still prone to the same risks as a computer. By installing an antivirus on your smartphone, you could also avoid transferring a virus to your computer via USB, which is a common problem these days.

4. Install Updates

Keep the mobile operating system and its applications up to date by promptly installing updates as soon as they become available. Installing updates or patches improves functionality, fixes security holes and ensures optimal protection for your device.

5. Install Trusted Apps

Many people unconsciously download and install apps that come with malware or spyware, which can potentially harm the device, steal data, or even infect the desktop computer whenever connected via USB. Do ensure to download from trusted sources by doing research or studying the publisher, app ratings and application security features before downloading.

6. Switch Off Connectivity

Limit the potential for unauthorized access to your device through Wi-Fi, location services or Bluetooth by disabling these connectivity options when not required.

7. Do not Clicking on Unverified or Suspicious URL Links

Ransomware is the newest threat to mobile devices. This malware locks a device until a sum of money is paid to the hacker so the victim can regain personal access to their smart phone. Make sure to run backup software automatically and regularly [14]. This is to ensure all data are secure and can be retrieved in the event of data loss or theft. Never click on links received via SMS or instant messaging applications from people you do not know. This can also prevent malware threats, phishing scams and virus schemes.

8. Unnecessary Information

You can minimize the risk of losing important data by deleting information that is no longer required on your device. You may also backup all unnecessary data to another external devices such as an external hard disk as a secondary device. Such data can include personal data, like photos, videos, addresses and health information. By having less data on your primary device, the risk of losing personal and important data can be reduced.

Statistics of Mobile OS Fragmentation

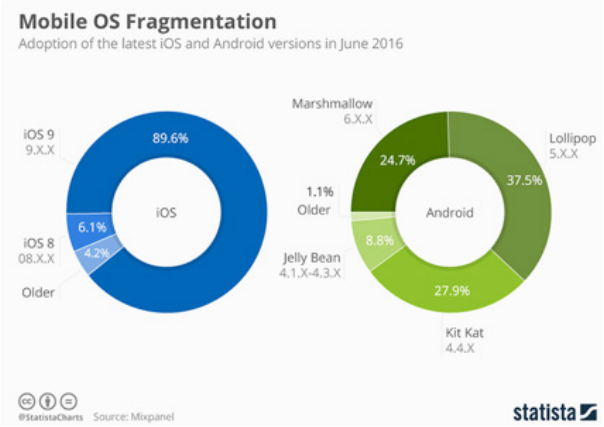


Fig. 3: Mobile OS fragmentation for iOS and Android

According to statistics from statisca.com [11], nearly 70% of all Android devices in use are still running older versions of Android, which opens users to security risks. Moreover, 89.6% of iOS devices are up to date with the latest iOS updates for optimal device protection.

Most Android devices do not receive the latest updates even though Google releases new Android versions with new features and performance improvements. This is because Android has so many different devices from so many different smartphone manufacturers, making their ecosystem hard to control.

On the other hand, Apple devices are produced by the same manufacturer, which makes their devices 89.6% up to date and easier to manage. To ensure that devices are using the latest

© CyberSecurity Malaysia 2017 - All Rights Reserved

mobile operating system, manufacturers are responsible for making sure their devices are up to date to function with the latest mobile operating system version in order to deliver regular updates to their customers.

Conclusions

Cybercriminals are aware there are large numbers of unpatched or unsecured mobile devices roaming the cyber world waiting to be prey. This is due to the general public's ignorance or lack of awareness of the importance of mobile security while operating their smartphones, laptops and tablet devices.

As the proverb goes, prevention is better than cure. This article showed how important it is for users to have a good understanding or essential basic knowledge of mobile security to prevent their devices or data from being stolen or lost. Users must be aware of any updates released for their device(s), such as enabling the device's passcode and only installing apps from trusted sources/developers.

Besides users, mobile device manufacturers should also be responsible for ensuring that all their customers' devices are up-to-date and able to install the latest mobile operating system version with security updates.

In conclusion, both mobile manufacturers and users play an important role in securing data and the mobile devices itself. In addition, awareness and knowledge of current issues, especially mobile threats and security, are very important for both mobile manufacturers and users.

References

1. What is mobile security (wireless security)? - Definition from WhatIs.com. (n.d.). Retrieved May 29, 2017, from http://whatis.techtarget.com/definition/mobile-security

2. Security | Android Open Source Project. (2017). Retrieved May 29, 2017, from https://source.android.com/security/

3. Android Security: Guide to Application Security | Veracode. (n.d.). Retrieved May 29, 2017, from https://www.veracode.com/security/android-security

4. Security Center - Overview. (n.d.). Retrieved May 29, 2017, from https://www.android.com/security-center/

5. A Complete History of the Android Operating System | TechCity. (n.d.). Retrieved May 29, 2017, from https://www.techcityng.com/history-of-the-android-operating-system/

6. The history of Android OS (Infographic). (n.d.). Retrieved May 29, 2017, from https://www.techinasia.com/talk/the-history-of-google-android-operating-system

7. Carlon, K. (2017). Android Nougat review: what's new in Android 7.1.2? | AndroidAuthority. Retrieved May 30, 2017, from http://www.androidauthority.com/android-7-0-features-673002/

8. Pandey, R. (2017). What's New in Android 7.1.2. Retrieved May 30, 2017, from http://www.androidbeat.com/2017/04/whats-new-in-android-7-1-2/

9. Apple Inc. (2017). iOS Security iOS 10. Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

10. Costello, S. (2017). iOS History and Details About Each Version. Retrieved May 30, 2017, from https://www.lifewire.com/history-of-the-ios-2000224

11. The Difference Between Android and iOS. Retrieved June 9, 2017, from https://www.statista.com/chart/5118/mobile-os-fragmentation/

12. Mobile Security: Best Practices For Minimizing Exposures. Retrieved June 9, 2017, from http://www.lasorsa.com/2016/02/26/mobile-security-best-practices-for-minimizing-exposures/

13. Ten Common Smartphone Mistakes That Expose You To Security Risks. Retrieved June 9, 2017, from http://www.makeuseof.com/tag/ten-common-smartphone-mistakes-that-expose-you-to-security-risks/

14. 9 Mobile Device Security Mistakes You Can Easily Avoid. Retrieved June 9, 2017, from http://www.rasmussen.edu/degrees/technology/blog/mobile-device-security-mistakes/

© CyberSecurity Malaysia 2017 - All Rights Reserved

CyberSecurity Malaysia New Building at Cyberjaya

By | Syahran bin Abdul Halim

In 2007, CyberSecurity Malaysia acquired a piece of land at the heart of Cyberjaya. Since then, we have been looking forward to our own building to accommodate all operations under one roof. We are now expecting to move into the new building by April 2019.

The complex is being built on a 4.9-acre site, sloping from east to west and bounded by only one road, Jalan Impact. The building will be located in the west corner of the site, furthest from the main road for several reasons, including security and aesthetics. It is a prominent location with a view of most of Cyberjaya, which is located in the valley below. The design of the complex benefits from existing topography by providing the main access to the complex in the middle of the site. This will offer the most dramatic entrance to the complex with the Cyberjaya skyline as the background.

The complex has been under construction since April 2016. It will consist of 2 towers, shared facilities, and exhibition and innovation centres. It is designed to reflect a progressive and dynamic organization moving toward the future. The design creates a workspace that stimulates creativity and promotes the well-being of users. The entire complex will have the capacity to accommodate a maximum of 500 occupants. The building will also house a dedicated server farm, various research and operational laboratories and the Security Operation Centre for MyCERT, all with the highest security levels. Entry to the tower building will necessitate passing through several security layers, including electronic detectors and biometric access to each floor.

Figure 1: Complex illustration by the designer

This complex will symbolize CyberSecurity Malaysia leading the cyber security industry into the future and will be the national cyber security hub. The CyberSecurity Malaysia gallery will showcase our services and expertise to the public.

Besides CyberSecurity Malaysia, other agencies residing within the complex will be Standard Malaysia, MyNIC and MKN. The innovation centre will also have space for the cyber security and information technology industry companies to set up research laboratories or offices.

A common centre with shared facilities will be located centrally within the complex for easy access for occupants and visitors. This centre will contain the main reception area, a multipurpose hall, training rooms, a cafeteria, a surau and a gymnasium. All complex occupants can use these facilities, as the concept is to create a healthy environment for all to work and play.

© CyberSecurity Malaysia 2017 - All Rights Reserved

Certificate vs Certification

By | Razana Md binti Salleh, Adlil Ammal bin Mohd Kharul Apendi, Marinah Syazwani binti Mokhtar, Nurul Husna binti Khasim, Hasnida binti Zainuddin

References

1. *ASTM E2659 – 17 Standard Practice for Certificate Programs (http://webstore.ansi.org/RecordDetail.aspx?sku=ASTM%20E2659-17)*

2. *ICE 1100 : 2010(E) - Standard for Assessment Based Certificate Programs (http://www.strategiclearningalliance.org/documents/ICE-1100-Accreditation-Standards-January2010.pdf)*

3. *ANSI/IACET 1-2013 Standard for Continuing Education and Training (https://www.iacet.org/standards/ansi-iacet-2013-1-standard-for-ce-t/)*

Designed by Canva: https://www.canva.com

© CyberSecurity Malaysia 2017 - All Rights Reserved

Cyber Security Terms That We Should Alert

By | Yuzida binti Md Yazid & Nur Athirah binti Abdullah

Authors : Nur Athirah Abdullah; Yuzida Md Yazid

CYBERSECURITY

TERMS TO KNOW!

Cybersecurity terms can sometimes be confusing or easily misunderstood at times. With high-profile cyber-attacks making news worldwide, it is important to stay updated on a number of cybersecurity terms. Here is a list of 10 terms for you!

ADWARE
An annoying form of malware that bombards you with ads when you go online, or use certain programs on your device.

CHARGEBACK
A card payment transaction, whereby the supplier initially receives payment but the transaction is later rejected by the cardholder or card-issuing company. The supplier's account is then debited the disputed amount.

DARK WEB
A part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

DATA BREACH
The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

DRIVE-BY DOWNLOAD
A malware most often installed accidentally. It happens when cyber crooks hide malicious software in ads or links to advantage of weaknesses in your device or web browser.

PATCH
A software update designed to fix bugs and repair vulnerabilities discovered by the software developer.

ZERO-DAY EXPLOIT
A hole in software that is unknown to the vendor. Such security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it. This exploit is called a zero-day attack.

ZOMBIE
A computer connected to the Internet that has been secretly compromised by malicious logic to perform activities under remote command and control.

SPIM
Spim is basically spam delivered through instant messaging (IM) instead of e-mail. Although less ubiquitous than its e-mail counterpart, spim is reaching more users all the time.

PHARMING
Pharming is when cyber crooks design fake websites or pages that look exactly like their legitimate counterparts, all with the intention of tricking people into entering private login information.

© CyberSecurity Malaysia 2017 - All Rights Reserved

Corporate Office:
CyberSecurity Malaysia
Level 5, Sapura@Mines
No. 7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel: +603 8992 6888
Fax: +603 8992 6841
Email: info@cybersecurity.my
Customer Service Hotline: 1300 88 2999
www.cybersecurity.my

©CyberSecurity Malaysia 2017-All Rights Reserved

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013 CERT. NO. : AR 4656

MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)

Status Company

Best Child Online Protection Website