CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 40 - (1/2016)

Understanding and Defending Against Mobile Botnets: A Case Study

Social Engineering Experiment via Social Media

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

Bruce Schneier, Secrets and Lies

ISSN 1985-1995
9 771985 199003

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

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

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,

Thank you for your continuous patronage of CyberSecurity Malaysia's e-Security Bulletin!

Because of you, we feel motivated to write more interesting articles.

For this 40th edition of e-Security Bulletin, we have compiled 20 articles for you — mostly technical articles that are eagerly sought after by researchers, practitioners and observers alike. Personally, I do make sure I read them all, in order to update and enhance my understanding of the current cyber security scenario in Malaysia. If you cannot read all of the articles, I highly recommend you to at least read the 'Social Engineering Experiment via Social Media', as well as 'The Case Study for Understanding and Defending Against Mobile Botnets'.

Till we meet again in the next edition of e-Security Bulletin; be smart and be safe!

Dr. Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

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

Understanding and Defending Against Mobile Botnets: A Case Study

By | Sharifah Roziah Mohd Kassim

Introduction

It is no exaggeration to say that mobile devices have become part of daily life and have been emerging tremendously over the past years. They are now handy devices for multiple usage, such as communication, sending SMS messages, socializing, chatting, reading emails, online banking and catching up on early morning news. Mobile devices actually offer a better attack avenue than non-mobile devices because users almost always carry them around, providing greater probability for stealing confidential information, credentials or even pictures. As for non-mobile devices, the probability of attack is lower because they depend upon the device's uptime and user's availability with the device.

Overview of Mobile Botnets

So what is a mobile botnet? It is just like a computer botnet, which is a piece of malicious code that targets and infects mobile devices such as smartphones in order to gain complete ownership of them. Infection can happen by various means and regardless of the smartphone platform. Once infected, the device will establish communication with a Command & Control (C&C) server that is controlled remotely by an attacker known as a botmaster. The C&C servers are normally geographically dispersed around the world to ensure the longevity of activities and to evade tracing by Legal Enforcement Agencies.

Just like computer botnets, mobile botnets take advantage of vulnerable mobile devices to compromise and gain full control of them, enabling the botnets to make phone calls, send SMS messages, and access confidential data, contacts and pictures that may be stored in the mobile device. Besides, for the botnet to be more widespread and maximize its impact, it will propagate by sending a copy of itself to other vulnerable devices through SMS messages and emails.

Examples

Mobile botnet infections can be traced back to as early as 2011. Two such examples are DroidDream and Gemini botnets. They are trojan game apps with bot-like capabilities that compromise Android devices. These were followed in November 2014 by the discovery of NotCompatible.C malware. This was considered the most advanced mobile botnet targeting Android-based devices including smartphones. Botnets are capable of gaining unauthorised access to secure enterprise networks.

In late 2014, WireLurker malware was discovered, which targeted Apple iPhones and iPads. Mobile botnets infect Apple devices through installing pirated versions of popular Mac applications. A botnet has the capabilities to download and install enterprise-signed apps to vulnerable devices without the user's knowledge.

In March 2014, a variant of the Zorenium Bot was found targeting and infecting IOS device operating systems, which had previously included Windows and Linux. Upon infection, it can bypass anti-virus software detection and allows attackers to use the mobile phones as agents to conduct DDOS attacks and other notorious activities. Apart from the above examples are CommWarrior and Sexy Space.

Methods of Infection

There are several ways in which mobile botnets can infect smartphones and they are quite similar to the methods used to infect computers.

1. A popular and traditional method of how a botnet can infect and spread is when a user clicks on an attachment or malicious URL that contains the botnet, normally bundled in emails.
2. Besides email, attachments or malicious URLs may attach to unsuspecting SMS messages.
3. A botnet also spreads through unsuspected illegitimate applications and when unknowingly browsing malicious websites.

Case Study

MyCERT received an incident from a foreign Computer Emergency Response Team (CERT) regarding the discovery of a Command & Control (C&C) server that stores thousands of mobile

phone numbers stolen from the contact lists of infected smartphones. The botnets residing in the mobile devices seemed to have established communication with a remote C&C server and delivered the stolen data including the mobile phone numbers to the server. This information could be retrieved by the attackers who control the C&C server.

In this case study, it was found that mobile botnets spread through SMS messages that target Android smartphones only. Other platforms were not affected. Users who clicked on a link in an SMS message they received inadvertently installed a malicious Android Package (APK) that took control of their smartphones.

In this case study, we found the infected smartphones can be hijacked remotely and potentially used for various fraudulent activities, such as buying digital goods and services without the smartphone owners knowing it. The infected smartphones become launching pads to further propagate the malware to other smartphones by sending SMS messages with links to the malicious APK.

Implications of mobile botnets on smartphones can be huge and serious if immediate action is not taken to mitigate the infection. The impacts can be as follows:

a. Cybercriminals or botnet herders direct the infected smartphones to buy digital goods from micropayment providers in Malaysia.

b. The botnet will send SMS messages to other smartphone users, which were extracted from the infected smartphone's address book, containing a malicious APK in order to propagate further.

c. Confidential information like contact numbers extracted from the infected smartphones' address books are stolen and the perpetrators can use them for malicious activities.

d. The botnet will establish a connection and make call-backs to a Command & Control (C&C) server controlled by the attackers.

Below is a diagram illustrating how a mobile botnet works.

Diagram 1: How a Mobile Botnet Works

Defend Your Mobile Devices

As best practices to safeguard smartphones, users are advised to:

a. Set a password for your smart phone. All major smartphone operating systems allow you to set a password and automatically lock your phone after a period of inactivity.

b. Verify an app's permission and the app's author or publisher before installing it.

c. Do not click on adware or suspicious URLs sent through SMS/messaging services. Malicious programs could be attached to collect users' information.

d. Always run a reputable anti-virus on your smartphone/mobile device, and keep it up to date regularly.

e. Switch off Bluetooth if it is not in use. This way, your phone will be less vulnerable to attacks.

Conclusion

Mobile devices, particularly smartphones, have become essential in our everyday life and the majority of us own at least one smartphone. However, it is the responsibility of each smartphone owner to ensure full protection is enabled for the device to prevent exploitation and botnet infections. Smartphones are now gaining popularity among attackers as a form of easy prey. As such, safeguarding devices must be given utmost priority to prevent unwanted incidents.

Reference:

1. http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-botnets.aspx

2. http://www.webopedia.com/TERM/M/mobile_botnet.html

3. https://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/1011/index.html

4. http://www.darkreading.com/cloud/the-rise-of-the-resilient-mobile-botnet/d/d-id/1317593

5. http://www.cybertrend.com/article/16969/mobile-botnets

Addressing the Threat of Cyber Terrorism

By | Mohd Shamil bin Mohd Yusoff & Norhafizah Hashim

What is Cyber Terrorism?

Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and information stored therein done to intimidate or coerce a government or its people in furtherance of political or social objectives [1] [2]. Furthermore, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic losses are such examples. Serious attacks against critical infrastructures may be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not be considered cyber terrorism.

Cyber Terrorism Attacks in Malaysia

Cyberspace is a virtual place that has become as important as physical space for social, economic, and political activities. Many countries around the world are increasingly dependent on cyberspace when using Information and Communication Technology (ICT) [3] [4]. This dependency renders these countries in an insecure position because cyberspace is borderless and vulnerable to cyberattacks. Individuals have the ability and capability to cause damage to a nation through cyberspace. Cyberattacks are also attractive because they are cheap in relation to the costs of developing, maintaining and using advanced and sophisticated tools. Many have declared that cyberspace is the fifth domain along with land, air, sea and space, and it is crucial to battlefield success.

In general, to understand cyber terrorism, it can be broken down into at least five elements that construe cyber terrorism [5] [6]:

i. Politically-motivated cyberattacks that lead to death or bodily injury;

ii. Cyberattacks that cause fear and/or physical harm through cyberattack techniques;

iii. Serious attacks against critical information infrastructures, such as finance, energy, transportation and government operations;

iv. Attacks that disrupt non-essential services are not considered cyber terrorism;

v. Attacks that are not primarily focused on monetary gain.

Malaysia has not experienced any serious cyberattacks, but several cyberattacks have affected the country including an attack in 2011 by a group calling themselves “Anonymous” [7].

Preventive Measures Taken by the Government

In Malaysia, the Government has taken initiatives to mitigate and combat cyberattacks. One of the initiatives is the development of the National Cyber Security Policy (NCSP), which was endorsed by the Government in May 2006 [8] [9]. NCSP consists of eight (8) policy thrusts: Effective Governance, Legislative and Regulatory Framework, Cyber Security Technology Framework, Culture of Security and Capacity Building, Research and Development towards Self Reliance, Compliance and Enforcement, Cyber Security Emergency Readiness and International Cooperation.

The NCSP was formulated to address threats and risks to the Critical National Information Infrastructure (CNII) and to develop action plans to mitigate such risks. CNII consists of assets (real and virtual), systems and functions that are vital to the nation, and whose exploitation, damage or destruction would have a devastating impact on national economic strength, image, defence and security, government capabilities to function efficiently and public health and safety. The NCSP is particularly focusing on protecting CNII against cyber threats [10] [11].

Alongside clear and effective governance, NCSP provides mechanisms for improving trust and cooperation among the public and private sectors. NCSP also focuses on enhancing skills and capacity building as well as advancing research and development initiatives towards self-reliance. It also maps out emergency readiness initiatives and dictates a programme of compliance and assurance across the entire

CNII. The NCSP also reaches out to Malaysia's international partners and allies. The policy describes ways in which Malaysia can share knowledge with the region and the world on cyber security-related matters. Malaysia developed NCSP as a proactive step in protecting critical sectors against cyber threats.

Other actions taken against cyberattacks are:

i. A layered approach for defence mechanisms
By having combinations of email filtering, installations of anti-virus software, pro-active malware protection, security policies and keeping protection software, operating systems and applications up to date can help tackle security-related concerns such as spam and malware attacks.

ii. Awareness
Internet users and organizations should constantly be offered cyber security awareness of current security threats and how to protect against threats via best practices and safeguarding their systems/networks from attacks.

How serious is Cyber Terrorism?

Cyber terrorism is real and extant. It is considered an attractive option for modern terrorists who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. It includes warfare attacks against a nation's state and forcing ICT infrastructure (including the critical national infrastructure) and assets to fail or get destroyed. Not only are cyber criminals not slowing down, but they keep upgrading and innovating ways of hacking into systems, stealing identities and data, hijacking computers and much more.

Ways forward to mitigate cyberattacks and terrorism include:

i. Strengthening domestic cyber security through inter-agency cooperation and Public-Private Partnership;

ii. Global collaboration and strategic alliances to strengthen regional cyber security in addressing cross-border cyberattacks and cybercrimes;

iii. Adopting more innovative, aggressive and proactive approaches in order to stay ahead of cyber threats - with both defensive and offensive capabilities;

iv. Enhancing the People-Process-Technology triad.

The Roles of CyberSecurity Malaysia in Combating Cyber Terrorism

CyberSecurity Malaysia is structured to be able to mitigate cyberattacks and cyber threats. One of the major characteristics of such threats is their cross-border nature, whereby Internet crimes do not conform to a nation's physical boundaries. On account of this, CyberSecurity Malaysia rigorously pursues international relations by establishing collaborative efforts with foreign government agencies and international organizations through bilateral and multilateral engagements. CyberSecurity Malaysia is also heavily involved in the establishment of cyber security multilateral engagement platforms, such as the Asia Pacific CERT (APCERT) and the Organization of Islamic Cooperation-CERT (OIC-CERT). These platforms see to the collaboration of similar organizations in mitigating international cyber threats.

In addition, other departments including Digital Forensics, the Malaysia Computer Emergency Response Team (MyCERT) and Security Assurance have specific arrangements with their counterparts overseas. Since 2001, CyberSecurity Malaysia has been actively participating in various cyber security events locally, regionally and internationally. All conferences, seminars and workshops have been of great benefit not only to the target audiences (who attended the event) but also to the country.

CyberSecurity Malaysia also organises its own yearly event in Kuala Lumpur, known as Cyber Security Malaysia – Awards, Conference and Exhibition (CSM-ACE). CSM-ACE stands out as the biggest and most talked-about public-private-community partnership event in Malaysia. We provide assistance in terms of detection, containment, analysis, eradication and recovery of incidents during a national cyber crisis. We also produce Security Advisory/Alerts during national cyber crises.

An awareness program known as CyberSAFE - Cyber Security Awareness for Everyone is CyberSecurity Malaysia's initiative to educate and enhance the general public's awareness of technological and social issues facing Internet

users, particularly the dangers of being online. CyberSAFE in Schools is a program in cooperation with Malaysia's Ministry of Education (MOE) aimed to reach out to young generations in schools, which comprise the major portion of Internet users in the country and are the most vulnerable group.

References:

[1] R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," Int. J. Comput. Sci. Inf. Secur., vol. 10, no. 2, pp. 149–158, 2012.

[2] Z. Yunos, "Putting Cyber Terrorism into Context," Published in the STAR In-Tech, p. IT11, 2009.

[3] Z. Yunos and R. Ahmad, "The Application of Qualitative Method in Developing a Cyber Terrorism Framework," in Proceedings of the 2014 International Conference on Economics, Management and Development (EMD 2014), 2014, pp. 133–137.

[4] R. Ahmad, Z. Yunos, and S. Sahib, "Understanding Cyber Terrorism : The Grounded Theory Method Applied," in IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Malaysia, 26-28 June, 2012, pp. 334–339.

[5] Z. Yunos, R. Ahmad, and N. A. A. Abd Aziz, "Definition and Framework of Cyber Terrorism," Proceeding Southeast Asia Reg. Cent. Count. Terror. Sel. Artic., vol. 1/2013, pp. 67–79, 2013.

[6] R. Ahmad, Z. Yunos, S. Sahib, and M. Yusoff, "Perception on Cyber Terrorism: A Focus Group Discussion Approach," J. Inf. Secur., vol. 03, no. 03, pp. 231–237, 2012.

[7] Z. Yunos, "The New Frontier for Terrorists," Published in the STAR In-Tech Malaysia, 2008.

[8] Z. Yunos, "Illicit Activities and Terrorism in Cyberspace," in Proceeding of CENS-GFF CyberSecurity Forum – The Geostrategic Implications of Cyberspace, 2011, pp. 12–13.

[9] Z. Yunos, R. Ahmad, S. M. Ali, and S. Shamsuddin, "Illicit Activities and Terrorism in Cyberspace : An Exploratory Study in the Southeast Asian Region," in Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2012), Malaysia, 29 May, Springer Lecture Notes in Computer Science, Volume 7299/2012, 2012, pp. 27–35.

[10] Z. Yunos and S. H. Suid, "Protection of Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Development of Strategy and Policy Framework," in IEEE International Intelligence and Security Informatics (ISI) Conference, Vancouver, Canada, 23-26 May, 2010, p. 169.

[11] Z. Yunos, S. H. Suid, R. Ahmad, and Z. Ismail, "Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework," in IEEE Sixth International Conference on Information Assurance & Security, Atlanta, GA, 23-25 Aug, 2010, pp. 21–27.

WordPress vs Joomla: A Comparative Study

By | Nur Fazila Selamat, Mohd Nor Akashah Mohd Kamal, Mohd Masri Abd Kamad

Abstract - At present, content management systems (CMS) are a well-known technology in the Web development industry, especially among website developers. CMS can ease the process of development and offers several useful features and benefits. WordPress, Drupal, Joomla, Blogspot and Moodle are several types of CMS applications. This article addresses only two open-source content management software, which are WordPress and Joomla. This article also provides an overview of these content management systems with their features and key vulnerabilities together with how to prevent them. A comparative study is done between the two abovementioned CMSs, namely WordPress and Joomla.

Keywords: Content management system, Joomla, WordPress, CMS

Introduction

In the current Information Technology era, there is great desire to automate and simplify processes. A content management system (CMS) serves as a tool to manage website content and information depositories. CMS is a software bundle that facilitates building a website that can be updated quickly and easily by non-technical staff members [1]. Such open source software is created and subsidized by a group or community of developers and can be downloaded at no cost. CMS is used to support creating, updating, publishing, translating, distributing, archiving, and retiring of digital information. It also includes standard features, such as tracking changes made to digital information [2]. Figure 1 represents statistics of websites that use CMS technologies. According to the statistics, WordPress (39%) has the highest usage of open source CMS, followed by Drupal (9%), Google Search Appliance (3%) and Adobe CQ (3%).

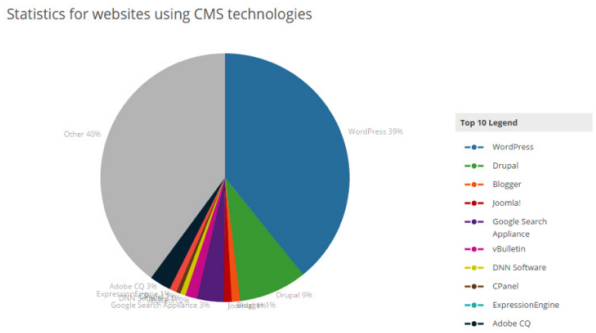


Fig. 1: Statistics for websites using CMS technology [3]

What is CMS?

A CMS is defined as an application (more likely web-based) that provides capabilities for multiple users with different permission levels to manage (all or a section of) content, data or information of a website project or internet/ intranet application [5].

Managing content refers to creating, editing, archiving, publishing, collaborating on, reporting, and distributing website content, data and information [5].

Fig. 2: Background of CMS [4]

Features of Content Management Systems

There are three types of features available in CMS. These are core features, design features and extra features. Details of these types of features are given below.

Core Features	Design Features	Extra Features
▪ Integrated and online help ▪ Modular and extensible ▪ Easy user and group management ▪ Group-based permission system ▪ Full template support for unlimited looks without changing a line of content ▪ Easy install and upgrade procedures ▪ Administration panel with multiple language support ▪ Hierarchy content with unlimited depth and size ▪ Integrated file manager ▪ Integrated audit log ▪ Small footprint	▪ XHTML and CSS compliant ▪ Auto-generated menu ▪ Every page can have different themes ▪ Design protected from content editors ▪ Multiple content areas on one page	▪ Search ▪ Polls ▪ News ▪ Blogs ▪ Newsletters ▪ CGCalendar ▪ File Uploading ▪ Glossary ▪ Forms ▪ User Management ▪ Guestbooks ▪ Google Sitemap

Table 1: Features of Content Management Systems [2]

Key Vulnerabilities of CMS

Web security is becoming more important as more enterprises outsource their business applications to software-as-a-service models [15]. As a web application, a CMS is an attractive target for attackers and a major source of security vulnerabilities [15]. Threats affect one or more security aspects. Some of the web application threats include the following.

- **Data manipulation**

This type of attack entails the process of changing data, which can violate data integrity. Common attack techniques include parameter manipulation and SQL injection [16].

- **Accessing confidential data**

Attackers access off-the-record data using techniques such as structured Query Language (SQL) injection and cross-site scripting (XSS).

- **Code execution**

Attackers can exploit CMS vulnerabilities to load files or programs containing defective codes onto a web server [16]. A consequence of this attack in 2015 was that most Joomla platform versions up to 3.4.5 were affected [17].

How to Prevent CMS Vulnerabilities?

Several processes need to be implemented on any CMS platform to prevent vulnerabilities, such as [9]:

- Ensure CMS is running in the latest version.
- Ensure the CMS systems are updated regularly.
- Use trusted sources for themes and plug-ins.
- Change the default settings and “ADMIN” name.
- Reduce credentials.
- Always use strong passwords.
- Protect the .htaccess file.
- Ensure CMS installation is backed up regularly.
- Plan a disaster recovery plan.

WordPress

1. What is WordPress?

WordPress was released in 2003 by Matt Mullenwegg [10]. WordPress is the world’s most popular content management system [3]. It started out as a platform exclusively for blogging but has grown and advanced significantly over the years. Today, over 40% of sites using CMSs are using WordPress [3]. In addition, over 60 million websites are using WordPress, showing just how popular it is [12].

Figure 3 below illustrates a sample website that uses WordPress, while Figure 4 shows the back-end structure of WordPress to administrate the site.

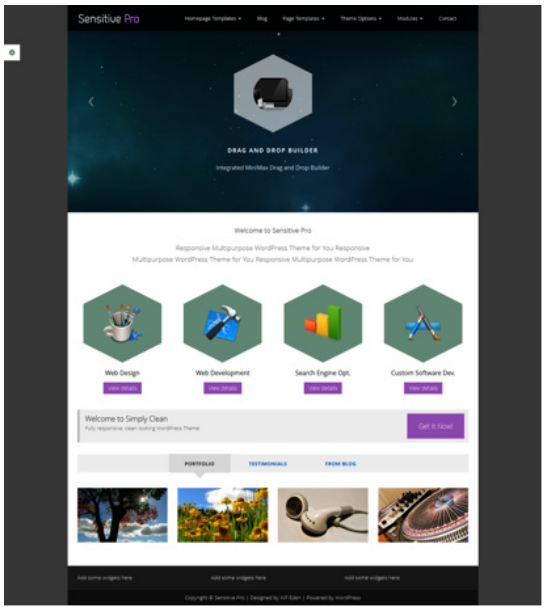


Fig. 3: Sample website using WordPress

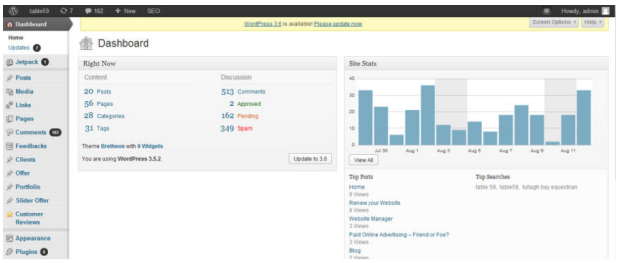


Fig. 4: Backend structure for WordPress

2. Features of WordPress

WordPress provides some features that can ease the development or editing process. Features offered by WordPress include [8]:

i. Simplicity
ii. Flexibility
iii. Ease of publishing
iv. Publishing tools
v. User management
vi. Built-in comments
vii. Search Engine Optimization (SEO)
viii. Multilingual
ix. Easy installation and upgrades
x. Own your data
xi. Media management
xii. Easy theme system
xiii. Extended with plug-ins
xiv. Freedom
xv. Community

Joomla

1. What is Joomla?

Joomla was released in 2005 forked by Mambo [10]. Joomla is a class of Open Source CMS written in PHP scripting language and uses a MySQL database for the backend [6]. Joomla is one of the best and most widely used CMS applications. It is suitable for creating corporate websites or intranets, online magazines, community-based portals and more. It has numerous built-in features as well as a large selection of extra modules and components to enhance the value of the website and enrich the visitors' experience [4]. Many aspects like extensibility and ease of use have made Joomla one of the most popular content management software. Best of all, Joomla is an open source software that is freely available to all.

Figures 5 and 6 show a sample page in Joomla for front-end and back-end views respectively.

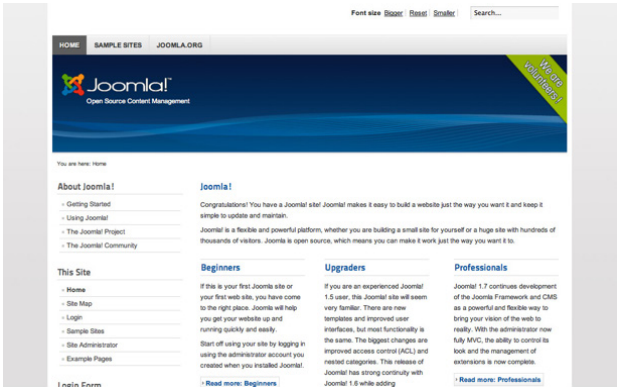


Fig. 5: Front-end of Joomla

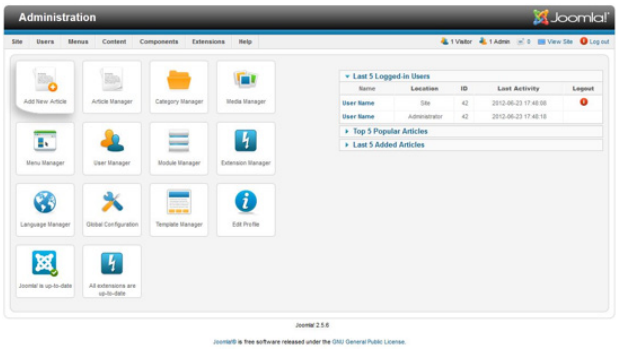


Fig. 6: Back-end structure of Joomla

2. Core Features of Joomla

Joomla offers several core features, including the following:

Multilingual
Joomla offers more than 64 languages.

Well-Supported
Thousands of professional (developer and other user) service providers throughout the world

can help build, maintain and market a Joomla project.

Easy Upgrades
There is a "One Click Version Update" feature to make this process super easy for users of any skill level.

Media Manager
A tool for easy uploading, organizing and managing media files and folders.

Better Search
The search ability of Joomla facilitates better and smarter searches for users.

Extensions
There are more than 8000 extensions to customize a website in Joomla.

Frontend Editing
Users can do content editing easy and fast by simply clicking and editing from the frontend.

Menu Manager
Allows creating as many menus and menu items as needed as well as structuring the menu hierarchy (and nested menu items) completely independent of the content structure.

WordPress vs Joomla: Comparative Analysis

i. Overview Comparison

For a quick overview, WordPress is the best pick for beginners as it works well for small to medium size websites, blogs and stores. Meanwhile, Joomla is great for e-commerce types of sites, but it requires at least some level of technical coding [10]. The table below shows a more in-depth comparison between WordPress and Joomla.

	WordPress	Joomla
Release Year	2003 by Matt Mullenwegg	2005, forked from Mambo
Popularity	> 140 million downloads	> 30 million downloads
Cost	Free	Free
Top Sites using the Platform	Forbes, CNN, SONY	HARVARD UNIVERSITY, THE HILL
Free Themes	2,000+	900+
Free Plugins	27,000+	7,000+
One Click Installation Availability	Available	Available
Manual Installation Time	5 minutes	10 minutes
"Skill" Level Needed	★ Technical experience is not necessary; it is intuitive and easy to get a simple site set up quickly. It is easy to paste text from a Microsoft Word document to a WordPress site, unlike Joomla.	★ ★ More complex than WordPress. Relatively uncomplicated installation and setup. With a relatively small investment of effort to understand Joomla's structure and terminology, it is possible to create fairly complex sites.
Update Frequency	42 days	36 days
Best Used for	Blogs, corporate websites, small-medium size websites	e-commerce, social networking sites

Pros	▪ User friendly ▪ SEO integration ▪ Responsive sites ▪ Great support	▪ Powerful ▪ User friendly ▪ E-commerce ▪ Developer community ▪ Extensions
Cons	▪ Security WordPress is a target for hackers and prone to attacks. Although security has got better over the past 12 months, there are still vulnerabilities in the CMS, particularly around the 3rd party plugin used. ▪ Updates WordPress (WP) releases system updates that are good for WP but may not be for the user. If the user needs are the same as those that WP tries to address, users are lucky. Otherwise, a user might get updates that harm rather than improve the website. ▪ Speed WordPress sites contain lots of generic codes unnecessary for every specific website, so the webpage loading time becomes slower.	▪ Small Module Marketplace Joomla has a much more limited marketplace for additional modules and add-ons. If you are looking for additional modules to customize a site, they can be harder to find and maintain through Joomla. ▪ Plugin Compatibility There may occur some frustrating compatibility issues between some of the plugins. It may turn out that it is impossible to get certain functionalities without some serious work on the PHP code.

Table 2: Comparison Chart between WordPress and Joomla [7][8][10][13][14]

ii. Comparison based on Popularity by Google Trends

Referring to Figure 7, Google Trends indicates that starting in 2010, WordPress has been strongly increasing in popularity compared with Joomla [18]. The figure also shows that as of January 2016, people's interest with WordPress is higher than with Joomla, and most of the time, people prefer using WordPress instead of Joomla.

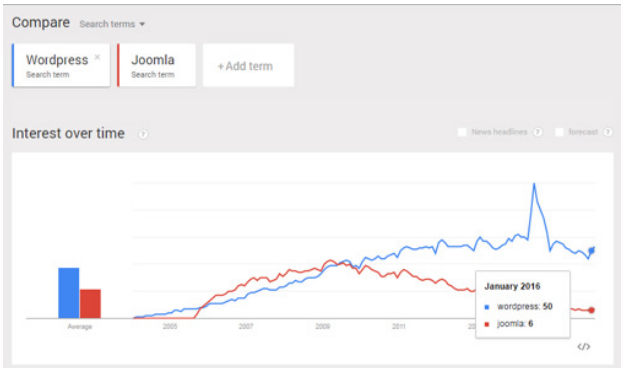


Fig 7: Popularity comparison between WordPress and Joomla according to Google Trend [18]

In addition, as we can see in Figures 8 and 9, there are several regions that frequent the use of CMS, either WordPress or Joomla as their platform. Figure 8 indicates that Bangladesh is the top community that most frequently uses WordPress as their CMS. Meanwhile, Figure 9 shows that Kenya is the region or community that most frequently uses Joomla as the backbone of their website or system.

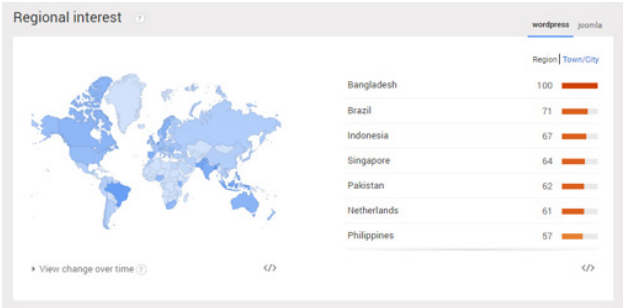


Fig. 8: Regional interest with WordPress [18]

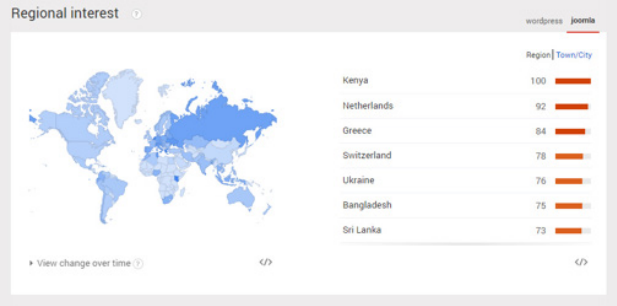


Fig. 9: Regional interest with Joomla [18]

Conclusion

Cybercriminals are aware that there are large numbers of unpatched installations of popular content management systems (CMS), including WordPress and Joomla. Therefore, it is crucial to have a good understanding of the risks of content management systems and of how to prevent risks. Based on the results of a comparative study, both WordPress and Joomla have various strengths and weaknesses. WordPress is more well-known than Joomla in terms of popularity, whereby WordPress has over 140 million downloads compared to Joomla with only 30 million downloads. However, selecting a CMS all depends on the user's requirements to support their web strategy both today and in the future. Users also recommend employing Google Trends [18] to get an idea of current CMS trends.

References

[1] Ghorecha, V., & Bhatt, C. (2013). A guide for Selecting Content Management System for Web Application Development. Computer Science Management Studies, 1(3), 13–17.

[2] Soediono, B. (2015). Open source content management software, Joomla & Drupal: A comparative study. Journal of Chemical Information and Modeling, 53(2394), 160. doi:10.1017/CBO9781107415324.004

[3] CMS technologies Web Usage Statistics. (n.d.). Retrieved February 12, 2016, from http://trends.builtwith.com/cms

[4] Ghorecha, V., & Bhatt, C. (2013). A guide for Selecting Content Management System for Web Application Development. Computer Science Management Studies, 1(3), 13–17.

[5] What is a Content Management System (CMS)?. (n.d.). Retrieved February 12, 2016, from http://www.comentum.com/what-is-cms-content-management-system.html

[6] Wakode, B. V, & Chaudhari, D. N. (2013). Study of Content Management Systems Joomla and, 569–573.

[7] About Joomla. (n.d.). Retrieved from http://www.joomla.org/about-joomla.html

[8] WordPress Features. (n.d.). Retrieved from https://WordPress.org/about/features/

[9] Alvarez, M. (2015). Pressing Your Luck With WordPress? A Look at CMS Security Risks. Retrieved February 17, 2016, from https://securityintelligence.com/pressing-your-luck-with-wordpress-a-look-at-cms-security-risks/

[10] Robert Mening. (n.d.). WordPress vs Joomla vs Drupal + CMS "Comparison Chart." Retrieved from http://websitesetup.org/cms-comparison-wordpress-vs-joomla-drupal/

[11] Hagen Graf. (n.d.). Joomla CMS. Retrieved from http://www.wilsonmar.com/joomla.htm

[12] Colao, J. J. (2012). With 60 Million Websites, WordPress Rules The Web. So Where's The Money? Retrieved from http://www.forbes.com/sites/jjcolao/2012/09/05/the-internets-mother-tongue/#7b00443955fe

[13] The 2015 WordPress vs Joomla vs Drupal Infographic. (n.d.). Retrieved from https://cmsreport.com/articles/the-2015-wordpress-vs-joomla-vs-drupal-infographic-13720

[14] Joomla! Core Features. (n.d.). Retrieved from https://www.joomla.org/core-features.html

[15] Symantec Global Internet Security Threat Report Trends for July–December 07 Volume XIII. (2008). Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

[16] Sametinger, J., & Wiesauer, A. (2009). Security in Open Source Web Content Management Systems, (August).

[17] Marc-Alexandre Montpas. (2015). Vulnerability Details: Joomla! Remote Code Execution. Retrieved from https://blog.sucuri.net/2015/12/joomla-remote-code-execution-the-details.html

[18] Google Trend-WordPress vs Joomla. (n.d.). Retrieved from https://www.google.com/trends/explore#q=WordPress%2CJoomla&cmpt=q&tz=Etc%2FGMT-8

Steganography Series: Peak Signal-to-Noise Ratio

By | Abdul Alif Bin Zakaria

Introduction

Steganography is the art and science of hiding messages. The word steganography comes from the Greek words "Steganós" meaning covered and "Graptos" meaning writing [5]. Steganography and cryptography are similar in that both are used to protect important information. However, steganography differs from cryptography because it involves hiding information without noticing any alteration made to the cover object. Cover objects or carriers are files such as text, images, audio or video in which secret messages are hidden. The secret message can be in the same form as the cover object. A file containing a secret message hidden in the cover object is called a stego object. Cryptography entails changing a readable into an unreadable message, while steganography involves hiding messages into another medium.

Steganalysis

Steganalysis is the art and science of detecting secret communication in steganography. In general, steganalysis techniques can be categorized into six levels depending on how much information is required about the hidden messages. The techniques are (i) Differentiating between the cover and stego object, (ii) Identifying the steganographic method, (iii) Estimating the length of a hidden message, (iv) Identifying the stego-bearing pixels, (v) Retrieving the stego key, and (vi) Message extraction [6]. Changes in statistical properties of the cover may lead to a steganalyst attempting to detect the existence of the secret communication [5]. One of the most common steganalysis methods implemented is to measure the quality of the stego image using Peak Signal-to-Noise Ratio (PSNR).

Image Pixel

An image is an array of numbers that represent the intensity level of each pixel comprising the image. A colour image is represented by arrays of each of the three primary colours, red, green and blue. By superimposing these three arrays, each pixel is a sum of those three colours that will produce a coloured image. Digital images are typically stored in either 24-bit (true colour) or 8-bit files (colour palette). 24-bit pictures have better resolution; thus, the file size would be larger and there would be more space available to hide information. 3 bytes are used to represent each pixel (1 byte for each colour) in 24-bit images. The 3 bytes can be represented as hexadecimal, decimal or binary values. A sequence FFFFFF represents a combination of 100% red, 100% green and 100% blue that will produce the colour white. Meanwhile, 00000 represents a combination of 0% red, 0% green and 0% blue that produce black. This combining method is applied to each pixel in order to compose an image. Information could be hidden by embedding secret messages into image pixels depending on the method implemented by the users.

Peak Signal-to-Noise Ratio

PSNR is a standard measurement method used in steganography in order to test the quality of stego images [2]. The higher the PSNR value, the higher the quality of the stego image is. If the cover image is C with size M × M and the stego image is S with size N × N, then each cover image C and stego image S will have a pixel value (x, y) from 0 to M-1and 0 to N-1 respectively. The PSNR is calculated as follows:

$$PSNR = 10\ log_{10}\left(\frac{MAX^2}{MSE}\right)$$

where

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\Big(C(x,y) - S(x,y)\Big)^2$$

Note that MAX is the maximum possible pixel value of an image. For example, if the pixels are represented by 8 bits per sample, then the MAX value is 255. MSE, or Mean Square Error is an error metric used to compare image compression quality. It represents the cumulative squared error between the compressed and original image. If the stego image has a higher PSNR value, then the stego image is of better quality.

Analysis

Figure 1 [4]: Jelly Bean Image

Jelly fish	256 x 256		306 x 468		512 x 512	
% embed	PSNR	MSE	PSNR	MSE	PSNR	MSE
0.1	42.5254	3.6353	42.5254	3.5982	42.5733	3.5954
0.2	39.5109	7.2776	39.5109	7.2147	39.5831	7.1576
0.3	38.4854	9.2159	38.4854	9.0156	38.6009	8.9741
0.4	38.4853	9.2161	38.4853	9.0158	38.6012	8.9734
0.5	38.4389	9.3151	38.4389	9.0151	38.6007	8.9745
0.6	38.3925	9.4153	38.3925	9.0153	38.6009	8.9741
0.8	38.3469	9.5145	38.3469	9.0145	38.6005	8.9749
0.7	38.3465	9.5155	38.3465	9.0155	38.6006	8.9747
0.9	38.3025	9.6123	38.3025	9.0144	38.6004	8.9751
1	38.2976	9.6232	38.2976	9.0154	38.6005	8.975

Table 1 [4]: Jelly Bean PSNR

Table 1 [4] shows a comparison of PSNR and MSE values of a "jelly bean" in Figure 1. The image was embedded with different data (secret message) capacities ranging from 0.1% - 1% of different image sizes (256 x 256, 306 x 468 and 512 x 512). It can be seen that with increasing embedded data capacity, the value of PSNR decreases and MSE increases. In other words, the more data that is embedded in the original image file, the more the picture quality will decrease. Depreciating picture quality happens because many bits of the original image have been changed or replaced by secret message bits.

The more bits that are modified in the original image, the more obvious the changes are to the naked eye. In steganography, if one can see a significant change in a cover object, the secrecy of data is exposed and it is contrary to the main objective of steganography, which is to hide the presence of messages [3].

Figure 2 [1]: Lena Image

Stego image performance decreases when more bits of cover image are modified. Figure 2 shows the differences in stego images that have been implemented with 1-bit to 7-bit data hiding using steganography. As the stego image gets more distorted, the PSNR value becomes lower and could increase the awareness of the existence of the hidden data.

Conclusion

It is hard to detect the presence of steganography because the existence of secret messages that are kept secret through steganography. One will never try to do steganalysis for all images, text, audio or video in communication to find secret or hidden message, as it would cost a lot of time and money. An efficient method implemented is by calculating the PSNR. Even though it is not the absolute solution to this problem, a steganalyst can at least narrow down the suspected stego object that contains a secret message, which could lead to finding the secret message.

Previous steganography series can be viewed on the CyberSecurity Malaysia website:

Title :
Steganography Series: Colour Palettes

Publication :
CyberSecurity Malaysia e-Security Bulletin. Vol 38 – (1/2015)

Link :
http://www.cybersecurity.my/data/content_files/12/1499.pdf

References

[1] Gupta H., Kumar R. and Changlani S. 2013. Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method. International Journal of Emerging Technology and Advanced Engineering. Vol. 3, No. 6.

[2] Ibrahim R. and Kuan T.S. 2011. Steganography Algorithm to Hide Secret Message Inside an Image. Computer Technology and Application. Vol. 2: 102-108.

[3] Shamimunnisabi and Cauvery N.K. 2012. Empirical Computation Of Rs-Analysis for Building Robust Steganography Using Integer Wavelet Transform and Genetic Algorithm. International Journal of Engineering Trends and Technology. Vol. 3, No. 3.

[4] Usha B.A., Srinath N.K. and Cauvery N.K. 2013. Data Embedding Technique In Image Steganography Using Neural Network. International Journal of Advanced Research in Computer and Communication Engineering. Vol. 2, No. 5.

[5] Zakaria A.A., Yusof N.A.M., Omar W.Z., Abdullah N.A.N. and Rani H.A. 2015. Analysis of Steganography Substitution System Methods Using New Testing Techniques Proposed for Strict Avalanche Criterion. International Journal of Cryptology Research. Vol. 5, No. 1: 61-76

[6] Chaturvedi P. and Bairwa R.K. 2013. Image Steganography Method for Hiding Secret Message in Colored Images by Using IWT. International Journal of Recent Research and Review. Vol. 6, No. 3.

Rise of the DD4BC Copycats

By | Farah Ramlee

Introduction

From September 2014 through July 2015, cyber extortion was taken to another level and DD4BC emerged as the latest crime with a new modus operandi similar to Ransomware. DD4BC is an abbreviation of DDoS for Bit Coin. DD4BC is an extortionist group responsible for many bitcoin extortion campaigns involving DDoS attacks and ransom demands. This type of extortion is distributed through email. The email content is used to inform the target that if the ransom demand does not meet the deadline, a low-level DDoS attack would be launched against the victim's server [2]. To show the seriousness of such extortion, a mini demonstrative attack will be launched to prove their point. [3] Like Ransomware, the ransom goes through the dark web by charging in BitCoin and keeps increasing while the attack is in action.

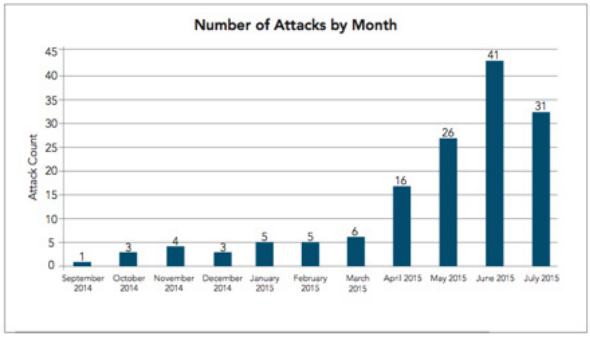


Figure 1: DD4BC DDoS attack activity increased dramatically in April but began tapering off in July (by Akamai) [4]

The financial service sector was most targeted, including banks, credit unions, currency exchange and payment processing companies. [1]

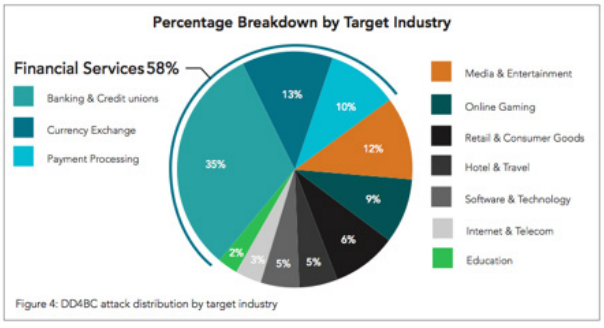


Figure 2: DD4BC attack distribution by target industry (by Akamai)[4]

DD4BC recently threatened to expose targeted organizations via social media, adding to the damage caused by the DDoS attack itself. The goal apparently was to garner more attention to the group's ability to create service disruptions by publicly embarrassing the target and tarnishing the company's reputation through these wide-reaching channels. {2]

According to Akamai researchers, the group's methodology typically includes multi-vector DDoS attack campaigns, revisiting former targets and also incorporating Layer 7 DDoS in multi-vector attacks, specifically concentrating on the WordPress pingback vulnerability. This vulnerability is exploited to repeatedly send reflected GET requests to the target to overload the website. This attack method is also incorporated into DDoS booter suite frameworks. The group used multi-vector DDoS attacks including NTP floods, SSDP floods, UDP floods, SYN floods, UDP fragment floods, ICMP floods, DNS floods, GET floods, SNMP floods and CHARGEN floods. 141 DDoS attacks confirmed as DD4BC were observed by Akamai and partners from September 30, 2014 to July 24, 2015. [1] The key cyber extortionist member was reportedly arrested in early January 2016. [3]

However, soon after, a new group called Armada Collective imitated the DD4BC tactics, techniques and procedures (TTP) hoping to gain billions of dollars. The possible drive for this act was probably that the price index of bitcoins keeps increasing and bitcoins are encrypted. The remaining cyber criminals took advantage and produced even more copycats, as companies were willing to pay the ransom to avoid being attacked. [6]

Analysis

Cyber999 received a report regarding this incident involving a cyber extortionist group, Armada Collective. However, the email reported below is just imitating the real Armada Collective because the attack did not happen on the said date.

```
---------- Forwarded message ----------
From: Armada Collective <armadacollectivedos@openmailbox.org>
Date: Fri, Mar 11, 2016 at 6:54 AM
Subject: DDOS ATTACK
To:

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

All your servers will be DDoS-ed starting Wednesday (March 16.) if you don't pay protection fee of 25 Bitcoins @
18A7h96ueXaoKKqEWQsQ7HQWkhKSTZqpUf

When we say all, we mean all - users will not be able to use your services at all.
If you don't pay by Wednesday, attack will start, price to stop will increase to 50 BTC and will go up 25 BTC for every day
of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 25 BTC @ 18A7h96ueXaoKKqEWQsQ7HQWkhKSTZqpUf

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM
US!
Bitcoin is anonymous, nobody will ever know you cooperated.
```

Figure 3: Sample ransom email from Armada Collective reported to Cyber999

Figure 3 shows that the email consists of a template starting with an introduction of them, followed by a ransom that the victim would be DDoS-ed on the given date if the payment in bitcoins was not done. The extortionist also included their bitcoin wallet ID.

```
Delivered-To:
Received: by xx.xx.xx.xx with SMTP id [illegible];
      Thu, 10 Mar 2016 15:11:44 -0800 (PST)
X-Received: by 1xx.xx.xx.xx with SMTP id [illegible];
      Thu, 10 Mar 2016 15:11:44 -0800 (PST)
Authentication-Results: mx.google.com;
   spf=pass (google.com: domain of armadacollectivedos@openmailbox.org designates xx.xx.xx.xx as permitted sender) smtp.mailfrom=armadacollectivedos@openmailbox.org
   dkim=pass header.i=@openmailbox.org
Received-SPF: pass (google.com: domain of armadacollectivedos@openmailbox.org designates xx.xx.xx.xx as permitted sender) client-ip=xx.xx.xx.xx;
Received: by xx.xx.xx.xx with POP3 id [illegible];
      Thu, 10 Mar 2016 15:11:44 -0800 (PST)
X-Gmail-Fetch-Info: 1 x.com 110
Return-Path: <armadacollectivedos@openmailbox.org>
Delivered-To:
Received: (qmail 43028 invoked by uid 89); 11 Mar 2016 06:49:51 +0800
Delivered-To: x.com-marketing@x.com
Received: (qmail 43015 invoked by uid 89); 11 Mar 2016 06:49:51 +0800
Received: from unknown (HELO smtp1.openmailbox.org) (xx.xx.xx.xx)
  by dns12.kutu.net with SMTP; 11 Mar 2016 06:49:51 +0800
Received: by mail2.openmailbox.org (Postfix, from userid 1004)
        id 28E492AC9A10; Thu, 10 Mar 2016 23:54:14 +0100 (CET)
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=openmailbox.org;
        s=openmailbox; t=1457650453;
        bh=[illegible];
        h=Date:From:To:Subject:From;
        b=[illegible]
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on openmailbox-b2
X-Spam-Level: **
X-Spam-Status: No, score=2.1 required=5.0 tests=ALL_TRUSTED,BAYES_50,
        DKIM_ADSP_ALL,SUBJ_ALL_CAPS,URIBL_BLOCKED autolearn=no autolearn_force=no
        version=3.4.0
Received: from www.openmailbox.org (openmailbox-b2 [xx.xx.xx.xx])
        by mail2.openmailbox.org (Postfix) with ESMTP id 8E8182AC9A85;
        Thu, 10 Mar 2016 23:54:02 +0100 (CET)
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII;
 format=flowed
Content-Transfer-Encoding: 7bit
Date: Thu, 10 Mar 2016 22:54:01 +0000
From: Armada Collective <armadacollectivedos@openmailbox.org>
To:
Subject: DDOS ATTACK
Message-ID: <60dbbd67d33c6a48a14ed551694cacbb@openmailbox.org>
```

Figure 4: Email header from the Armada Collective Copycat

Figure 4 shows that the email header from the so-called Armada Collective with the email was originally sent using a free email web server called OpenMailbox. The sender's IP address is internal, which means it belongs to the application, hence preventing the detection of the originating IP source. This is in fact a way that culprits are able to get away, as the application protects its users under their own privacy. However, we have reported regarding this email through their web-reporting channel.

Another case that caught our eye was reported by an organization that received an extortion email with a different threat. The threat content was not to DDoS their servers, but the email mentioned that time bombs were physically placed at some unstated stations and would blow up on the said date if the ransom demand were not fulfilled.

```
-----Original Message-----
From: trainman@sigaint.org [mailto:trainman@sigaint.org]
Sent: Tuesday, 15 March, 2016 1:37 AM
Subject: We planted time bombs some of the station

We planted time bombs some of the station . This is terrorism .
The bomb will explode at 18:00 on March 16 .
If you want to know where is the bomb , you must pay 70BTC for us . Do you know bitcoin ?
Pay to 1HPFfCwrq6aRJeqtk37RzbMmG8xCJ52PsS (or discover the bomb on their own)

Notice: we will plant time bombs another station if you don't pay 70BTC for us .


Trainman
```

Figure 5: Email received regarding a time bomb threat

```
Received: from xxxx.com.my (xx.xx.xx.xx) by xxxx-CASHUB01.xxxx.com.my (xx.xx.xx.xx)
with Microsoft SMTP Server id 8.3.406.0; Tue, 15 Mar 2016 01:39:21 +0800
Return-Path: <trainman@sigaint.org>
Received: from [xx.xx.238.120] (EHLO mx1.sigaint.org) by xxxx.com.my
(MicroWorld SMTP 6.6.64); Tue, 15 Mar 2016 01:51:54 +0800
Resent-Date: Tue, 15 Mar 2016 01:51:54 +0800
Resent-From: <trainman@sigaint.org>
X-Originating-IP: xx.xx.238.120
X-Auth-User: trainman@sigaint.org
X-Filename: D:\PROGRA~1\MailScan\in\SMT1526546516011.TMP
Received: from sigaintevyh2rzvw.onion (localhost [127.0.0.1])    by localhost
(OpenSMTPD) with ESMTP id ed7edf39;  Mon, 14 Mar 2016 17:37:21 +0000 (UTC)
Received: from 127.0.0.1      (HTTP authenticated user trainman)      by
localhost with HTTP;     Mon, 14 Mar 2016 17:37:21 -0000
Message-ID: <0f62900404119e7ecb1d3e5191f5aed7.webmail@localhost>
Date: Mon, 14 Mar 2016 17:37:21 +0000
Subject: We planted time bombs some of the station
From: <trainman@sigaint.org>
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal
X-ForeignSender-IP: xx.xx.238.120
X-URLS: sigaint.org
To: Undisclosed recipients:;
```

Figure 6: Email header received regarding a time bomb threat

Figure 6 shows the email was sent using yet another public mail server called Sigiant. However, it was written in the website's disclaimer that any incidents should be reported if any abuse was traced using the server. In this case, an email from trainmain@sigiant.org with the source IP address xx.xx.238.120 was detected. The incident was then escalated to the respective ISP for further action.
In both cases, none of the attacks were launched after the dates passed. We may conclude these were just other copycats following the TTP of the original DD4BC for money extortion through the net.

Conclusion

Different types of DDoS attacks can affect specific IT network elements and require various DDoS mitigation techniques. Attackers identify the weakest links that will cause the most damage. To help protect against extortionist groups and subsequent DDoS attacks, advice and recommendations are given as the follows for defensive measures [5]:

- Deploy anomaly- and signature-based DDoS detection methods to identify attacks before a website becomes unavailable to users.
- Distribute resources to increase resiliency

and avoid single points of failure due to an attack.

- Implement Layer 7 DDoS mitigation appliances on the network in strategic locations to reduce the threat to critical application servers.

The best practice to prevent your network from getting a DDoS attack is to develop a checklist or standard operating procedure (SOP) to follow in the event of a DDoS attack. [8] A proper DDoS mitigation plan also needs to be in place to help minimize damage and conduct "business as usual" during an attack.

If you need any assistance, do not hesitate to contact Cyber999 via the following channels:

E-mail:
cyber999@cybersecurity.my

Phone:
1-300-88-2999 (monitored during business hours)

Fax :
+603 89453442

Mobile:
+60 19 2665850 (24x7 call incident reporting)

SMS:
CYBER999 REPORT EMAIL COMPLAINT to 15888

Business Hours:
Mon - Fri 08:30 - 17:30 MYT

Web:
http://www.mycert.org.my

References

[1] https://www.stateoftheinternet.com/resources-web-security-threat-advisories-2015-dd4bc-case-study-ddos-attacks-bitcoin-extortion-ransom.html

[2] http://www.prnewswire.com/news-releases/akamai-releases-findings-of-increased-attacks-and-more-aggressive-tactics-from-dd4bc-extortionist-group-300139405.html

[3] http://www.scmagazine.com/key-member-of-dd4bc-arrested-in-international-crackdown/article/465097/

[4] http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf

[5] https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html

[6] http://www.securityweek.com/dd4bc-armada-collective-inspire-cyber-extortion-copycats

[7] https://blogs.akamai.com/2015/09/case-study-operation-dd4bc.html

[8] https://www.us-cert.gov/ncas/alerts/TA12-024A

Successful Cybersecurity Capacity Building

By | Adam Palmer, FireEye

Long-term capacity building is the foundation for success in achieving cybersecurity goals. A capacity building plan should include a dynamic assessment and improvement process that aligns with a long-term strategy. This should be a flexible approach that is modified as technology and threats evolve. It is proposed in this article that the goal of a cybersecurity programme should achieve a level referred to as "Adaptive Defence." Adaptive Defence is the ability to detect and respond to identified security needs by utilizing intelligence-based information and effective response planning.

Adaptive defence entails more than achieving "Basic Cyber Hygiene." This base level must be expanded to include advanced threats and unknown attacks. 70% of the time malware is used only once. Traditional means of 'basic hygiene' are no longer sufficient to protect against today's cyber threats, which are unique, complex and no longer preventable by using traditional prevention methods.

The SANS Institute and the Council on Cybersecurity, a consortium of security experts from across public and private sectors, has published a list of 'Top 20 Security Controls' - a relatively short list of high-priority, highly effective actions that provides a useful and effective starting point for every enterprise seeking to improve their cyber defence. Two key controls in particular – CSC-5 and CSC-13 – include recommended measures that go beyond traditional hygiene for malware and boundary defence. In the USA, the National Institute of Standards and Technology (NIST) Cybersecurity Framework best practices include NIST 800.53 SC-7 (Boundary Protection), SC-44 (Detonation Chambers) and SI-3 (Malicious Code Protection). These are elements of cybersecurity best practices that are particularly critical to any effective cyber hygiene program and they have been adopted and recommended by leading independent global security experts.

Each of the core Adaptive Defence domains are examined in detail below.

Detection: Detection includes utilizing intelligence from a range of sources and making decisions based on a flexible programmatic approach. Threat intelligence should include awareness of known threat groups, their known attack methodologies and anticipated attack vectors. Identifying who may be the source of an attack can support understanding the objectives of the attackers and why they may be targeting an organization. An adaptive defence security programme should evolve from passive monitoring to active "hunting" for evidence of threat actors within a network. This approach assumes the presence of an attacker that is using unknown intrusion techniques.

Prevention: Prevention includes basic activities to avert known threats. These activities comprise traditional security controls that are essential to a security programme. However, these basic controls must be supplemented by additional behavioural-based heuristic detection capabilities that can prevent attackers from exploiting an unknown vulnerability.

Response: Response should include both the capability to recover quickly from a cyberattack and a measurement of the time necessary to resume critical operations after an attack. Response should also include the following sub-domain controls:

- Incident Management
- Service Continuity Management
- External Dependency Management

The Response Strategy must establish an incident response coordinator and precisely define protocols to inform key stakeholders. These protocols should govern privacy disclosure requirements and assignment of work streams for investigation, remediation, communication and response plan execution.

Analysis: Analysis consists of containment, forensics investigation and skill chain reconstruction. An effective strategy should emphasize on adaptation based on analysis of known attacks. Post-incident analysis forms the basis of an "adaptive" response by adjusting controls based upon actual known risks. Analysis of known attacks should promote the adoption of appropriate technical and organizational measures to safeguard data at a security level

appropriate to actual risks. Understanding attack methodologies promotes informed decision-making, intelligence integration and timely response.

Long-Term Planning

The most important concept of a capacity building plan is that each organization has unique needs. An organization must identify critical areas that correlate with a desired security readiness posture. Within each area are maturity levels. Maturity levels are established by measuring progress along a continuum of risk-based preparedness from low readiness levels to advanced full capability. This risk and capability evaluation process allows decision makers to benchmark existing cybersecurity preparedness and evaluate core competencies, and it provides an operational framework for capacity building that also measures improvement dynamically.

Cybersecurity is not only a technical solution. The foundation for all technical solutions should be based on a clear understanding of policy requirements and strategy goals. Compliance is not "true security." Many threats can evade basic compliance measures that tend to only promote "basic hygiene." The overall objective of an Adaptive Defence capacity building programme is to create more than a mere compliance or basic hygiene capability as recommended above.

The capacity building structure should be designed so as to enable a comprehensive, long-term and holistic approach. Each activity domain within the suggested capacity building programme can be summarized as follows:

Framework Support:

- The assessment of operational needs and development of a strong sustainable framework that provides comprehensive operational security and procedures for operations.

Operational Standards:

- Comprehensive assessment of existing legislative policies covering criminalization, procedural law, electronic evidence, jurisdiction, private sector responsibilities and liabilities, and international cooperation, using good practice benchmarks and relevant regional and national standards

Operational Training:

- Delivery of training at the basic, intermediate, and advanced levels on advanced electronic evidence collection and handling
- For the government, the delivery of investigator and prosecution training at the basic, intermediate and advanced levels on the role and presentation of electronic evidence and applicable substantive and procedural law in the prosecution and adjudication of cybercrime cases
- Organization of public private partnership expert working groups to create protocols on the involvement of specialized procedures, use of investigative measures, guidelines for intelligence sharing operations, and the introduction and consideration of electronic evidence in legal forums.

Sustainability:

- Providing long-term coordination and support mechanisms to effectively transfer capabilities from global experts or security vendors to internal organizational staff and to maintain team readiness

Cooperation:

- Facilitating working relations between law enforcement and local offices of key global digital service providers, developing procedures and due legal process requirements, and facilitating the sharing of strategic threat information from key global cybersecurity providers with intelligence analysts
- Establishing advanced teams working with law enforcement and intelligence groups to apply legal, procedural and technical tools to monitor and respond effectively to threats

A suggested phased implementation plan is outlined below:

Phase I: Operational Framework Assessment & Development

a. Assessment of Operational, Procedural, and Training Requirements

b. Development and Review of a Capacity Building Framework and Capacity Building Programme Recommendations

Phase II: Implementation

a. Establishing on-site cooperative partnership teams led by global experts to implement capacity building programmes from basic to advanced levels

b. Training in advanced detection and response capabilities that ensure compliance with

international regulatory frameworks and best practices

c. Evaluating implementation and adjustment to meet identified standard goals

Phase III: Sustainability and Maintenance

a. Additional support for staff on tools and techniques as determined necessary through monitoring and evaluation

b. Implementing long-term external cooperation and support mechanisms

Progress in programme implementation should be tracked through ongoing monitoring of the needs indicators established in an initial assessment. The purpose of ongoing monitoring is to ensure accountability through transparent and clearly-documented records with a view to enable clear oversight, decision-making and transparent operations. Information required for the indicators should be collected with a periodicity appropriate to each indicator, taking into account the time required for outputs and outcomes to have effect. Results from calculated available indicators can be used to ensure that activities, outputs and outcomes are in line with the expected results.

The challenge of advanced cyber threats is unlikely to be resolved in the near future. Both private organizations and the government must commit to a long-term programme of capacity building for prevention, detection and response. It is critical for capacity building actions to aim clearly towards a sustainable response that achieves an “active defence.” Investment should be made in establishing functional and sustainable solutions that create a solid foundation for the future.

Getting to Know The Knowledge Management Centre of CyberSecurity Malaysia

By | Zaleha Abd Rahim

Introduction

Wikipedia defines 'Special Library' as a library that provides specialised information resources on particular subjects, serves a specialised and limited clientele and delivers specialised services to that clientele. In other words, Special Library is a term for a library that is neither an academy or school, nor a public or national library. Normally, special libraries are developed to support the vision and mission of an organisation. Special libraries are 'special' in their collections and services, which are more targeted and specific to the needs of the users.

The Knowledge Management Centre (KMC) of CyberSecurity Malaysia falls under this category, whereby we specialize in subject matters related to information security and cyber security. The Knowledge Management Centre was established in 2008 as part of the CyberSecurity Malaysia initiative to realize the vision of a National Cyber Security Reference and Specialist Centre by the year 2020. Previously, it was known as the Knowledge Resource Centre (KRC). However, the name has been changed to the Knowledge Management Centre to reflect its role and discipline in promoting a collaborative and integrated approach to the creation, capturing, access and use of knowledge assets. The centre acts as a platform for cyber security professionals and communities to seek a comprehensive collection of cyber security-related information materials. The Knowledge Management Centre also aims to provide a conducive learning and knowledge acquisition environment for cyber security professionals and practitioners across the nation.

KMC Key Objectives

- To complement the government's effort to produce 'K-Workers' particularly in the field of cyber security
- To contribute to CyberSecurity Malaysia's goal of becoming a Learning Organisation that empowers employees to be innovative and productive human capital, possess positive attitude and forge strong teamwork
- To gain national recognition as a national knowledge hub through the establishment of a place that provides a mind-stimulating knowledge acquiring environment in the field of cyber security.

Collection Development

The Knowledge Management Centre (KMC) envisions being a National Knowledge Reference Point in the area of cyber security. For this reason, our collections consist primarily of print and electronic resources focusing on cyber security-related information materials in order to meet the information needs of cyber security professionals and communities. The collections are basically divided into a few categories:

- **Main Collections:** Printed and online resources covering disciplines specified by CyberSecurity Malaysia and the information security community nationwide.
- **Reference Collections:** Dictionaries, encyclopaedias, directories, biographies, numerical data compilations, handbooks, manuals, bibliographies and yearbooks.
- **Control Access Collections:** Materials that are commonly used, such as theses, dissertations, research reports, seminar/ conference papers, official publications (e.g. annual reports) and small-size publications (e.g. statistics, surveys).
- **Serial Collections:** Cyber security-related journals, magazines, newspapers and bulletins.
- **Multimedia Collections:** Non-print materials in the form of audio, CDs and DVDs.
- **Leisure Reading Collections:** Light reading materials covering bestsellers, fiction, motivation, hobbies, crafts, etc.
- **Cybersiana Collection:** Articles and slide presentations written by CyberSecurity Malaysia professionals

Services And Activities

The Knowledge Management Centre of CyberSecurity Malaysia supports and upholds the CyberSecurity Malaysia vision, i.e. 'To Be a Globally Recognised National Cyber Security Reference and Specialist Centre by 2020.' Therefore, we provide services and activities to cater and meet the information needs of staff. In addition to the basic operational services, such as cataloguing, classification, check-out and check-in of materials, we also provide information dissemination services, such as the Current Awareness Service [CAS] and Selective Dissemination of Information [SDI]. However, we re-brand the services by giving special names and disseminate information daily in order to keep our staff well-informed.

Monday:
Pick of the Week -- we choose several titles and display the books in the centre. Then we broadcast the titles via email to inform staff, especially newcomers, that we have those titles in the collection and they are most welcome to borrow them. However, if we purchase new titles, we change the broadcast to What's New.

Tuesday:
SDI K-Brief -- we choose a subject and select a few articles related to the subject. Then we email the abstracts of the selected articles to all staff. Those who are interested to read the full text of the articles are encouraged to request a copy from us.

Wednesday:
Current Awareness Service (CAS) -- we disseminate information extracted from new issues of technical journals and magazines received in a particular month. This way, our users will update their knowledge on the latest trends and technologies on cyber security matters.

Thursday:
Santai Jom Baca is targeted for those who want to take a break and relax by reading leisure materials such as Men's Health, Impiana; Harmoni; Reader's Digest; Pa & Ma; Umpan; Saji, etc.

Friday:
K-Share materials are extracted from several resources and those who are interested to read the full text over the weekend are most welcome to request a copy from us.

KMC also offers a service known as **'InfoQuest'** where CyberSecurity Malaysia staff can request Knowledge Management staff to assist with identifying and finding articles of interest.

Today, knowledge matters. Therefore, more organisations are recognising knowledge as their most valuable and strategic resource to sustain their competitive advantage. The Knowledge Management Centre of CyberSecurity Malaysia aims to develop a knowledge-intensive culture by encouraging and aggregating behaviours, such as knowledge sharing and proactively seeking, acquiring and offering knowledge. Therefore, in addition to the information dissemination services, the Knowledge Management Centre also takes the initiative to organize several knowledge sharing activities, as we strongly believe these activities help CyberSecurity Malaysia with acquiring, capturing, storing and utilizing knowledge for problem solving, dynamic learning, strategic planning and decision making.

Cafe Ilmu @ KMC

Cafe Ilmu @ KMC was initiated to encourage CyberSecurity Malaysia staff to share and exchange their reading experiences and knowledge in an informal environment. Staff share and discuss what they have read and audiences are most welcome to add value based on their own knowledge and experiences as well. Since the centre's collection is very limited and focused on information security and cyber security matters, we encourage our Cafe Ilmu @ KMC participants to share their own reading materials regardless of subject interest. After the session, a summary is written and emailed to CyberSecurity Malaysia staff in order to benefit those who were not able to join and participate in the session. Later, those summaries are compiled and published as a KM Newsletter.

[Picture: Dr. Zahri Yunos sharing his reading entitled 'It Worked for me in Life and Leadership' by Colin Powell]

Jom Borak Ilmu

This is a platform where staff of CyberSecurity Malaysia can present and share their specific knowledge, especially technical knowledge

once they return from any training, seminar or conference. Again, it is done in an informal environment with the hope that knowledge will flow freely and trigger informative discussions. This is also a good platform for staff to practice their communication skills and public speaking.

[Picture: Ahmad Dahari Jarno from the SA Department sharing his technical expertise on a Social Engineering Experiment]

Technical Colloquium

The Technical Colloquium serves as a platform for CyberSecurity staff to present their research papers in order to solicit feedback and comments before their papers are submitted for journal publications. In addition, Technical Colloquium is a knowledge sharing platform for researchers to enhance their communication and presentation skills.

[Picture - Khairul Akram from the Digital Forensics Department presenting his paper]

Occasionally, the Knowledge Management Centre also organizes activities, such as Infohunt, Merdeka Day Quizzes, ISMS Awareness Day, Thematic Exhibition and KM Appreciation Day.

Summary

Knowledge is an important asset to CyberSecurity Malaysia as it can enhance communication and collaboration among employees, create new knowledge and add value to the entire organisation. For these reasons, the Knowledge Management Centre plays its role effectively and efficiently to ensure that CyberSecurity Malaysia's vision and mission are met.

References

1. https://en.wikipedia.org/wiki/Special_library

2. KRC Policies and Procedures

National Cryptographic Algorithm Projects

By | Isma Norshahila binti Mohammad, Nik Azura binti Nik Abdullah Shah, Norul Hidayah binti Lot@Ahmad Zawawi, Liyana Chew binti Nizam Chew

Introduction

Cryptography plays a crucial role in information security. Cryptography systems are used to protect valuable information resources for both data in transit and at rest. However, there have been a variety of cryptographic problems arise, involving cryptographic algorithms in communication to protect classified information. Therefore, many countries, such as Japan, the USA and European countries have shown initiatives to develop a mechanism to identify trusted algorithms. Trusted algorithms are used by standard bodies and governments. This article briefly explains four national cryptographic algorithm projects that have been set up, namely NESSIE, CRYTREC, projects by NIST and eSTREAM.

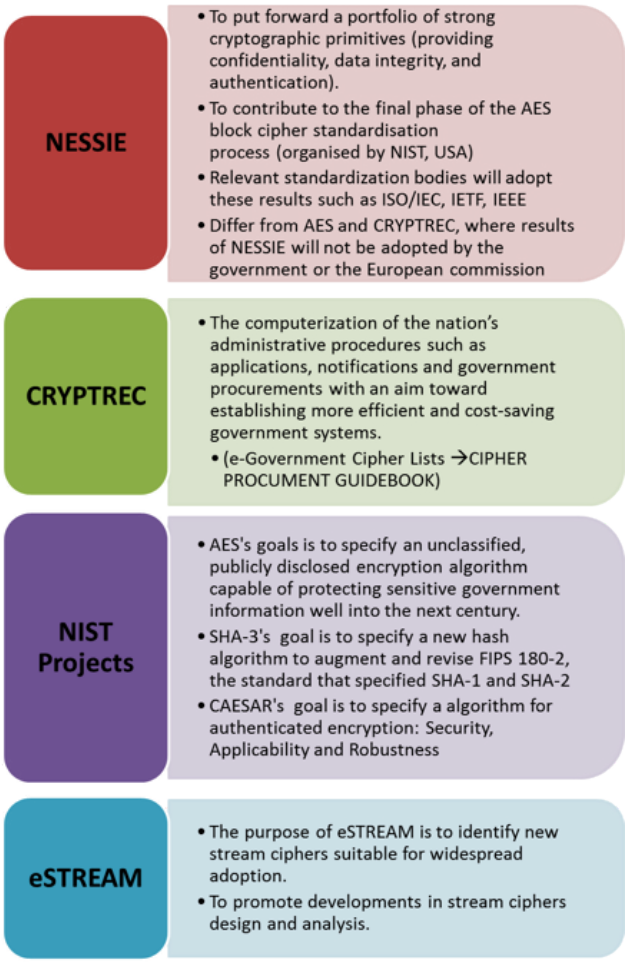
NESSIE is a project within the Information Society Technologies (IST) Programme of the European Commission. It was founded from 2000 to 2003 to identify secure cryptographic primitives. The project was comparable to the NIST AES process and the Japanese government-sponsored CRYPTREC project, but with notable differences.

CRYPTREC is an abbreviation of Cryptography Research and Evaluation Committees and refers to a project to evaluate and monitor the security of e-Government recommended ciphers as well as to examine the establishment of evaluation criteria for cryptographic modules. The task of evaluating existing cryptographic techniques has been entrusted to the Information Technology Promotion Agency, Japan (IPA).

AES, SHA-3and CAESAR are projects by National Institute of Standards and Technology (NIST), United States of America. AES is a competition ran by NIST to find a block cipher to replace the Data Encryption Standard (DES). The NIST hash function competition, which is SHA-3 competition, was set up to develop a new hash function called SHA-3 to complement the older SHA-1 and SHA-2. CAESAR is a competition for Authenticated Encryption: Security, Applicability and Robustness schedule from 2014 to 2017.

eSTREAM is a stream cipher project by ECRYPT (European Network of Excellence in Cryptology). This project was set up to identify new stream ciphers suitable for widespread adoption. The submissions to eSTREAM fall into either or both of two profiles, which are Profile 1: Stream ciphers for software applications with high throughput requirements and Profile 2: Stream ciphers for hardware applications with restricted resources.

The objectives and goals of each project are as follows:



Types of Primitives

A list of cryptographic primitives per project is as follows:

NESSIE

Block cipher	•High. Key length of at least 256 bits. Block length at least 128 bits •Normal. Key length of at least 128 bits. Block length at least 128 bits. •Normal-Legacy. Key length of at least 128 bits. Block length 64 bits
Synchronous stream ciphers	•High. Key length of at least 256 bits. Internal memory of at least 256 bits. •Normal. Key length of at least 128 bits. Internal memory of at least 128 bits.
Self- synchronizing stream ciphers	•High. Key length of at least 256 bits. Internal memory of at least 256 bits. •Normal. Key length of at least 128 bits. Internal memory of at least 128 bits.
Message Authentication Code (MACs)	•High. Key length of at least 256 bits. •Normal. Key length of at least 128 bits.
Collision-resistant hash function	•High. Output length of at least 512 bits. •Normal. Output length of at least 256 bits.
One-way hash functions	•High. Output length of at least 256 bits. •Normal. Output length of at least 128 bits.
Families of pseudo-random functions	•High. Key length of at least 256 bits. •Normal. Key length of at least 128 bits.
Asymmetric encryption schemes (deterministic and randomised)	•The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.
Asymmetric digital signature schemes	•The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.
Asymmetric identification schemes	•The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions. •The probability of impersonation should be smaller than 2^{-32}.

CRYPTREC

Public-Key Systems	• Classes by functions (a combination of a cryptographic scheme and primitive/auxiliary functions) • In terms of functions there are classes as Confidentiality, Signature, Authentication, Key Sharing
Symmetric Systems	• Block Ciphers - Block size of 64, 128 bits or longer, consists of data randomizing part and key scheduling part. • Stream Ciphers
Hash Functions	• Assumptions that password authentication, digital signature and message authentication were used • Required of cryptographic hash functions are unidirectionality and no collision • Stream ciphers with hash value of 128 bits or longer.
Pseudo-Random Number Generating Schemes	• Assumed to be used for generating cryptographic keys and key seeds. • Requires the ability to generate high quality random numbers that will make it almost impossible to forecast through quantitive calculation.

NIST

AES	• A block cipher supporting a block length of 128 bits and key lengths of 128, 192, and 256 bits.
SHA-3	• A new hash function to complement the older SHA-1 and SHA-2.
CAESAR	•Block ciphers •Dedicated stream ciphers •Stream ciphers based on block ciphers •Dedicated hash functions, sponges, etc. •Hash functions based on block ciphers •Dedicated MACs •MACs based on hash functions •MACs based on block ciphers •Authenticated encryption based on any of the above •Dedicated ciphers with built-in authentication

eSTREAM

- Stream ciphers for software applications with high throughput. Must support 128-bit key. Must support 64-bit IV and 128-bit IV.
- Stream ciphers for hardware applications with highly restricted resources. Must support 80-bit key. Must support 32-bit IV and 64-bit IV.

Evaluated Algorithms

Cryptographic algorithms evaluated for each project are as follows:

NESSIE

Block Cipher	• Anubis, Camellia, CS-cipher, Grand Cru, Hierocrypt. – Hierocrypt-L1 and Hierocrypt-3, IDEA., Khazad, MISTY1, Nimbus, Noekeon, NUSH, Q.,RC6, SAFER++, SC2000, SHACAL. – SHACAL-1 and SHACAL-2.
Stream Ciphers and Pseudo-random number generators	• BMGL, SNOW, LEVIATHAN, LILI-128, SOBER. – SOBER-t16 and SOBER-t32.
Hash Functions	• Whirlpool
Message Authentication Code(MACs)	• UMAC, Two-Track-MAC
Asymmetric encryption schemes(deterministic and randomised)	•ACE-KEM (upgrade of ACE-Encrypt), EPOC. – EPOC-1, EPOC-2 and EPOC-3, ECIES, RSA-OAEP (revised to RSA-KEM [584]), PSEC. – PSEC-1, PSEC-2, PSEC-3 and PSEC-KEM
Digital signature schemes	• ACE Sign, ECDSA, ESIGN, QUARTZ, RSA-PSS, FLASH and SFLASH.
Digital identification schemes	• GP
Evaluation methodologies	• General Next Bit Predictor

CRYPTREC (2012)

Public Key Cryptographic Schemes	• Signature - DSA, ECDSA, ESIGN, RSA • Confidentiality - ECIES, HIME(R), RSA • Key agreement - ECDH, DH, PSEC-KEM
Symmetric Key Cryptographic Schemes	• 64-bit block cipher - CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, Triple DES • 128-bit block cipher - AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, RC6 Block Cipher, SC2000 (128-bit block cipher) • Stream cipher - MUGI, MULTI-S01, RC4
Hash Functions	• RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512
Pseudo-Random Number Generator	• PRNG in ANSI X9.42-2001 Annex C.1/C.2, PRNG in ANSI X9.62-1998 Annex A.4, PRNG in ANSI X9.63-2001 Annex A.4, PRNG for DSA in FIPS PUB 186-2 Appendix 3, PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1, PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1

NIST

AES	• CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, Twofish
SHA-3	• Abacus, ARIRANG, AURORA, BLAKE, Blender, Blue Midnight Wish, BOOLE, Cheetah, CHI, CRUNCH, CubeHash, DCH, Dynamic SHA, Dynamic SHA2, ECHO, ECOH, EDON-R, EnRUPT, ESSENCE, FSB, Fugue, Gröstl, Hamsi , JH, Keccak, Khichidi-1, LANE, Lesamnta, Luffa, LUX, MCSSHA-3, MD6, MeshHash, NaSHA, SANDstorm, Sarmal, Sgàil, Shabal, SHAMATA, SHAvite-3, SIMD, Skein, Spectral Hash, Stream Hash, SWIFFTX, Tangle, TIB3, Twister, Vortex, WaMM, Waterfall
CAESAR	• ++AE, AES-CMCC, AES-COBRA, AES-CPFB, Artemia, AVALANCHE, Calico, CBA, CBEAM, Enchilada, FASER ,HKC, iFeed[AES], Julius, KIASU, LAC, Marble, McMambo, PAES, PANDA, POLAWIS, Prøst, Raviyoyla, Sablier, Silver, Wheesht, YAES

eSTREAM

• HC-128 (also HC-256), Rabbit, Salsa20/12 (also Salsa20/8, Salsa20), SOSEMANUK, Grain v1 (supersedes: Grain v0), MICKEY 2.0 (also MICKEY-128 v2), Trivium, F-FCSR-H (also F-FCSR-16; supersedes: F-FCSR), CryptMT v3 (supersedes: CryptMT v1, Fubuki), Dragon, LEX, NLS v2 (supersedes: NLS v1), DECIM v2 (supersedes: DECIM v1), Edon-80, MOUSTIQUE (supersedes: MOSQUITO), POMARANCH v3 (supersedes: POMARANCH v1), ABC v3 (supersedes: ABC v1), DICING P2 (supersedes: DICING P1), Phelix, Polar Bear v2 (supersedes: Polar Bear v1), Py, Achterbahn-80 (also Achterbahn-128), Hermes8, TSC-4 (supersedes: TSC-3), VEST P2 (supersedes: VEST P1), WG P2 (supersedes: WG P1), ZK-Crypt P2 (supersedes: ZK-Crypt P1), Frogbit, Mir-1, MAG, TRBDK3 YAEA, Yamb, SFINKS

Decision Factors

Cryptographic algorithms for each project were selected based on the following decision factors:

NESSIE
- Security
- Performance in implementations
- Cipher strengths (compare with standards and well-known algorithm)

CRYPTREC
- Cipher strength,
- Long-term (10 years) cipher security, and
- History of cipher usage by the general public

AES
- General Security
- Software implementations
- Restricted-space environments
- Hardware implementations
- Attacks on implementations
- Encryption versus decryption
- Key agility
- Other versatility and flexibility
- Potential for instruction-level parallelism

SHA-3
- Message Digest Size of 256
- Use the largest message block size available
- No salt inputs

CAESAR
- Security
- Cipher strength
- Features
- Design rationale

eSTREAM
- Profile 1: should be good in software in terms of speed and security.
- Profile 2 : should be good in hardware in terms of performance, security and suitability for deployment on devices.

Approved Algorithms

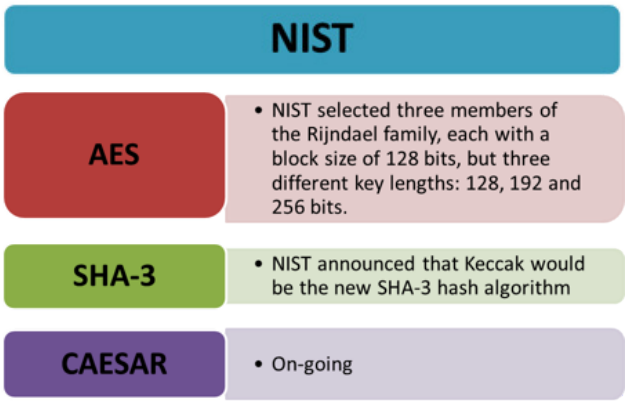
The approved cryptographic algorithms for each project are listed below:

NESSIE

Block Cipher	• IDEA, Khazad, MISTY1, SAFER++64, SAFER++128, Camellia, RC6, Shacal
Synchronous stream ciphers	• SOBER-t16, SOBER-t32, SNOW, BMGL
MAC algorithms and hash functions	•Two-Track-MAC: K.U.Leuven, Belgium and debis AG, Germany; •UMAC: Intel Corp., USA, Univ. of Nevada at Reno, USA, IBM Research •Laboratory, USA, Technion, Israel, and Univ. of California at Davis, USA; •Whirlpool*: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium
Public-key encryption algorithms	•ACE-KEM* (IBM Zurich Research Laboratory, Switzerland - derived from ACE Encrypt), EPOC-2* (Nippon Telegraph and Telephone Corp., Japan), PSEC-KEM* (Nippon Telegraph and Telephone Corp., Japan (derived from PSEC-2), ECIES* (Certicom Corp., USA and Certicom Corp., Canada), RSA-OAEP* (RSA Laboratories Europe, Sweden and RSA Laboratories,USA)
Digital signature algorithms	• ECDSA (Certicom Corp., USA and Certicom Corp., Canada), ESIGN* (Nippon Telegraph and Telephone Corp., Japan), RSA-PSS (RSA Laboratories Europe, Sweden and RSA Laboratories, USA), SFLASH* (BULL CP8, France), QUARTZ* (BULL CP8, France)
Identification scheme	• GPS*: Ecole Normale Supérieure, Paris, BULL CP8, France Télécom and La Poste, France

CRYPTREC

Public Key Cryptographic Schemes	• Signature-- DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS • Confidentiality - RSA-OAEP, RSAES-PKCS1-v1_5 • Key agreement - DH, ECDH, PSEC-KEM
Symmetric Key Cryptographic Schemes	• 64-bit block ciphers - CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3-key Triple DES • 128-bit block ciphers - AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000 • Stream Ciphers - MUGI, MULTI-S01, 128-bit RC4
Other Techniques	• Hash Functions - RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512 • Pseudo-random Number Generators - PRNG based on SHA-1 in ANSI x9.42-2001, PRNG based on SHA-1 for general purpose in FIPS 186-2(+change notice 1) Appendix 3.1, PRNG based on SHA-1 for general purpose in FIPS 186-2(+change notice 1) revised Appendix 3.1



- Profile 1 - HC-128, Rabbit, Salsa20/12, Sosemanuk
- Profile 2 - F-FCSR-H v2, Grain v1 , MICKEY v2 , Trivium

References

1. *https://competitions.cr.yp.to/*

2. *http://www.ecrypt.eu.org/stream/finallist.html*

3. *https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process*

4. *http://www.iacr.org/archive/ches2010/62250240/62250240.pdf*

5. *https://www.cosic.esat.kuleuven.be/publications/article-439.ps*

6. *https://en.wikipedia.org/wiki/Advanced_Encryption_Standard*

7. *http://www.ecrypt.eu.org/stream/portfolio.pdf*

FIPS 140-2 Evaluation Laboratory Accreditation and Its Programs

By | Norul Hidayah binti Lot@ Ahmad Zawawi, Liyana Chew binti Nizam Chew, Nik Azura binti Nik Abdullah, Isma Norshahila binti Mohammad Shah

Introduction

The Federal Information Processing Standard (FIPS) 140-2 cryptographic module is a set of standards that have been approved and adopted at the international level. This standard outlines a clear evaluation and is reliable for evaluating the security capabilities of information technology products. The evaluation process is conducted by the Cryptographic and Security Testing Laboratory (CST Lab) and the evaluation report is reviewed by a body under the National Institute of Standard Technology (NIST) called the National Voluntary Laboratory Accreditation Program (NVLAP) to ensure that the security of cryptographic product is assessed to comply with standard guidelines. Verification of the cryptographic product is an important process to guarantee its security foundation before a certification is awarded. Figure 1 below shows the number of CST Lab(s) in each country that conduct cryptographic product evaluation based on the FIPS140-2 standard.

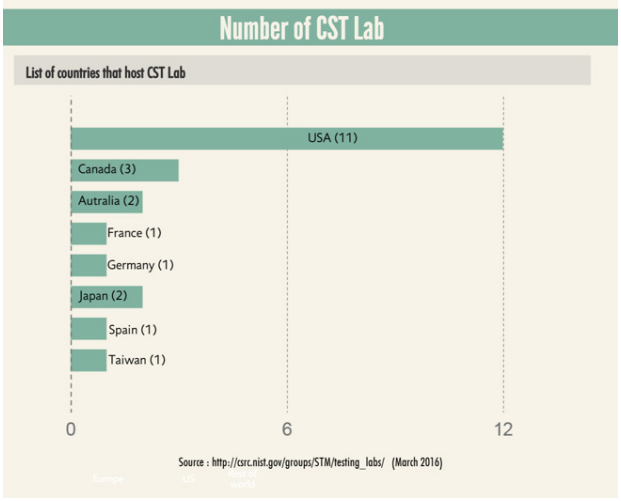


Figure 1: List of countries that have CST Lab(s)

This article briefly explains the flow of the FIPS140-2 accreditation laboratory process as well as the Cryptographic and Security Testing laboratory validation program consisting of the Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP).

1. FIPS140-2 Accreditation Laboratory Process

The following are the six steps in acquiring accreditation from NVLAP, NIST to enable an evaluation lab to perform FIPS140-2 evaluation.

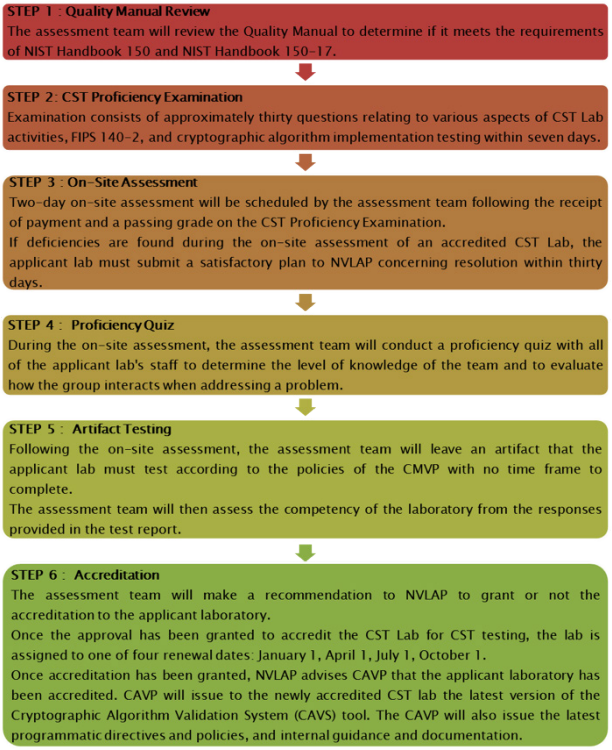


Figure 2: FIPS140-2 Accreditation Process

2. Cryptographic and Security Testing Laboratory (CST Lab) Validation Program

The Laboratory Accreditation Program (LAP) for CST Lab was established by NVLAP to accredit laboratories that perform cryptographic module validation conformance testing and algorithm testing known as the Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP).

Cryptographic Module Validation Program (CMVP)

CMVP is a validation program developed jointly by the Information Technology Laboratory

(ITL) of NIST and the Communication Security Establishment Canada (CSEC). The purpose of CMVP is to ensure the availability and assurance of secure cryptographic modules for the protection of information through conformance testing of cryptographic modules against the FIPS140-2 standard.

There are five steps in the CMVP process as shown in Figure 3:

Step 1: Implementation Under Test (IUT)

a. The vendor submits the cryptographic module for testing to an accredited CST Lab under a contractual agreement.

b. Cryptographic module validation testing is performed using the Derived Test Requirements (DTR) for FIPS Publication (FIPS PUB) 140-2, which are Security Requirements for Cryptographic Modules. If the CST Lab has any questions or requires clarification of any requirement with regard to the particular cryptographic module, the lab can submit Requests for Guidance (RFG) to NIST and CSE.

Step 2: Review Pending
Once all the testing requirements have been completed, a validation submission is prepared and submitted to NIST and CSE for validation.

Step 3: Under Review
A reviewer each from NIST and CSE is assigned to review the validation report, the non-proprietary security policy and other supporting documents.

Step 4: Coordination
During the review process, NIST and CSE will combine their comments on the validation report as required and then submit them to the CST Lab for action. This process will continue until all comments and/or questions have been satisfactorily addressed.

Step 5: Finalization

a. The vendor pays a validation fee prior to validation.

b. Once the cryptographic module has been validated, NIST and CSE will issue a certificate through the CST Lab to the vendor.

c. The new validated cryptographic module will be given an entry in the FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation List on the NIST website.

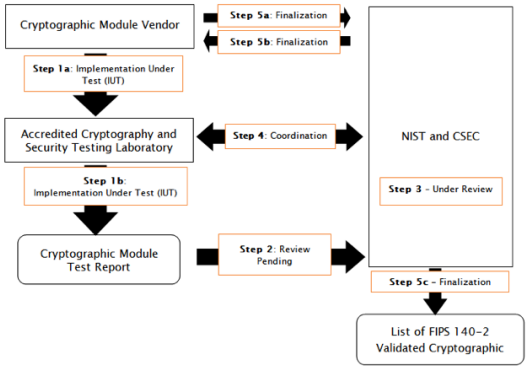


Figure 3: CMVP Process

Cryptographic Algorithm Validation Program (CAVP)

CAVP is a validation program jointly developed by ITL of NIST and CSEC for the validation of all FIPS-approved and NIST-recommended security functions. ITL developed a validation test suite to test the correctness of a security function's implementation for every FIPS-approved and NIST-recommended. CAVP is a pre-requisite to the CMVP.

There are eleven steps in the CAVP process as shown in Figure 4:

Step 1
The vendor selects one of the accredited CST Labs to oversee the algorithm validation testing of their cryptographic algorithm implementation. Note that the cryptographic algorithm implementation can be tested in-house by the vendor, or it can be sent to the selected CST Lab for testing (the term "tester" refers to the party performing the algorithm test).

Step 2
The CST Lab requests from the vendor information related to each cryptographic algorithm to be tested in the implementation.

Step 3
Using the validation system document, the tester implements the validation system test suite via the vendor's algorithm implementation.

Step 4
For each algorithm being tested, the CST Lab uses this information and the CAVS tool to generate input test vectors to be used in the validation tests.

Step 5
The CST Lab supplies the input test vectors to the tester.

Step 6
The tester uses the test vectors as inputs into the implementation.

Step 7

a. The results are forwarded to the CST Lab.

b. The CST Lab uses the CAVS tool to verify the validation test results. If the results are not correct, the CAVS tool records which test failed. The lab informs the vendor that the implementation does not meet the requirements of the associated reference and provides the information generated by CAVS to assist the vendor in determining where their algorithm implementation deviated from the reference specifications.

Step 8
Upon passing the cryptographic algorithm implementation validation test, the CST Lab submits an algorithm validation submission request package to NIST. This package contains the official validation request from the lab and all the files generated from the CAVS tool including a file summarizing the validation test results for each algorithm tested.

Step 9
NIST reviews the package for completeness and verifies that all tests have passed. If this is true, NIST and CSEC validate the implementation.

Step 10
NIST enters all relevant information related to this validation into an internal database that generates the Cryptographic Algorithm Validation Consolidated Certificate, which contains multiple cryptographic algorithm implementations. NIST signs this certificate and sends it to CSEC for their signature.

Step 11
Once validated, the cryptographic algorithm implementation is posted to the CAVP website. A separate cryptographic algorithm validation list exists for each approved cryptographic algorithm for which NIST has available testing.

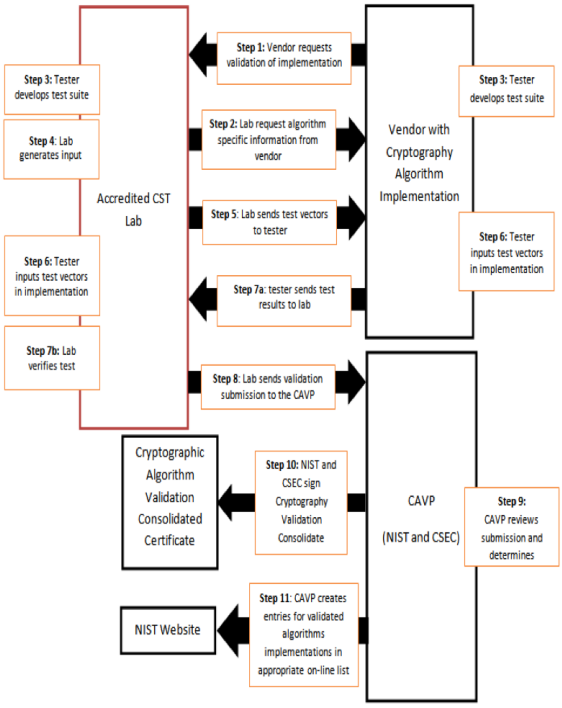


Figure 4: CAVP Process

Roles and Responsibilities

There are four parties involved in CMVP and CAVP. Each party has roles and responsibilities that are described in Figures 5 and 6:

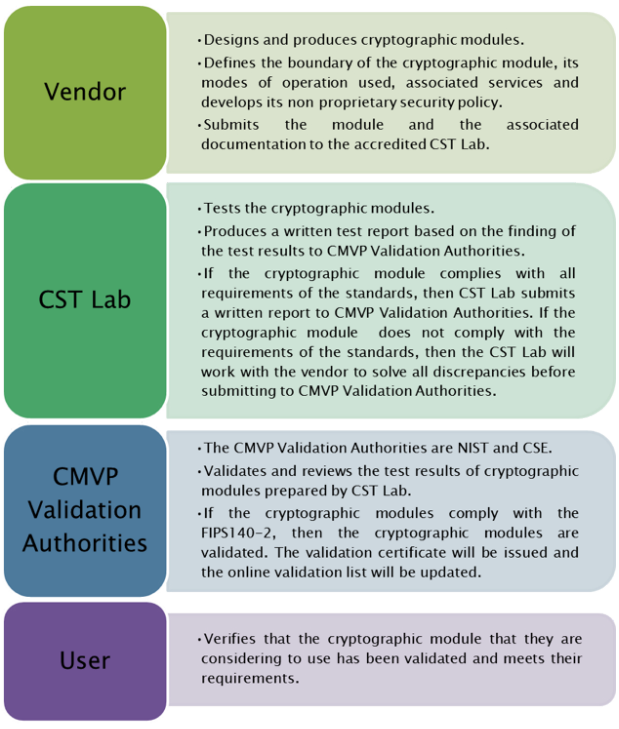


Figure 5: Roles and Responsibilities in CMVP

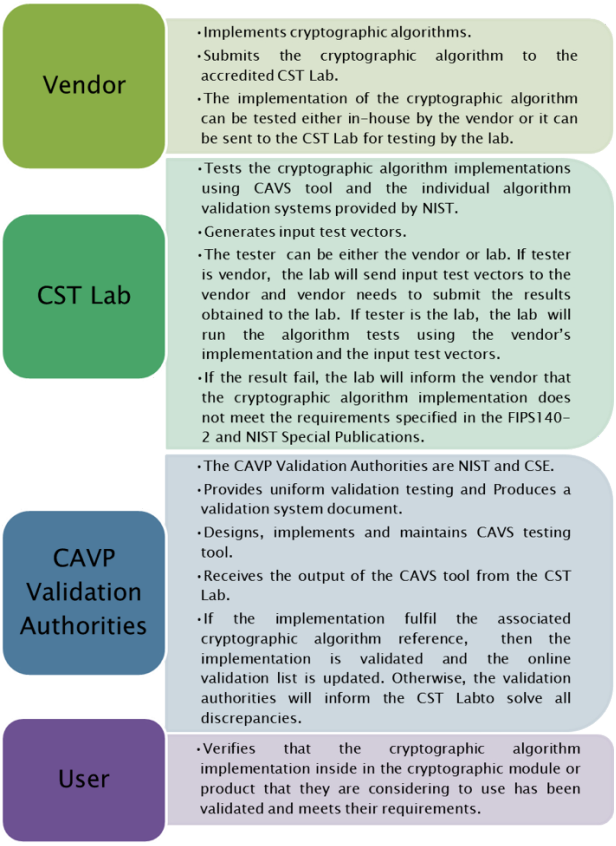


Figure 6: Roles and Responsibilities in CAVP

Conclusion

It is recommended for organizations to use validated cryptographic modules that comply with the requirements of FIPS140-2 in order to improve the protection of sensitive information. Although this standard is formally accepted by the Government of the United States of America and the Government of Canada, this program has been adopted by many other industries and countries. Organizations who choose to adopt this FIPS140-2 standard are well-served by the benefits of the security assurance provided by the validated modules.

References

3. *http://www.nist.gov/nvlap/*

4. *http://csrc.nist.gov/publications/nistbul/itlbul2014_11.pdf*

5. *http://csrc.nist.gov/groups/STM/cavp/documents/CAVPMM.pdf*

6. *http://www.nist.gov/nvlap/upload/NIST-HB-150-17-2013.pdf*

7. *http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPMM.pdf*

Vulnerability Assessment & Penetration Testing (Vapt): Approach And Methodology

By | Norazlila Binti Mat Nor

Introduction

Vulnerability assessment is defined as a comprehensive on-site security vulnerability testing and evaluation process performed by security analysts to identify security weaknesses and potential exposures to threats in the target systems. Penetration testing meanwhile attempts to exploit vulnerabilities in the system to determine whether unauthorized access or other malicious activity may possibly pose a threat to the system.

The objective of this article is to explain the approach and methodology of how to conduct Vulnerability Assessment & Penetration Testing (VAPT) in an organization. However, this is not a guide on how to hack networks and systems.

Approach and Methodology

The overall VAPT approach encompasses three (3) phases: pre-assessment, assessment and post-assessment. The activities are summarized in Figure 1 below.

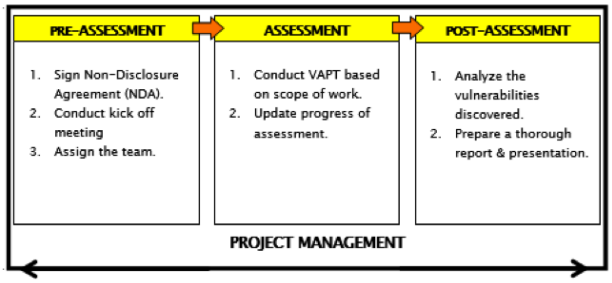


Figure 1: Phases and activities of VAPT

Phase 1: Pre-Assessment

1. Signing a Non-Disclosure Agreement

Before any VAPT activities begin, any supporting documents required, especially the Confidentiality and Non-Disclosure Agreement (NDA), must be finalised. The Confidentiality Agreement states that the information provided by the target organization will be treated as confidential and proprietary while NDA protects an organization's confidential information during business dealings with customers, suppliers, employee or any third parties.

Among the points recommended for inclusion in the NDA are:

- Identify truly valuable information and information that is critical to the organization.
- Clearly specify that the person/organisation who signs the agreement should not disclose what is mentioned within.
- Clearly identify all parties in the agreement.
- Specifically include the starting date and length of the nondisclosure period.

2. Conducting a Kick-Off Meeting

In order to perform VAPT successfully, good planning and preparations need to be done. Basically, a kick-off meeting should be held between the client and the security analysis team. The kick-off meeting will address the scope of work and objective of the assessment. The security analysis team should present to the client the expected output or assessment deliverables.

During the kick-off meeting, a project timeline also needs to be finalized. This is important to ensure that while VAPT activities are carried out, the normal business or daily operations of the organization are not compromised. The security analysis team are required to obtain permission on the allowable penetration testing hours and other client rules and regulations that need to be adhered to.

3. Assigning the Team

Based on the scope of work agreed upon, the assessment team should establish the project team structure. The project team will usually consist of a project manager, project management executive, quality assurance, team leader and team members. The roles and responsibilities of each member must be clear and if possible, the project team structure should be presented to the client. This is to ensure the client reaches the right person in charge if any problems arise while conducting VAPT.

The roles and responsibilities of each member

include but are not limited to:

a. Project Manager

- Responsible for the overall VAPT and reporting.
- Ensuring timely completion of project activities and submission of deliverables.
- Planning, developing and managing the overall project implementation.

b. Project Management Executive

- Managing day-to-day aspects of the project to ensure smooth operation throughout the project timeline.
- Monitoring and tracking project activities.
- Recording project expenses and invoices.
- Following up with the client on outstanding matters.
- Managing and ensuring all matters and change requests are properly addressed and resolved.

c. Quality Assurance

- Evaluating all aspects of the report, such as content, structure, overall style and format.
- Reviewing and evaluating the accuracy and completeness of the report content.

d. Team Leader

- Delivering, conducting and leading the assessment.
- Preparing updates on the progress of the assessment.
- Developing a VAPT report.
- Ensuring the client data are protected during the assessment.

e. Team Members

- Conducting VAPT based on the scope of work.
- Assisting the team leader with developing the VAPT report.
- Providing expert advice on related technical matters.
- Supporting the team leader with facilitating key project activities.

Phase 2: Assessment

1. Conducting VAPT

Ideally, VAPT activities begin with gathering information on the target or scope of assessment. A number of ways are available to do the necessary information gathering by using online tools or manual searching. The collected information is very useful to the project team to conduct the VAPT in the next stage.

One of the popular information gathering tools is Nmap, which is made for scanning large networks. It can also be used to determine what operating systems are running on a network as well as the type of packet filters/firewalls are in use, and numerous other characteristics.

Moreover, information can be gathered manually by searching the Internet. Many organizations reveal their activities, contact information and history information on their websites. Hence, conducting queries on the web might reveal information about domain names and networks that could be used to conduct further attacks.

Subsequent to information gathering, the project team will start with vulnerability assessment to discover any potential vulnerabilities present in the systems. Vulnerability assessment is essentially conducted using automated tools. Such tools are Nessus, SAINT and Retina for network security assessment and Acunetix for web application security assessment. The tools will scan a specific network or web application and are able to produce a list of possible vulnerabilities existing, together with steps to be taken to eliminate the vulnerabilities. The list will then be utilized in penetration testing.

Penetration testing is a method to evaluate security weaknesses of a web application and database, computer system or network device by simulating an attack from malicious outsiders as well as insiders performed on-site and remotely. The goal of this activity is to demonstrate the existence or absence of known vulnerabilities that could be exploited by attackers. Even the potential vulnerabilities already listed during vulnerability assessment do not mean that the exploitation or simulation can be done during the assessment period, as some of the exploits can take longer to succeed. Penetration testing is also not always successful even though it is theoretically possible.

2. Updating the assessment progress

During VAPT activities, it is recommended to

update the client on the assessment progress regularly. This is to ensure the client is aware of the extent of project completion. Most clients are very certain with project timelines and are unhappy with delays. This is why any problems or hiccups should be communicated to the client to ensure project success. The findings from the assessment can also be highlighted to the client on a daily basis, especially high-impact vulnerabilities.

Phase 3: Post-Assessment

1. Analysing the Vulnerabilities Discovered

This process involves presenting the data analysis results, categorising the vulnerabilities based on impact level ratings and proposing areas of improvement.

All data gathered during the vulnerability assessment and penetration testing will be compared and analysed against security best practices, the security environment and classification of vulnerabilities. Any vulnerability found during assessment will also be verified to avoid false positive findings.

2. Developing a Report

During the last phase of VAPT, the project team will be working offsite to develop a report. The report usually consists of vulnerability assessment findings and areas of improvement to mitigate the vulnerabilities.

Among the contents that should be included in the report are:

a. A technical description of each vulnerability

b. An anatomy of exploitation including steps taken and proof in the form of screenshots

c. Business or technical impact inherent in the vulnerability

d. Vulnerability classification that describes the impact level as a function of vulnerability risk and ease of exploitation

e. Technical descriptions of how to mitigate the vulnerabilities

Conclusion

There will always be new vulnerabilities and weaknesses in a network and its services as well as means of exploitation. This is due to the nature of an ever-changing network and its services adapting to new user demands. Technology advancements and the need for improvement inadvertently put networks or applications at risk.

The foundation of this VAPT exercise is to demonstrate that there is always a need to ensure establishing security processes like auditing and analysis to reduce risks and that VAPT must be conducted on a continuous basis.

References

1. Penetration Testing Procedures and Methodologies. EC Council Press.

2. Conducting a Penetration Test on an Organization. SANS Institute InfoSec Reading Room.

3. How Penetration Testing is Conducted. Core Security

4. Penetration Testing Guidance, PCI Security Standards Council

5. The Penetration Testing Execution Standard. www.pentest-standard.org/

6. Vulnerability Assessment and Penetration Testing. http://www.veracode.com/security/vulnerability-assessment-and-penetration-testing

Comparing sampled Information Security Body of Knowledge with ISO/IEC 27001

By | Razana Md Salleh, Sharifah Norwahidah Syed Norman

Introduction

Experience from recent years shows that cyberattacks aimed at informational systems of state bodies, the healthcare, energy, finance and transport sectors, and other critical national infrastructure (CNII) bodies are increasing and may lead to unpredictable consequences. With the rising threats, the need for skilled information security practitioners to safeguard critical systems is also on the rise. This has led to various academic, industrial and government bodies worldwide and especially in the United Kingdom and United States to start establishing a common body of knowledge for practitioners in the information security (IS) area. A body of knowledge, referred to as BOK, is a framework that contains a collection of information that provides a basis for understanding terms and concepts in a particular knowledge area. It defines the fundamental information that people working in the area are expected to have [1].

This article addresses the fundamentals of BOK for the IS field, which is used to develop certification programs for the beginner IS practitioner level, i.e. the first level of competency, as a first step in the IS career for recent graduates or those transferring from different careers. With BOK, IS practitioners are expected to have foundation knowledge and skill sets to assist with protecting an organization.

Comparing sampled IS BOK with ISO/IEC 27001

The main international standard for IS compliance is the International Standard ISO/IEC 27001:2013 Information Security Management System [2]. The standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) in an organization. The revised version of the standard contains 14 domains (from 11 domains in the 2005 version), constituting 114 controls.

In the ISO/IEC 27001 Standard, personnel competency is addressed in clause 7.2, which specifies the requirement for an organization to determine the necessary competence of person(s) doing work under its control that affects its information security performance. In addition, a new Standard document is currently being developed - the ISO/IEC 27021 – which entails competence requirements for information security management professionals. This indicates that having competent personnel is critical to preserving the confidentiality, integrity and availability of an organization's information.

Besides the Standard requirements, academic research has been conducted on the purposes of BOK for the IS field. One of the studies from 2007 proposed a common BOK for the IS field [3]. It was found in that research that IS field is a multi-disciplinary endeavour, so in reality, IS practitioners require knowledge in fields such as management, ethics, sociology and political science. According to the study, the existing IS BOK focuses on specific IS sub-domains, thus offering limited understanding and narrow perceptions of the overall domain. The common BOK proposed for IS contains 10 basic domains that can serve as a foundation to design academic curricula and courses for the beginner-level IS practitioners as follows:

1. Security Architectures and Models
2. Access Control Systems and Methodologies
3. Cryptography
4. Network and Telecommunications Security
5. Operating System Security
6. Program and Application Security
7. Database Security
8. Business and Management of Information Systems Security
9. Physical Security and Critical Infrastructure Protection
10. Social, Ethical and Legal Considerations

Various certification bodies are also actively offering beginner level certification in the IS field, such as CESG [4] and SANS [5] to name a few. The CESG certified professional (CCP) scheme for practitioners (entry level) is based on the BOK established by the Institute of Information Security Professionals (IISP), which consists of eight (8) main competency groups:

1. Information Security Management
2. Information Risk Management
3. Implementing Secure Systems
4. Information Assurance Methodologies and Testing
5. Operational Security Management
6. Incident Management
7. Audit, Assurance and Review
8. Business Continuity Management

On the other hand, the SANS Institute offers an introductory level certification, which is the GIAC Information Security Fundamentals (GISF). It covers nine (9) domains that fit the task of security administration. The domains are:

1. Security Policy and Procedures
2. Configuration Management and Change Control
3. Cryptography Fundamentals
4. Networking Foundations
5. Networking Security
6. Data Protection
7. Systems Security
8. Information Security Principles and Risk Management
9. Authentication, Authorization, Accountability

Based on the BOK extracted from the Standard, and research works and certification programs from CESG and SANS mentioned above, a comparison of BOK for beginner-level IS practitioners is tabulated in Table 1. The IS domains from ISO/IEC 27001 serve as a baseline.

	IS Domain (ISO 27001)	Common BOK for IS (research papers)	CESG (CCP Accreditor Role - Practitioner Level)	GIAC Info Sec Fundamental (GISF)
1.	Risk management	√	√	√
2.	IS policy	√	√	√
3.	Organization of IS	√	√	√
4.	HR security	√	√	√
5.	Asset management	√	√	√
6.	Access control	√	√	√
7.	Cryptography	√	-	√
8.	Physical and environmental security	√	√	√
9.	Operations security	√	√	√
10.	Communications security	√	√	√
11.	System acquisition, development and maintenance	√	√	√
12.	Supplier relationships	-	√	-
13.	Incident management	√	√	√
14.	Business continuity	√	√	√
15.	Compliance	√	√	√

Table 1: Comparison of Sampled IS BOK with ISO/IEC 27001

Analysis

From the comparison data in Table 1 it is observed that 13 out of 15 or 87% of the IS domains in the ISO/IEC 27001 Standard can be mapped with the findings from research papers and BOK for CESG and SANS certification programs. CESG certification for the practitioner level does not cover cryptography in its BOK. On the other hand, neither research papers nor GIAC or GESF includes the supplier relationship domain in their BOK. This observation could mean that the knowledge regarding supplier relationships and cryptography is not for beginner-level IS practitioners. This observation may also be due to limited resources at the time this article was written, which restricts an in-depth comparison, for example including the depth of coverage of each domain in detail.

Conclusion

The ISO/IEC 27001 Standard requirement states that only competent IS practitioners should be responsible for ensuring the confidentiality, integrity and availability of information in an organization. In order to measure competency levels, a baseline that defines the knowledge, skills and abilities of IS practitioners must be developed. As a start, measurement can be done by having a common BOK for the IS field. Besides, beginner-level certification programs can also be developed to equip IS practitioners with foundation knowledge and skill sets to assist with protecting an organization.

References

1. Bishop, M., & Engle, S. (2006, June). The software assurance CBK and university curricula. In Proceedings of the 10th Colloquium for Information Systems Security Education.

2. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

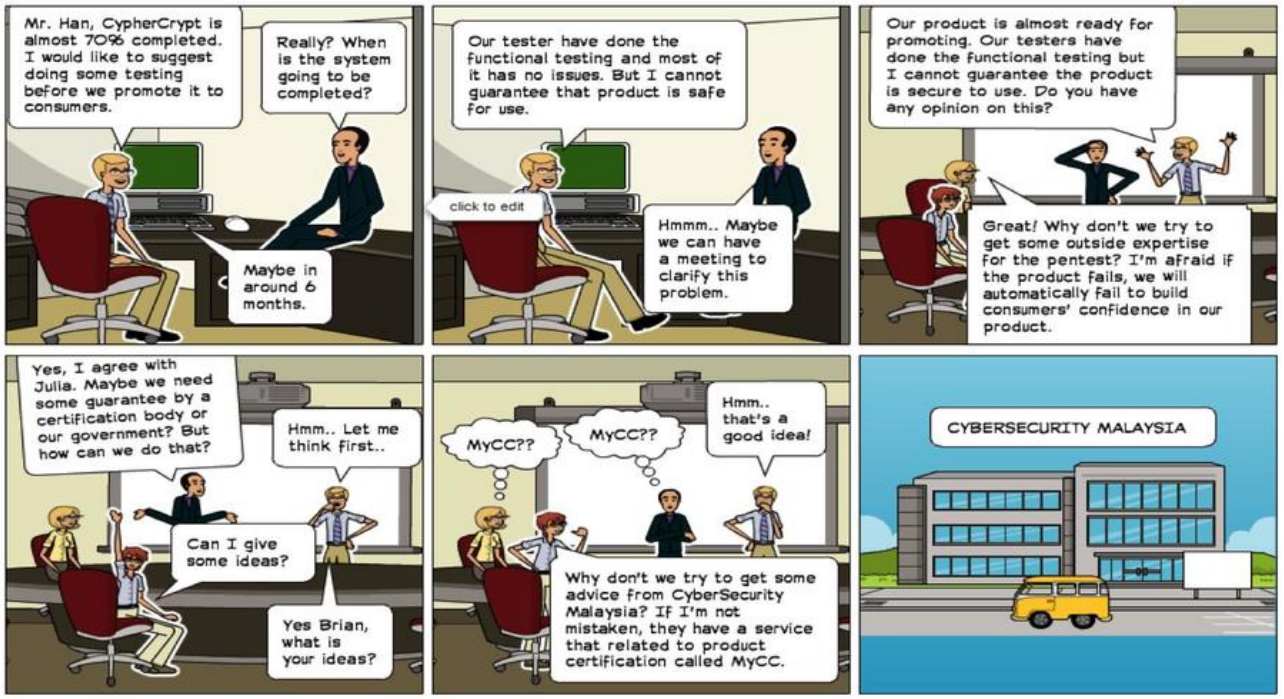
3. Theoharidou, M., & Gritzalis, D. (2007). Common body of knowledge for information security. Security & Privacy, IEEE, 5(2), 64-67.

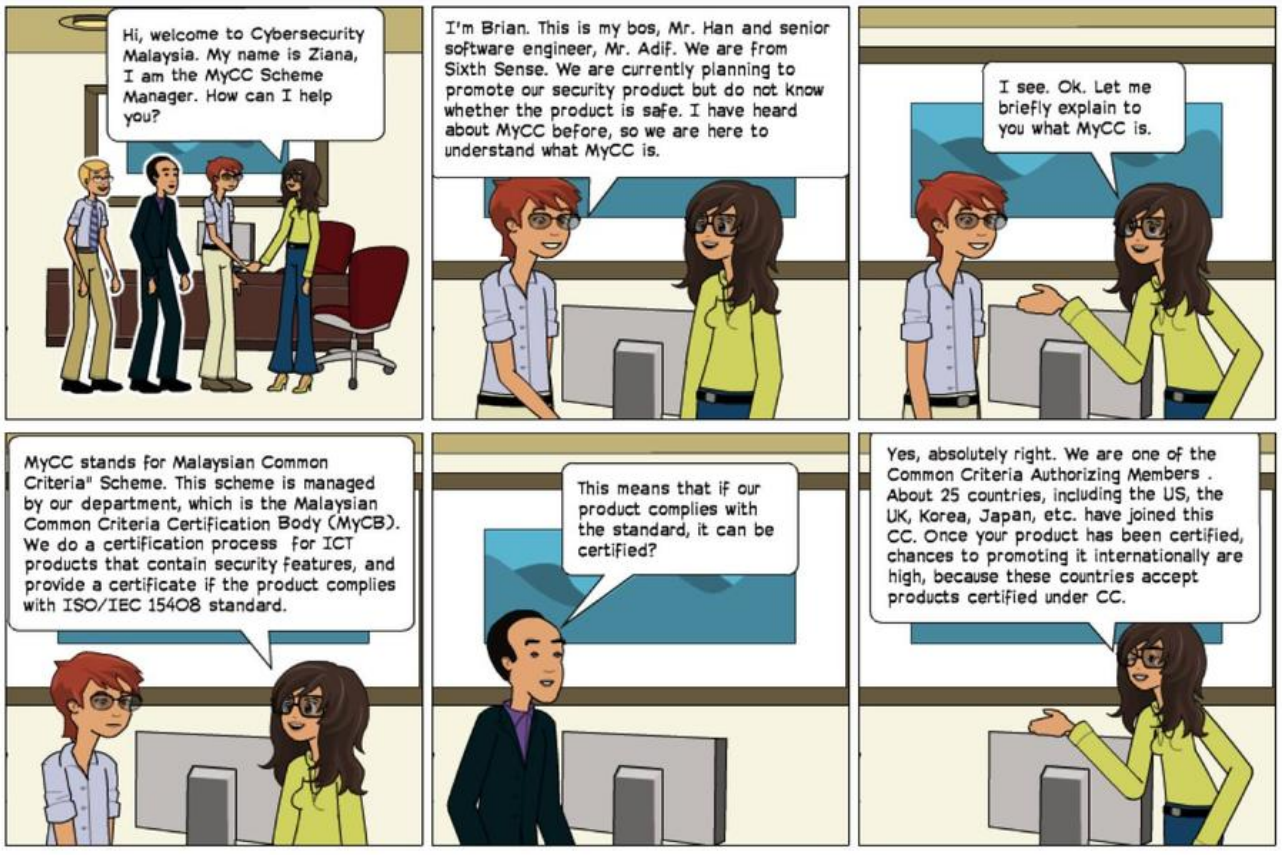
4. CESG (2014, April). Application Guidance CCP Accreditor Role, Practitioner level.

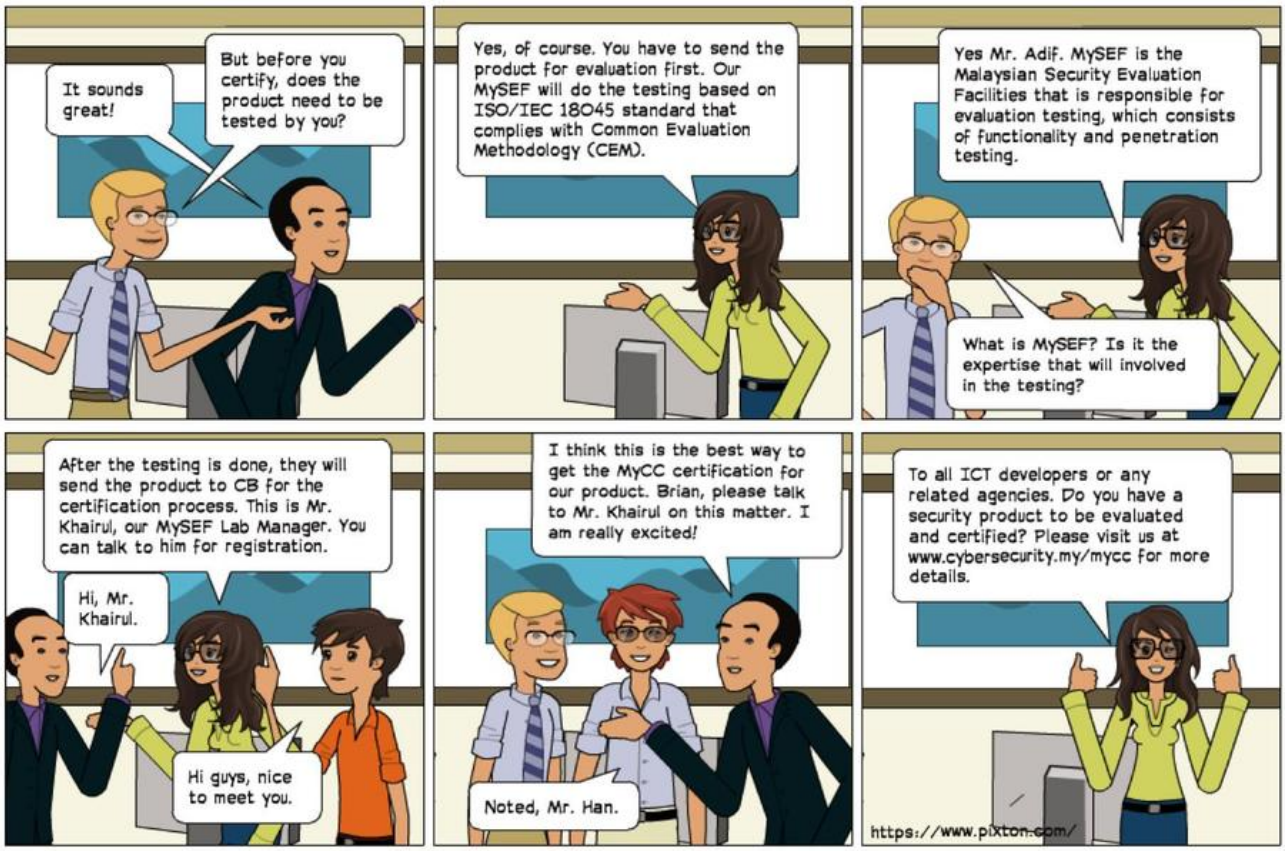
5. GIAC Information Security Fundamentals (GISF) http://www.giac.org/certification/information-security-fundamentals-gisf

ICT Product Evaluated and Certified? Go for MyCC!

By | Nur Shazwani bt Mohd Zakaria







Securing Your Online Gaming Experience

By | Muhamad Faeez Bin Pauzi, Nor Safwan Amirul Bin Salleh

Introduction

The popularity of online gaming has increased tremendously over the past few years. With the rising numbers of Internet users, the amount of games, gamers, sponsors and tournaments is by far different from what it was before. Playing games is now considered a career similar to sports, or e-Sports to be exact, with competitive gaming tournaments held around the world.

Figure 1: Gaming tournaments are now held in stadiums or arenas instead of cyber cafes [1]

The most incredible outcome of this phenomenon may be the sums of prize pools collected, especially from crowd funding programs. Last year, the fifth edition of 'The International,' a world championship of the computer game Dota 2 broke the record when the prize pool reached over US$18 million.

Figure 2: Prize pool for The International 5 will produce an instant millionaire [2]

However, as amazing as it seems, it also means that online transactions involving money for online gaming are widely used nowadays, especially to purchase in-game items. A gaming account will normally have an inventory in which a user can keep in-game items. Those with extra money on hand will have inventories full of valuable items that can be sold for real money.

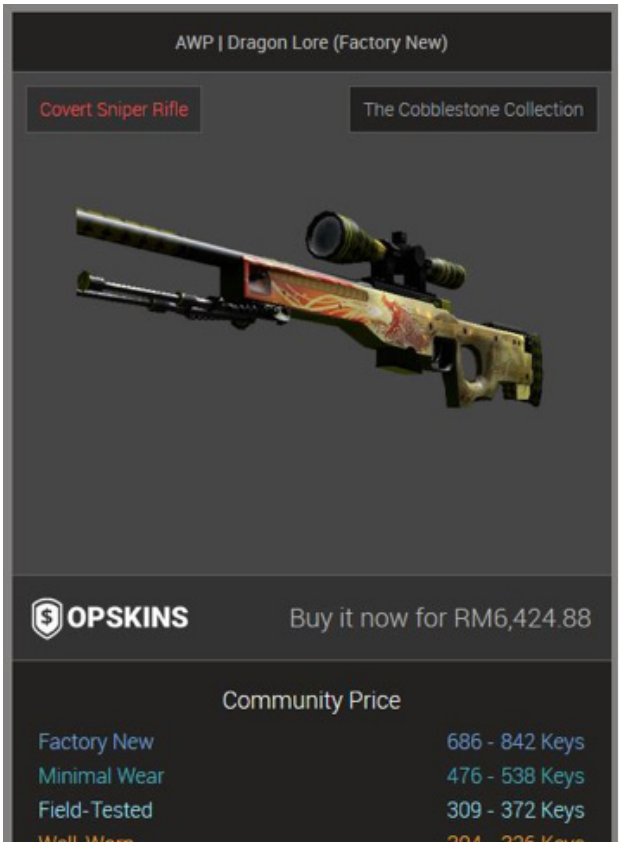


Figure 3: Example of in-game item for a CSGO game [3]

This will inevitably attract cyber criminals to obtain user account credentials so they can steal users' in-game items or overtake the whole account. The following are a few basic steps and some good online habits to keep in mind to prevent cyber criminals from ruining your online gaming experience.

1. SECURE YOUR HOME NETWORK

Your home network is the best place to start, since many devices can be connected to it. This is to prevent devices with infected malware from spreading the malware or gaining access to your computer using your home network. Make sure your Wi-Fi network is encrypted by

identifying it using SSID and a password to connect to your home network. You also need to use the strongest security level for your router, such as WPA2 or WPA [4].

A router normally has many default settings that are set by the vendors, which are publicly available on the Internet for an easier setup process. Unfortunately, this could also make your router more vulnerable to unauthorized access. Always change the default IP address and default log-in password for your router to prevent unauthorized access to your router's web interface. In addition, turn off remote access-related features so attackers cannot have remote access and always update the router's firmware with the latest patch or update.

2. INSTALL ANTIVIRUS AND THE LATEST UPDATES

Gaming is deemed a download-heavy activity, since you need to have installer files, the latest patches, anti-cheats and sometimes third-party modifications on a computer to play games [5]. It is possible for you to download a malicious file that could compromise your computer, especially when you are downloading files from unknown or unfamiliar websites.

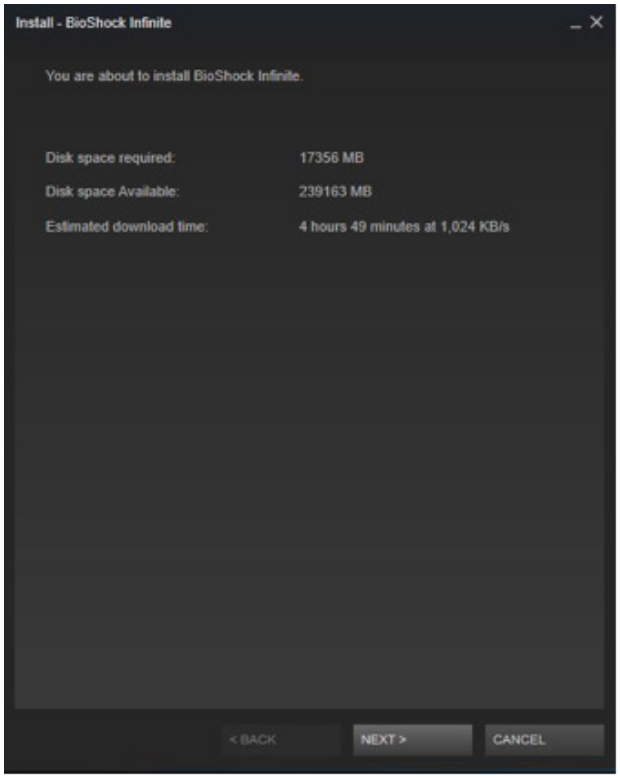


Figure 4: Installing a game using Steam, a well-known online game platform

Using an antivirus software will provide another layer of protection for your computer. Most antivirus programs have a real-time scanner that will actively scan files as they enter your computer. If it detects an infected file or program it will delete or move it to a quarantine folder, thus preventing it from interacting with the rest of the computer.

Antivirus will also protect your computer from other threats, such as clicking on suspicious links or attachments in emails and visiting untrustworthy websites. This is normally done by blocking the user from opening the website/ attachment or prompting a warning for the user before continuing.

3. EDUCATE YOURSELF ABOUT PHISHING SCAMS

Phishing will always be a common threat to gamers. Knowing how phishing is done can stop you from being one of the victims of this scamming technique. Phishing is an attempt by attackers to acquire personal user information like usernames, passwords and credit card numbers using various tricks.

Phishers may try to trick you into giving away your personal information via emails, phone calls, text messages and even Internet chat rooms. There are also cases where phishers will attempt to fool you into installing a malicious program, known as spyware, which can track and record the information you enter into your computer. The most common types of phishing scams related to gaming are links that redirect to forged websites, suspicious emails requesting you to update your account and malicious websites [6].

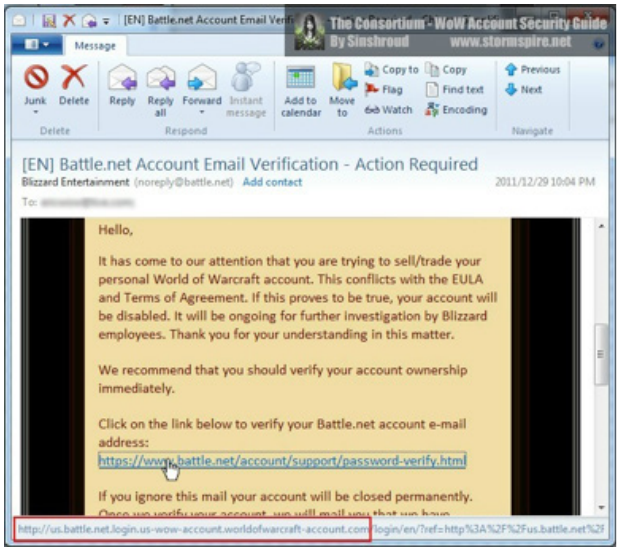


Figure 5: Scammers making use of hyperlinks to hide fake links [7]

With knowledge, an antivirus and a bit of scepticism, these sly tricks by trickster can be avoided. Try to spend some time educating yourself about the latest phishing techniques.

Victims normally share their experiences on forums or websites.

Always think twice before responding to suspicious emails or downloading attachments within. Never give out any personal information via email, social media platforms, text messages or instant messages. Last but not least, instead of clicking on the link, go to your web browser and type in the website's URL [6].

4. USE A STRONG PASSWORD

A password is like a digital key to unlock your gaming account. In order to protect it from attackers, you need to create a password that is easy to remember and at the same time strong and hard to guess. In case a user's account gets hacked, people would think that the person responsible is a great hacker. Too bad nobody bothers to consider the strength or complexity of the password for the hacked account.

Always ensure that you are using strong and unique passwords for your accounts, which include your gaming, social and online banking accounts. This will prevent attackers from gaining access to all your accounts if any one of them is hacked. Be extra cautious with your email account password, because if attackers get access to it, they could use the "forgot login" function to reset the password for any of the accounts connected to that email address [8].

A number of golden rules for creating a smart and strong password are as follows:

- Length is very important. Generally go for a minimum of 12 characters [9].
- Include numbers, symbols, and capital and lower-case letters.
- Do not use obvious dictionary words and combinations of dictionary words such as "password."
- Make the password personal to remember it easily, but make sure that "personal" information is not available online.
- Change the password periodically, for example once every six months.

References

1. HLTV.org, ESL One Cologne 2015 – Day 4. Retrived from http://www.hltv.org/gallery/view/48807 on 17 September 2015.

2. Dota 2, The International Compendium. Retrived from http://www.dota2.com/international/compendium/ on 17 September 2015.

3. CSGO Analyst, AWP | Dragon Lore (Factory New). Retrieved from http://csgo.steamanalyst.com/id/120615/ on 17 September 2015.

4. Dong Ngo, Home networking explained, part 6: Keep your network secure. Retrieved from http://www.cnet.com/how-to/home-networking-explained-part-6-keep-your-network-secure/ on 17 September 2015.

5. Joel Lee, The Worst Security & Malware Threats for Online Gamers. Retrived from www.makeuseof.com/tag/security-malware-threats-online-gamers-aware/ on 17 September 2015.

6. Nadia_Kovacs, How To Protect Yourself From Phishing Scams. Retrived from https://community.norton.com/en/blogs/norton-protection-blog/how-protect-yourself-phishing-scams on 17 September 2015.

7. Sinshroud, WoW Account Maximum Security Guide. Retrived from http://stormspire.net/consortium-quality-guides/4614-wow-account-maximum-security-guide.html on 17 September 2015.

8. David Jacoby, False Perceptions of IT Security: Passwords. Retrieved from https://blog.kaspersky.com/false-perception-of-it-security-passwords/7036/ on 20 September 2015.

9. Chris Hoffman, How to Create a Strong Password (and Remember It). Retrieved from http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/ on 20 September 2015.

A Picture is Worth a Thousand Words – Investigating Images

By | Noor Azwa Azreen Binti Abd Aziz

Introduction

In the past there was a saying, "what you see is what you get." However, as humans evolve, the way they see and interpret images changes as well. In an online investigation, an image seen with the naked eye is just the "tip of the iceberg." Investigators need to dig deeper by evaluating the image and searching for clues both found on the surface and also hidden in plain sight. This is because online images may contain valuable and essential information. Furthermore, the evidence that can be found in an image may potentially lead to other evidence in a case investigation or even directly to the source of the image. Investigators should take to heart that 'a picture is really worth a thousand words.'

Cross-Examining The Image Itself

Before using online tools or resources to investigate an image, every aspect of the image itself should be cross-examined to assist with identifying individuals, locations and properties that may be relevant to an investigation. Investigators should assess the image to determine whether it is believable or not. Then they ought to find clues they can extract and explain from the picture before drawing a conclusion. It is also important for investigators to understand the inner thoughts of the person who captured the image. Nonetheless, investigators need to additionally learn to anticipate and detect inaccuracies or misleading features of an image.

Image Search

During an investigation involving uploaded digital imagery, investigators need to consider the following matters:

i. How are online images categorized and tagged?

ii. Where are specific images likely to be located?

iii. What are the images likely to contain?

iv. Who has uploaded the images?

v. For what purpose were the images uploaded?

vi. How will the above factors affect which online tools and techniques are probably the most effective in locating specific images?

Investigators must have knowledge and skills for researching images online as well as searching information embedded in images. In addition, investigators need to know and understand the tools available for image searching.

Image Tagging

Images can be categorised in numerous ways depending on the nature of the website to which they were uploaded. Image tagging is an act of embedding information pertaining to an image into the image file itself. The information may include technical details, copyright information, keywords, dates, full descriptions and the photographer's details. Traditionally, this kind of information is stored with the image in a database, enabling users to search, retrieve and use the image based on its metadata.

People often use the same photo as a profile picture for different social networks. In this regard, investigators could do reverse image searches on sites like TinEye and Google Images to help identify linked accounts. Facial recognition technology is also widely used by sites such as Facebook, whereby the facial recognition software "Face" serves to locate images of people from numerous Web-based databases.

Locating Images

It is possible to locate images in several areas of the Internet, including the following:

i. The surface Web via regular search engines.

ii. The deep Web, which can only be done by searching the site directly.

iii. Social media sites, such as Digg and Reddit may group images into topics relevant to a

particular subject. Investigators will have to search by topic or subject to get the image.

iv. Some images on social network sites like Facebook, Myspace, Friendster and Bebo can be located depending on the user's privacy settings in relation to their uploaded images.

Creative Searching

Images can have various meanings, depending on what the site owner intended. Many images are tagged only by date, some by name or location, some are parts of series, while others have no names. In locating a specific image, investigators need to know exactly what they are looking for; they also need to be creative with their searching methods, such as the use of keywords and relevant searching tools. Filters should be removed during an investigation as the keywords may have double meanings or reveal images that are not relevant to the investigation.

Ownership

It is not simple to find the source of an image because uploaded images can be altered, redistributed, tagged and downloaded by others online due to the lack or absence of restrictions. At times, an online image does not even represent the actual person.

Thus, investigators must carefully examine the image to ensure that it is genuine and not a malicious copy. Exchangeable Image File format (EXIF data) can also be useful to assist investigators in their examinations. It is also important for investigators to download the image separately from the webpage, as the image may be removed from the server and disappear from the downloaded webpage since it is not an integral part of the webpage.

Google Images

Through Google Images, keywords are entered into the search box and visual results are returned from surface websites based on the frequency, location, and relevance of keywords. Image results can be refined by size, colour, type, and time by clicking on the Search Tools link at the top of the page and selecting a relevant link. The Advanced Image Search section of Google images allows users to specify image search parameters based on aspect ratio, keywords, colour, file format, size and several other specifications.

Google Image Search

Google image search has a feature with which a user can either upload an image to search or choose a Uniform Resource Locator (URL) that specifies an image by clicking the camera button. Google image works similar to TinEye but appears to focus more on the overall characteristics of the image on which to base its results. The original image will be found, as well as other websites containing this image.

TinEye

TinEye is owned by Idée and based in Toronto, Canada. TinEye is identified as the world's first reverse image search engine. It developed an image search technology that looks at the patterns and pixels of images and videos to make each image or frame searchable by colour, similarity or exact duplicate. Users can initiate a search using TinEye in one of two ways: either by uploading an image or by entering the location of an image that is already online using the URL. The search results are based on the Best Match, the Most Changed, the Biggest Image, the Newest, the Oldest and the Most Changed. Investigators can determine whether images have been "Photoshopped" or otherwise altered by a third party. Beneath each search result are two further refining options, Compare and Link. The Compare link provides a comparison between the initially submitted image and the selected result. In addition, the Switch button allows switching back and forth between the two images to highlight any differences.

Flikr

Flickr was established in 2004 and is a global network owned by Yahoo. With over 6 billion images, Flickr is a great intelligence tool, and users are not required to create a Yahoo account to search images and profiles. Images can place an individual in a specific location at a specific time, often with specific people. Geo-tagged images can provide additional confirmation pertaining to geographical location, and EXIF Data can add further details regarding the images. An important service that goes hand-in-hand with Flickr is Creative Commons, located at http://creativecommons.org. An online method of copyrighting all media types, the Creative Commons licence allows users to specify the viewing, editing, distribution and reproduction

terms of original materials that are displayed online.

Cooliris

Cooliris was founded in 2006 by Austin Shoemaker and Soujanya Bhumkar. Cooliris is a highly innovative image sharing and search tool. It is an Apple-based application that combines images from Instagram, Flickr, Picasa, Photobucket, Facebook and many other image sharing portals.

Examining Exif Data

EXIF Data stores interchange information on image files, particularly those with the .jpg file extension. It contains information regarding the origin of an image captured using a digital camera or any other relevant type of imaging device. To access the EXIF Data, the image must first be downloaded to one's computer hard drive. Having downloaded the image to a computer hard drive, investigators need to access the image properties to obtain the EXIF Data. EXIF Data provides general information about the image and further details that contain very specific information regarding the construction and creation of the image.

Image Verification

Investigators need to verify the authenticity of an image and whether it was altered or distorted by anyone. Investigators must capture a screenshot of the image and search the image using TinEye, Google Image or ImageMagick. Then they should look for the same image on other sites to identify whether any alterations have been made, such as logos or names added to buildings, office locations, products, etc. It is necessary for investigators to also determine whether a person in a particular picture is really in the picture itself or they were added. Investigators can also determine whether the picture was altered or "Photoshopped" by using http://www.pskiller.com/. Besides, investigators could also examine any EXIF data for the image, if any.

Conclusion

Investigators should never take for granted the worth of an image because "a picture is really worth a thousand words." Images can provide valuable information in numerous ways, by offering clues that are hidden in plain sight or that require a closer look behind the scenes of an image. Therefore, image uses are crucial to exhibiting the progress of an investigation.

References

1. Toddington International Inc., Investigating Images, https://toddington.com/lesson/usint-03-topic-13/, access on 27 April 2015.

2. Hill, Dr. Stephen from Snowdrop Consulting Ltd, Online Investigations, http://www.acfe.com/uploadedFiles/ACFE_Website/Content/european/Course_Materials/2013/ppt/4B_Stephen-Hill.pdf, downloaded on 24 April 2015.

3. Jake van der Lan, 2013. A Guide to Internet Investigation, http://www.nasaa.org/wp-content/uploads/2012/09/GuideToInternetInvestigations-v-1-9-5-December2013.pdf, downloaded on 28 April 2015.

Top Five Common Penetration Tools

By | Nur Sharifah Idayu Mat Roh, Noraziah Anini Mohd Rashid

Introduction

A penetration test, sometimes called a pentest, is an attack on a computer system/machine in search of security weaknesses to gain access to important information in a computer/machine. Basically, a penetration tester or pentester gathers information to identify the targeted machine and review the information collected to plan a real attack. This way, the pentester can identify existing vulnerabilities or if present defence is sufficient. Several tools are available nowadays for pentesters to carry out penetration testing.

1. Wireshark

Wireshark (known as Ethereal) is a fantastic open source network protocol analyser for Unix and Windows. It allows examining data from a live network or from a file captured on disk. Users can interactively browse the capture data, and view a summary and detailed information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds of protocols and media types. Below is an example used for password sniffing using an HTTP protocol.

STEP 1:

Open Wireshark, then capture the interface and click start.

STEP 2:

Key in the 'http' at the filter value and search for the target IP address, for example 192.168.1.13 (victim), then find the 'POST' on the HTTP protocol.

STEP 3:

Analyse the POST info and you will read the username and password of the victim web application.

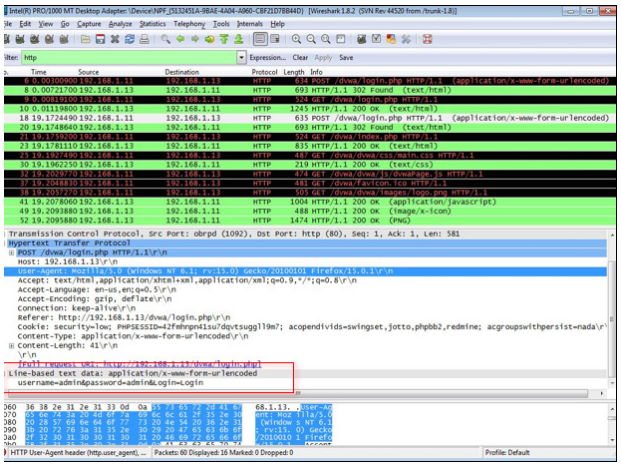


Figure 1 Password sniffing

2. SQL Inject Me

SQL Inject Me is the Exploit-Me tool used to test for SQL Injection vulnerabilities.

A malicious user can possibly view records, delete records, drop tables or gain access to the server. The tool works by submitting HTML forms and substituting the form values with strings that are representative of SQL injection attacks. Below are sample steps of how to use SQL Inject Me.

STEP 1:

Open the victim URL, e.g. http://192.168.1.13/dvwa/login.php

STEP 2:

Download and install SQL Inject Me from Firefox Mozilla add-ons. Click on Open SQL Inject Me Sidebar. A list of available forms will be displayed.

STEP 3:

Click on the loginForm menu. Choose Run all tests. Tick all elements on the form.

STEP 4:

Change the loginForm:username value to 1' OR '1'='1 and the loginForm:password value to 1' OR '1'='1 . Then click the Execute button.

Figure 2 SQL Inject Me

STEP 5:

The result will be displayed in a new tab. according to the result, there are 68 failures, meaning the web application exploitation was successful.

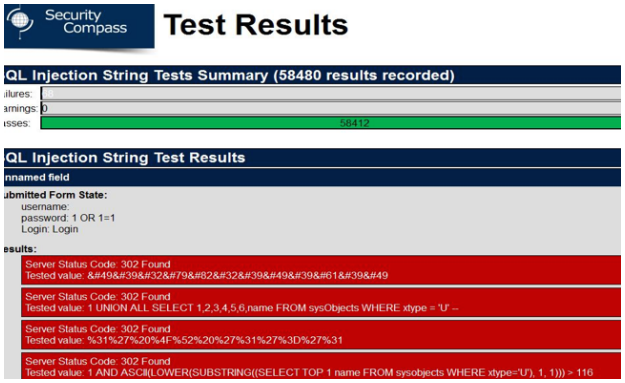


Figure 3 SQL Inject Me result

3. XSS Me (cross site scripting)

Cross Site Scripting is a method of hacking (cracking) used to change the code of a vulnerable website to include a malicious script. This website is then sent to other people to view, which causes script initialization. Detecting XSS vulnerabilities early in the development process will help protect a web application from unnecessary flaws. XSS-Me is the Exploit-Me tool used to test for reflected XSS vulnerabilities. Below are example steps on how to use XSS Me.

STEP 1:

Open the victim URL, for example http://192.168.1.13/ghost

STEP 2:

Download and install XSS me from Firefox Mozilla add-ons. Click on the Open XSS me Sidebar. A list of available forms will be displayed.

STEP 3:

Choose Run all tests. Tick all elements for the form and then click the Execute button.

Figure 4 XSS Me

STEP 4:

The result will be displayed in a new tab. According to the result, there are 11 failures, meaning the web application exploitation was successful.

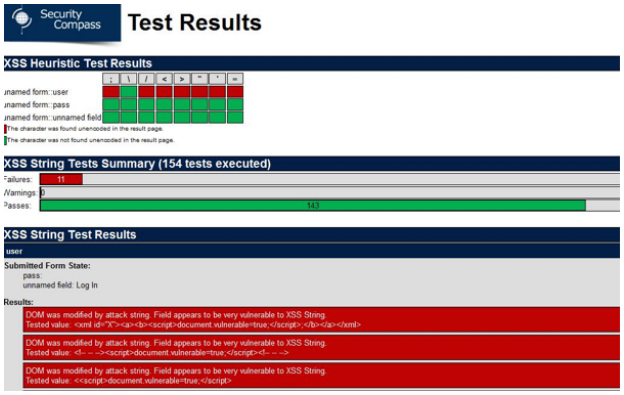


Figure 5 Result XSS me

STEP 5:

Send text-based attack scripts that exploit the interpreter in the browser, to the username and password fields on the Webconfig login page.

STEP 6:

In the username and password field, type <script>alert("TEST");</script>). Click the Login button. If the web application has an XSS vulnerability, the victim will display an alert popup.

Figure 6 Cross site scripting

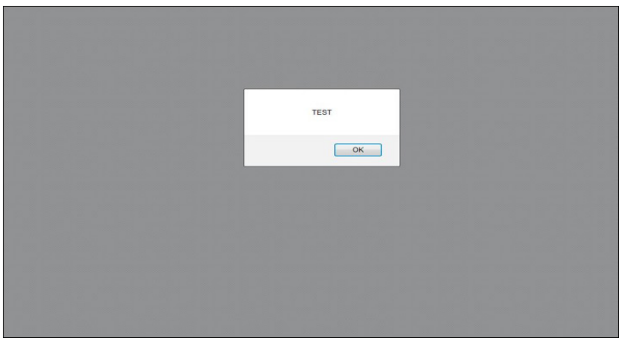


Figure 7 Successful XSS exploitation

4. Nmap (Network Mapper)

Nmap is an open source security tool for network exploitation, security scanning and auditing. Nmap is a popular tool used by penetration testers in the reconnaissance stage, which is the stage of gathering information before any real attacks are planned. Data acquired through Nmap gives the penetration tester the hosts of the targeted network, open ports, version used by the machine, and operating system and hardware characteristics of the network devices. For example, by knowing the machine's open port, the penetration tester can later use the open port to deploy attacks. There are four (4) common commands that can be used to acquire crucial information.

Disclaimer: The IP address used below is only an example for testing purposes. The actual IP address in a real environment may be different.

Command 1:

Scan a single IP address by typing nmap 192.168.1.13. The penetration tester will get the open port information and the MAC address of the targeted machine.

```
Starting Nmap 6.01 ( http://nmap.org ) at 2015-09-30
11:11 Malay Peninsula Standard Time
Nmap scan report for 192.168.1.13
Host is up (0.0000060s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:62:66:E4 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 6.54
seconds
```

Command 2:

Scan a range of IP addresses using a wildcard by typing nmap 192.168.1.*. The penetration tester will get the open port information and MAC address that is in the range of IP addresses beginning with '192.168.1.*'.

```
Starting Nmap 6.01 ( http://nmap.org ) at 2015-09-30
11:14 Malay Peninsula Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:09:5B:D7:B4:42 (Netgear)

Nmap scan report for 192.168.1.10
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.10 are closed
MAC Address: 68:5B:35:BD:89:33 (Unknown)
```

Command 3:

Scan the network by excluding the IP address from being scanned by typing nmap 192.168.1.0/24 –exclude 192.168.1.11. This command will exclude IP address 192.168.1.11 from the scanning.

```
Starting Nmap 6.01 ( http://nmap.org ) at 2015-09-30
11:20 Malay Peninsula Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:09:5B:D7:B4:42 (Netgear)

Nmap scan report for 192.168.1.10
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.10 are closed
MAC Address: 68:5B:35:BD:89:33 (Unknown)

Nmap scan report for 192.168.1.13
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:62:66:E4 (Cadmus Computer Systems)

Nmap done: 255 IP addresses (3 hosts up) scanned in
20.78 seconds
```

Command 4:

Find out if the host/network is protected by a firewall by typing nmap
–sA 192.168.1.13. Nmap will report whether the IP address is protected by a firewall by using filter/unfiltered. If the port is protected by a firewall, nmap can bypass it by using the command nmap –PN 192.168.1.13.

```
Starting Nmap 6.01 ( http://nmap.org ) at 2015-09-30
11:22 Malay Peninsula Standard Time
Nmap scan report for 192.168.1.13
Host is up (0.0034s latency).
All 1000 scanned ports on 192.168.1.13 are unfiltered
MAC Address: 08:00:27:62:66:E4 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 6.18
seconds
```

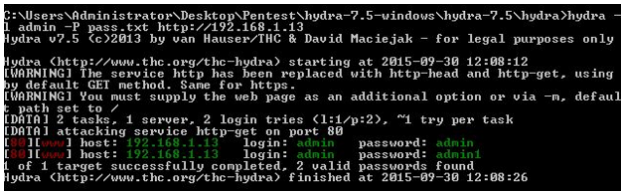
5. THC Hydra

Hydra is an online password cracking tool. This tool can perform rapid dictionary attacks against more than 50 network protocols, including telnet, ftp, https, https, smb, several databases, and many more. Hydra can use brute force on website login credential by using a list of usernames and passwords.

Disclaimer: The IP address and text files used below are only examples for testing purposes. The actual IP address and files in a real environment may be different.

Command:

Typing hydra –l admin –P pass.txt http://192.168.1.13. Brute force the website using a single username and a list of passwords. The penetration tester can also replace –l with –L to include a list of usernames instead of only one username.



Conclusion

Nowadays, there are hundreds of network penetration tools available that can be used for testing. However, it is advisable to use a suitable tool based on the testing environment criteria and multiple suitable tools to achieve firm output.

Social Engineering Experiment – Social Media

By | Ahmad Dahari Bin Jarno

Abstract

Vulnerabilities and unethical hacking have rigorously evolved from many different perspectives including Information Technology (IT) products, systems and its environments. Yet according to this evolution, it can be concluded that the biggest vulnerability is human beings themselves as users of IT products, systems and environments.

Thus, in many IT incident events, people are the weakest link as either the trigger point of attacks or as leading to the cause of problems in systems through mistakes that could be avoided. Lack of awareness, putting value to responsibility and taking into consideration further details are the less expected weaknesses of humans as IT consumers.

As such, new breeds of hackers use these new opportunities to manipulate these weaknesses of humans as IT consumers. They carry out unethical hacking activities with the objectives of bringing down target systems or looking for profit that may be beneficial in financial terms.

Hacking on Humans

According to history, hacking started around the late 1950s, when the phreaking attack entered the world of IT. This type of hacking is done through the phone by listening to a specific tone, thus allowing the user to manipulate the weakness of phone dialling capabilities just to feed their need for free phone calls. As the world of communication and IT has evolved, better technologies introduced seem to be irrelevant since attack/hacking tools and techniques are closely trailing to catch up with inventions. Nowadays, faster computing processing capabilities allow hackers to easily send attack commands to targets with the support of faster networking capabilities.

Nonetheless, even in this era of new inventions and technologies, humans have maintained their place to which hackers look for any vulnerabilities due to human mistakes and lack of awareness with IT security. Some perspectives of IT hacking tools and techniques have introduced new ways of hacking IT infrastructure through human manipulation and behavioural observations. Likewise, hacking is also known to be usable to leverage human trust for profitable income by hacking target financial profiles.

"Hacking humans," also well-known as social engineering attacks are currently under heated discussion throughout the IT hacking community. The idea is to essentially manipulate the trust and response behaviours of the target in light of the fact that sharing confidential and private information among IT users is a form of human bonding. This links to the quote "sharing is caring." Social engineering attacks can be performed directly or indirectly on targets based upon the type of information the attacker/hacker needs. The key component of a successful social engineering attack on IT users/humans is being able to gather information about the target user by replicating their exact identity through understanding the user's habits, communication attitudes and cravings/needs.

In this article, the focus of discussion is on indirect social engineering attacks through the usage of publicly available information on the Internet and the chain of information offered on social media platforms linked to target users.

Social Engineering through Social Media

Social Media platforms like Facebook (FB), Twitter (TW), Instagram (IG) and many others around the Internet are fond to IT users as places where everyone shares information, stories, life updates and many other types of information through friendship and social lifestyles. As the platforms broadly evolve from time to time, they are places where IT users keep private information. Still, some of those facts are lingering around the Internet, unfortunately, as public information.

Hackers that are highly interested in Social Engineering attack techniques targeting victims through Internet information sharing (also known as cyberstalkers) use these opportunities

to study more about their target users (victims) without the need for physical interactions. These attack techniques are known as indirect social engineering attacks. Hackers can either choose the method of sending fake, phishing emails to targets or conducting online surveys that offer high value awards (for example, vacation coupons or cash vouchers) that will attract potential victims.

Through these methods of information gathering (reconnaissance), hackers will start digging further to understand the victim's habits, favourites, life conditions (health, finances, relationships, etc.), weaknesses, points of interest, places visited and many more. The list can be miles long based on the hacker's creativity and experience with social engineering attacks. Chains of information linking various points will benefit the hackers in understanding the target victims through the relationships the victims have with friends, family members, Internet sites, social media subscriptions and many other categories of information links.

An example of a social engineering experiment is when a hacker tries to duplicate the identity of an online user who has large financial savings and yet, the user is a very frequent online shopper. The scenario here is that the hacker is planning to steal the target user's (victim) financial saving account by means of knowing crucial information about the target victim's financial credentials. In Malaysia, most culture of financial customer service providers requires simple verification of identity such as ID number, credit card number and full name. Further verification questions are mostly related to the last purchase made, where the last purchase was made and card credit payment method. For a hacker, this can easily be known by monitoring the target user's social media account (commonly Facebook) based on posts made by the victim. Through social media, hackers can also gather information such as ID number based on the user's education or work history posted online publicly.

Hackers can gather and record this type of information with great imagination and creativity in understanding online behaviour of victims as social media users.

Social Engineering Experiment

In the area of studying social engineering attacks with focus on social media platforms, several experiments or test scenarios can be performed with the intentions of the hackers' points of interest. The following is a list of interests likely relevant to hackers in carrying out social engineering attacks through social media platforms.

a. **Financial Credentials:** Hackers dig relevant information on the target user that leads to exposing their financial credentials, such as credit card number, ID, name and purchasing habits.

b. **Identity Theft:** Hackers use publicly available information to understand the target user with the objective of duplicating the target user's identity, thus using such treasured information to further exploit other persons or entities like companies.

c. **Blackmailing:** Hackers use a target user's public information that links to any relevant secret information, for instance information regarding a company's reputation. This high amount of information gathering can take months of work. Yet, at the end of the journey, the information can be beneficial in many ways, especially in terms of financial gains from blackmail methods. Some of these techniques can be applied to jeopardize any individual's reputation or status.

Continuing with the discussion on social engineering attacks using social media platforms, a hacker requires several seeds of information as preliminary components to start a social engineering attack. These can be the victim's full name, nickname, email address, phone number and other information related to the target's lifestyles including hobbies, favourite food and favourite social media platforms. In this era of fast communication and information sharing, almost all information about certain individuals is available on the Internet. With Google crawling capabilities that keep evolving to their best, more information is being shared on the Internet without the information owners knowing.

With these seeds of information, hackers will use Internet platforms, such as search engines, social media, blogs, online journals, online photo sharing, and many other online subscriptions that are publicly available in search of more information from the links to the seed information. The following are several search engines that are applicable for information crawling by focusing on given seeds of information.

a. **Google with Google Hacking Techniques** (URL: www.google.com): Google Hacking Techniques are among the most famous tricks that hackers use to search relevant information by focusing the search keywords exactly to the specific needs of the requester.

b. **Social Searcher** (URL: www.social-searcher.com): This platform allows the requester to query target user credentials by using their name/ID/nickname that links to any known social media, such as Facebook, Twitter, Google+, etc.

c. **Zuula Search** (URL: www.zuula.com) is one of the alternatives to Google as a search engine. It can perform multiple search queries on other online search engines, such as Bing, Yahoo, Gigablast, Mahalo, etc.

d. **PIPL** (URL: www.pipl.com) and **PEEKYOU** (URL: www.peekyou.com): It is possible to search individuals by querying their full name, username, phone number or location.

A social engineering attack commences with the retrieval of relevant query outputs from these relevant search engines. For example here, an attacker makes the assumption that the target victim is using his/her full name that links to a company name. Subsequently, from the company bulletin board, it is known that the victim has a Twitter account and uses a nickname as tagged by his/her colleagues. From this information, it is known that some of the family members tag the same Twitter ID that links to a Facebook account owned by his/her family members. Unfortunately, the target's family members have publicly shared information about his/her hometown, current events relative to the family, family members' names and many more.

In this way, crucial, private information can be gathered from these resources and can be manipulated in unethical ways by hackers. The following is a list of information that may be manipulated for unethical actions that are beneficial to hackers/attackers. Any type of information that may seem irrelevant to an individual can be treasure for an hacker/attacker.

No.	Information Types:	Information Manipulations:
A.	Posts and pictures shared on social media of new items purchased, etc.	The attacker can use this information to pretend to be bank customer service calling the victim to verify credit card information. From there, the attacker can gather the victim's financial credentials, such as 16 digit credit card number with its 3 digit authorization code.
B.	Information about family members, family credentials and relatives of the victim.	The attacker can perform identity theft of an individual by knowing crucial information about his/her family members, daily activities and many more. This can also lead to blackmailing or kidnapping.
C.	Information about a company, lifestyle, popularity, public relations, etc.	The attacker can use this information as blackmail input to jeopardize the individual's reputation with the objectives of gaining financial credit or benefitting another entity/company.

Table 1: Information that is crucial for hackers/attackers

On this note, there are no limits to hackers/attackers manipulating information from any point of the link that seems irrelevant to the victim. From a hacker's point of view, this information is like seeds to their treasure. Thus, from many perspectives it is ultimately worthy to unethical hackers, especially for financial gains.

Figure 1 shows areas of information that are useful for social engineering attackers.

Figure 1: Example of information in Facebook (Hacker Interest)

Figure 2 shows a basic information search using Google hacking techniques. This is one of the favourite search engines used by hackers for Social Engineering attacks.

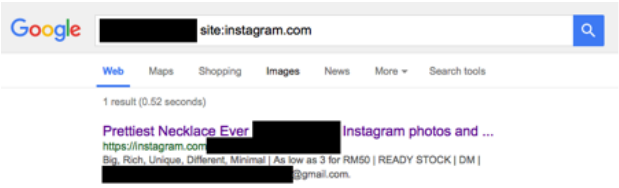


Figure 2: Screenshot of Google findings in Social Engineering hacking

Prevention is BETTER than Cure!

It is often said that prevention is better than cure. Even a single piece of information flowing through the Internet without the owner's knowledge or authorization could be a fortune for a hacker/attacker to gain from. Information links to an individual can be so valuable to them that hackers/attackers are likely to manipulate this information to gain some profit from it.

As IT users, the responsibility to manage our information is crucial in ensuring clear segregation and classification of information types is in place with clear understanding of managing this information based on needs. The first step that IT users can take is not to stay away from the current trends of social media platforms but rather to manage them accordingly with the best understanding of information management. By understanding the risks of information disclosure, users must take responsibility with each information disclosure and segregate information based on classifications. This way, users can be active on social media platforms with less worries by following certain rules of communication with limitations to information disclosure.

IT security perspectives and features have already been implemented in most social media platforms like Facebook, Twitter and Instagram. Under the preference setting, users can set certain access to posts, pictures, tagging and other relevant information, to control public access to viewing the information. Another perspective of security in access control is limiting access to information by first reviewing it before posting it, for instance picture tagging, information sharing or post publishing.

As for online journals, blogs and entities that post credential information relatively private to a certain extent, it is recommended to contact the person in charge of the portals to disclose all information. If any issues arise in communicating with these individuals, it is recommend to contact close authorities in Malaysia like the Malaysia Communication & Multimedia Commission and also MyCERT at CyberSecurity Malaysia.

Conclusion

Having great platforms of communication and information sharing such as social media (Facebook, Twitter, Instagram, etc.) allows IT users and communities to share information without the limitations of physical boundaries and geo-location conditions. When IT security perspectives are taken into consideration due to problems with information disclosure, privacy and risks of human threats, many entities and individuals are concerned about the future of information sharing and its management while projecting data protection.

Therefore, in ensuring the information flows correctly and is respectively managed with low risk, awareness of social engineering threats and broadcasts should be offered accordingly to the public. Likewise, continues improvement in online platforms will make the public more confident and assured with using social media platforms. In conclusion, all sectors of ICT infrastructure and culture should have all hands on deck in mitigating the risks of social engineering attacks.

References

1. *Hacking the Human – Social Engineering Techniques and Security Countermeasures, by Ian Mann, 2008, published by Gower Publishing Limited, Gower House.*

2. *Kali Linux Social Engineering, by Rahul Singh Patel, Dec 2013, published by Packt Publishing Ltd. Livery Place.*

3. *Low Tech Hacking – Street Smarts for Security Professionals, by Jack Wiles, Dr, Terry Gudaitis, Jennifer Jabbusch, Russ Rogers and Sean Lowther (2012), published by Syngress.*

4. *No Tech Hacking – A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing, by Jonny Long, 2008, published by Syngress.*

5. *Social Engineering – Art of Human Hacking, by Christopher Handnagy, 2011, published by Wiley Inc.*

6. *Google Hacking – Cara baru Melakukan Hacking Tanpa Tools, by Efvy Zam Kerinci, 2007, published by Neomedia Press.*

7. *vii. Google Power – Unleash the Full Potential of Google, by Chris Sherman, 2005, published by Mc. Graw Hill.*

Securing The Cyber Space Through International Collaboration of Computer Emergency Response Teams

By | Mohd Shamir Hashim

Project Background

The Internet has changed modern life. Information sharing has never been easier and the accelerated data transfer flow has made modern society reliant on the Internet in daily life. Individuals and organizations are now very dependent on the Internet for information sharing, daily operations and business, and research.

However, this also attracts parties with ill intentions or cyber criminals to conduct illegal activities online. This is because the Internet provides anonymity and a borderless landscape, which has proven to be a great hurdle for law enforcement agencies in conducting investigations on such crimes.

Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) are entities that provide services for ensuring that cyber space is safe by resolving their respective constituencies' computer security incidents or cyber incidents. Apart from mitigating cyber incidents, these entities also offer cyber security training and awareness.

Since the Internet does not conform to the physical boundaries of countries nor geographical factors, cybercrimes can be easily committed across borders and outside of any particular law enforcement jurisdiction. Therefore, as the point of contact for cyber incidents, CERTs find it beneficial to form collaborations beyond their respective constituencies to solve incidents.

International Information Security Collaborations

The European Union Agency for Network and Information Security (ENISA) is an organization working for the European Union (EU) institutions and member states, which responds to cyber security problems in the EU. This collaboration strives to achieve a high and effective network and information security level for the benefit of EU citizens, consumers, businesses and public sectors. Another CERT collaboration in Europe is TF-CSIRT, which is a task force that promotes collaboration and coordination among the CERTs in Europe and neighbouring regions.

For the Asia region, a similar collaboration is the Asia Pacific Computer Emergency Response Team (APCERT). This is a group of CERTs from various Asia Pacific countries that work together to ensure Internet security in the region based on genuine information sharing, trust and cooperation.

At the global level, the Forum of Incident Response and Security Teams (FIRST) brings together a wide variety of security and incident response teams from the government, commercial and academic sectors. This is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

Organization of Islamic Cooperation – Computer Emergency Response Team

Establishment

The Organization of Islamic Cooperation (OIC) is the second largest inter- governmental organization after the United Nations and has a membership of 57 states from across four continents. The organization oversees the interests of Muslim communities in the spirit of promoting international peace and harmony among various people worldwide. With the cyber environment becoming a vital part of communities, some member states are voicing out the need to establish a CERT collaboration using the OIC platform. Therefore, during an annual meeting of the Islamic Development Bank (IDB) Board of Governors in Putrajaya, Malaysia in June 2003, the idea was tabled and accepted. Malaysia was assigned to lead a task force consisting of leading OIC member states to establish the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT).

In 2008, during the 35th OIC Session of the Council of Foreign Ministers held in Kampala, Uganda, a resolution was put forward expressing concern that Internet technologies

and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security. Thus, in realizing that the nature of the Internet and cyber space is not confined to the physical boundaries of a country, the OIC agreed on the establishment of a cross-border collaboration to share information and initiatives to counter cyber threats.

The OIC-CERT is governed by a seven (7)-member Steering Committee (SC) consisting of a Chair and Secretariat. The SC, elected by members periodically during the Annual General Meeting, is responsible for ensuring that OIC-CERT activities are in line with its objectives of securing the cyber environment.

Activities for the Information Security Community

1. **Strengthening relationships amongst CERTs in the OIC member countries and others**

   OIC-CERT uses the OIC platform to leverage on international collaboration. Although the collaboration is OIC-centric and is based on the spirit of resolving to form the OIC-CERT that states that cyber space is not confined by countries' borders, OIC-CERT established cooperation ties with other similar organizations such as APCERT and AfricaCERT. Such cooperation, as stated in the Memorandum of Understandings, has expanded the reach of the respective collaborative platforms and their regional and global members.

   In addition, OIC-CERT is also open to non-OIC state members and industries. Such cooperation allows these organizations to exchange expertise, and with the convergence of knowledge and technologies to support cyber security enhancement in the respective regions. This provides various benefits to communities, such as improved mitigation of cyber threats to keep the cyber environment safe.

2. **Encouraging experience and information sharing**

   OIC-CERT conducts information security seminars and forums that involve experts from the member states and industries. With the pool of resources available, such events offer societies valuable knowledge, experience and awareness of cyber security. This can be seen at the OIC-CERT Annual Conference, where large numbers of information security professionals from all over the world gather and participate in the seminars, workshops and forums. Events like this serve as platforms for multinational professionals to meet and provide international exposure and access mainly to local professionals from the hosting countries.

3. **Cultivating and fostering education and outreach ICT security programs**

   Capacity building is one of the major reasons for CERT collaboration. Members share knowledge and technologies to strengthen each other's capabilities in order to maintain a secure cyber environment. This is done through workshops and training sessions. OIC-CERT conducts technical and regional workshops as part of its capacity-building initiatives. These activities provide members with the necessary knowledge from setting up and operating CERTs to managing network security. Such workshop was organized and hosted in Brunei, with participants from four continents attending. As a result of this workshop, the participating member states experienced a boost in their CERT capability.

   OIC-CERT regional workshops focus on subject matter requested by the respective regions. Each region may have different priorities in managing cyber threats, thus focus will differ. These workshops have been conducted in the Middle East hosted by Egypt, in Africa hosted by Morocco and in Asia hosted by Malaysia. The workshops are co-financed by the hosting countries and the Islamic Development Bank.

   In order to utilize the capabilities gained from the workshops, OIC-CERT conducts annual cyber drills to test members' knowledge of responding to inter-border cyber incidents. The drills allow participating members to face realistic incidents, test out internal procedures, exercise technical capabilities and analyse cyber threats. It also provides the opportunity to gauge members' readiness levels in mitigating emerging cyber threats to avoid serious impact on member countries. Apart from OIC-CERT members, collaborative partners are also invited to participate, including APCERT and AfricaCERT members.

   From the drills, analyses are done to identify areas of weakness for consideration in OIC-CERT training programs.

To further enhance the capacity building program, OIC-CERT is embarking on a professional certification program to provide cyber security professionals with the right knowledge, skills, abilities and experience. The objective of this program is to create a world-class competent workforce in cyber security and to promote the development of cyber security professional programs.

4. **Promoting collaborative technology research, development and innovation in the ICT security fields**

   In addition to training, OIC-CERT is implementing collaborative projects among members. One such project is the Malware Research and Coordination Facility led by Malaysia. This project provides members access to necessary data for research on malicious computer codes. This will be used to develop eradication solutions and provide an overview of the community's malware infection landscape. This is a public-private cooperation project because technology and knowledge from the industry are needed in seeking appropriate solutions for malware eradication. The government of Malaysia supports the initial project cost and participating members provide the operating costs in subsequent years.

Challenges

Support for OIC-CERT has grown. Starting with only six (6) member states in 2009, the collaboration has increased to 21 member states today. However, considering that OIC has 57 member states, OIC-CERT members only represent 34% of the OIC community. Factors contributing to this may be:

- The political turmoil faced by some member countries that have their governments focusing on critical matters such as defence and physical security rather than ICT requirements;
- The lower economic status of some member countries that requires them to prioritize basic needs like physical infrastructures, food and clean water;
- Lack of governmental support to join the OIC-CERT o wing to the lack of awareness of the importance of cyber security or for other political reasons.

Another main challenge is regarding the funds required to implement the activities. As of now, the hosting OIC-CERT members provide funds to cover the venue and local logistics for the event. The IDB also provides some funding to support selected activities. However, a better solution for obtaining funds is required to avoid dependence on contributors.

Conclusion

OIC-CERT is an international collaborative platform for cyber incident mitigation, which is open to any suitable CERT, whether supported and/or funded by the government, the private sector or a combination thereof that is interested in sharing the objectives of OIC-CERT. This platform promotes good values and best practices to the Internet community through awareness and capacity building programs. Activities conducted to date have managed to reach out to information security communities within the OIC and worldwide through collaborative arrangements with similar organizations.

This information security collaboration will continue to encourage participation from all parties to fulfil its objective of a secure cyber environment for Internet users.

This article was shortlisted as one of the top five projects for the WSIS Champion Prize 2016. On May 4, 2016 at the World Summit of the Information Society (WSIS) Forum in Geneva, this article won a WSIS Champion Prize under category C11, International and Regional Cooperation, alongside projects from Canada, Mexico, Tunisia and the United Arab Emirates. CyberSecurity Malaysia received a letter of appreciation from the ITU Secretary General, H.E. Houlin Zhao.

Drafting Security Target 101

By | Ahmad Dahari Bin Jarno

Abstract

Developers have the task to develop new products for markets and consumers are the ones from whom developers make money; thus, both parties complement each other as they co-exist in the ICT environment. As the world is evolving with technology, competition in the IT product field is not generous with either developers or consumers, whereby markets provide consumers with plenty of options for choosing and buying.

A neutral concept is formed at this point, which is the introduction of product testing through functional testing, compliance testing and security testing. The beauty of the concept is that consumers tend to use these testing notions as a checklist for their procurement policies, whereas it haunts product developers when consumers question their product security aspects. Products generally must be functional, follow certain best practices in development and design, and most importantly, must have security features to protect data residing with product data management.

Accordingly, common criteria have been established for decades. Criteria are based on the Orange Book and facilitate developers and consumers to be on the same page of understanding in terms of ensuring that IT products are functionally tested, follow world standards and provide the security assurance needs highlighted by consumers. The next question that arises is, where should all this information be written? The answer is a document called Security Target.

Security Target vs. Product Specification

Understanding a product in general can be done in several ways, such as reading the brochure, testing it out during product demo or testing it after purchasing as some consumers do not buy directly from the retail store. Even now, most IT products allow consumers to download technical product specifications from the developer's website. Unfortunately, the information described in the technical specifications does not elaborate fully on three (3) main components: functionality, compliance requirements and security features.

In light of these factors, the Common Criteria Communities have come up with the requirement for developers to provide such detailed documentation starting with a document called Security Target. This document describes a product declared by the developer by providing detailed information from the aspect of high level product overview description inclusive of technical specifications. There is added value with the specification of product security features as it follows a set of regulations defined by the Common Criteria Members, which is also known as a standardized set of requirements. Best of all, it is a public document.

According to a comparison, it is determined that Security Target is a superior to the Product Specification document because it fulfils the three mentioned components.

Security Target 101

Drafting a Security Target document requires firm and thorough understanding of the product and the ability to interpret the language elements of the Common Criteria. Language interpretation here refers to elaborating product information into a language that binds developer understanding and consumer perception of the market value of items, including items created based on certain known IT technologies.

The Security Target document consists of four (4) main information quadrants that are interlinked to form a map that defines a product and its technology. Even though Security Target is mostly referred to as a mandatory document in Common Criteria Evaluation and Certification, it can also serve as a product brochure, product specification and a justification of compliance document. The four quadrants comprising Security Target are as follows:

i. Quadrant 1: Product Overview consisting of Target of Evaluation (TOE) Overview, TOE Type, non-TOE Hardware/Software/ Firmware and TOE Description with elaboration on the Physical and Logical Scopes of TOE.

ii. Quadrant 2: Product Development based on the Problem Statement that consists of the Security Problem Definition and Security Objectives.

iii. Quadrant 3: Product Features consisting of a list of Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

iv. Quadrant 4: Product Justification consisting of rationale mapping between Quadrant 1, 2 and 3, which shows the reasons for developing each product feature, supported with specific objectives of its development. Likewise, this is where consumers tend to identify the limitations and advantages of a product without needing to go through the entire pile of programming documentation.

With regard to the four quadrants stated above, the next question is how to start writing, or where to start? A Security Target for a product can be drafted from scratch by first understanding the product through the reason for its development. Each IT product is developed to serve a specific purpose, thus the purpose is to solve IT problems and limitations. Starting with quadrant 2, writers can first list all the problem statements that relate to the product features, each of which is meant to solve a problem. For example, "an unauthorized person may send impermissible information through TOE that results in the exploitation of resources on the Internal network." Here, the product defined as Target of Evaluation (TOE) counters the statement with a feature that states "TOE shall mediate the information flow between users and web applications intended based on user requests." The product feature thus facilitates such mitigation with its feature "Access Control Filtering and Security Management."

Next, in quadrant 3, all product features are defined in detail using specific language defined by the Common Criteria requirements. Writers can pick and choose any of the security features from Common Criteria Part 2: Security Functional Components (SFRs). Likewise, it is the same for Security Assurance Requirements (SARs), whereby selecting the Evaluation Assurance Level (EAL) for product evaluation is all up to the developer. The trick of selecting the best SFR that fits the product features is to start selecting a minimum of ten (10) units of SFRs only, with a baseline of one SFR from each SFR chapter (e.g. User Data Protection, Security Audit, etc.). Each SFR is equipped with dependency requirements that are mandatory to be fulfilled; thus, ten (10) SFRs may lead to twenty (20) SFRs based on the dependency itself.

In completing quadrants 2 and 3, the writer can start elaborating on the product overview under quadrant 1. In this section, the writer needs to focus on writing the product details, especially in the TOE Overview and TOE Description. TOE Overview shall contain a description of the product to allow the consumer to understand the product by glancing at the information and not necessarily going into detail like referring to the Technical Specification document. However, a taboo here would be to elaborate any marketing words/statements. Note that the developer is not a judge for the consumers to help determine which product is best. The idea is to let the consumers be the judge of the product, as consumers are the ones who understand the product background and what it can offer to fit its purpose to serve the consumers.

Finally, the justification statement is placed in quadrant 4. Justification needs to be clear and consistent, which can be done via mapping in tables. Each SFR declared in quadrant 3 needs to be mapped back to quadrant 2 regarding whether each feature of TOE is relevant to counter, mitigate and reduce the risk of the threats. Furthermore, each security objective stated is meant to link back to all SFRs by showing that the descriptions are consistent through the definition statement of CC Part 2 Annex A. A tip and trick here is to understand each SFR declaration by reading the CC Part Annex A. Additionally, a small number of Assumptions, Threats, Organization Security Policies (OSP) and Security Objectives in quadrant 2 will lead to easy justification and mapping. All mapping and justifications are elaborated under the Rationale scope in Security Target.

Moreover, with plenty of information to work on the draft, it is crucial to have several handy tools in designing the structure of the Security Target and its content.

Writing Toolkits

Writing a technical document like Security Target is far from easy with all the information that needs to be incorporated within one document and that should say it all. Having an impressive toolkit will lessen the burden. The toolkits used for drafting any technical document vary among CC consultants. Nonetheless, the following toolkits should be of assistance and ease the burden, especially in processing abundant

information.

i. Gathering Information and Centralized Notes:

   a. Windows Snipping Tools and Application HoverSnap: These two tools are helpful for doing automated image capturing while studying the product features, interfaces and design. During the initial drafting stage, the Security Target captures all images of the product features, design and interfaces and will thus lessen the need to flip back and forth to refer to the actual product. Thus, there is less need to access the product remotely, which sometimes gives rise to connectivity and accessibility problems.

   b. Evernote and DropBox: These two provide good platforms to record all information gathered during a discussion session with the programmer. All files are saved in one location and can be accessed when needed. Evernote provides a centralized note collector and Dropbox provides a centralized file storing system. Also, both are free.

iii. Drafting the Security Target:

   a. Microsoft Word, Visio and PowerPoint: This software comes in a bundle installer that is recommended for writing the Security Target and other CC documentation. It offers an acceptable format for open source document writing tools. Microsoft Visio is used to design product architecture deployment and Microsoft PowerPoint is to design the block diagram of the logical scope of TOE.

   b. Adobe Acrobat Pro: This software facilitates exporting any PDF document to a word document and vice versa. It is a useful tool when sharing documents online and also for protecting documents using passwords.

iii. Remote Access, File Sharing and Document Review Discussion:

   a. Google Document: It is recommended to hold a discussion online while commenting and reviewing CC documentation like the Security Target.

   b. Google Drive: It is synced with Google Document and allows sharing documents with sharing protection through group access and links.

   c. TeamViewer: This remote access software is easy to configure and free to use.

   d. Google Hangouts and Skype: These are software for discussion and videoconferencing.

Conclusion

Security Target is an important document of Common Criteria Evaluation and Certification. Thus, having good knowledge of writing the Security Target as well as being equipped with supporting toolkits can simplify the processes of information gathering, content writing and easing the discussion sessions between all parties. Likewise, producing a document such as Security Target allows the developer to be more transparent with the consumer in describing their product without compromising any confidential information. The consumer is also able to sincerely decide on a product's capability and capacity through all its relevant features.

References

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4.

2. Using the Common Criteria for IT Security Evaluation, Debra. S. Herrmann, 2003, Auerbach Publications.

3. Successful Common Criteria Evaluations: A Practical Guide for Vendor, Wesley Hisao Higaki, 2010, CreateSpace Independent Publishing Platform.

Impersonation and Spoofing Fraud Q4 2015

By | Kilausuria Abdullah

Introduction

Impersonation refers to any activity or act of pretending to be another person for the purpose of fraud. The word "spoof" means to hoax, trick or deceive. Therefore, in the IT world, spoofing refers to tricking or deceiving computer systems or other computer users. Hiding one's identity or faking another user's identity on the Internet is typical examples.

Impersonation and spoofing are basically activities used by perpetrators to manipulate victims' trust for the purpose of fraud. Some incidents include using the victim's original identity to make a fake account, purchase new items, etc. Besides impersonating victims, perpetrators can also spoof victims' emails to make the victims trust the email content.

Analysis

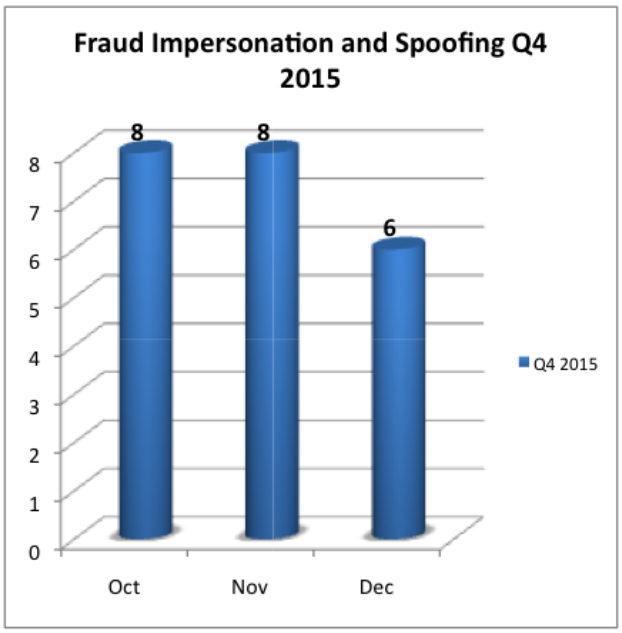
The analysis in this article is based on sample incidents received by Cyber999 In the fourth quarter of 2015. A total of 22 incidents were received on impersonation and spoofing fraud as shown in Table 1 and Graph 1.

Impersonation and Spoofing Fraud for Q4 (Oct-Dec) 2015

Incident Category	Oct	Nov	Dec	TOTAL
Impersonation and spoofing	8	8	6	22

Table 1: Impersonation and Spoofing Q4 (Oct - Dec) 2015

Note: The statistics reflect the number of incidents.

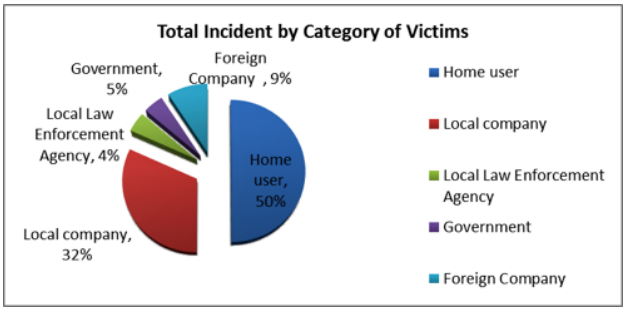


Graph 1: Impersonation and Spoofing Fraud Q4 (Oct – Dec) 2015

The categories of victims who reported impersonation and spoofing fraud incidents are shown in Table 2 and Graph 2.

Types of reporting users	Total
Home users	11
Local companies	7
Local enforcement agency	1
Government	1
Foreign companies	2

Table 2: Total Incidents by category of victims



Graph 2: Total incidents by category of victims

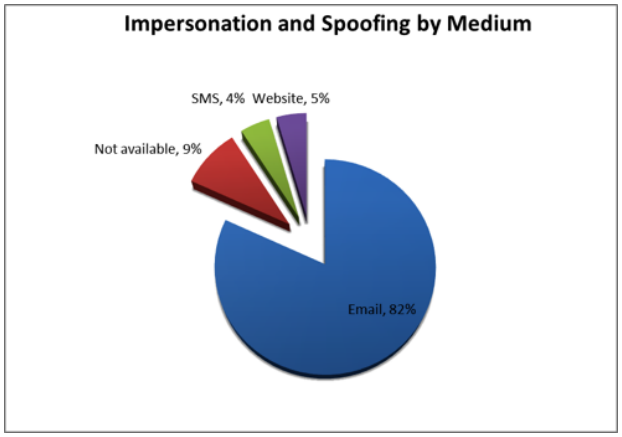
According to the graph above, for Q4 2015 there are five categories of users who reported fraud incidents. The majority of incidents were reported by home users, contributing 50% of all reported incidents. Local companies

reported about 32% of all incidents and foreign companies about 9%.

In this quarter, impersonation and spoofing incidents were identified based on the medium used by the perpetrators. The medium types used for impersonation and spoofing incidents identified in this quarter are presented in Table 3 and Graph 3.

Medium of Impersonation and Spoofing	Total
Email	18
Not available	2
SMS	1
Website	1

Table 3: Figures on medium used for impersonation and spoofing Incidents



Graph 3: Percentage of impersonation and spoofing by medium

Based on the analysis for Q4 2015, impersonation and spoofing incidents mostly occurred via email as the main medium, which represents 82% of all incidents. This was followed by telephone/ smart phone as the medium, contributing 13% of overall impersonation and spoofing incidents in Q4 2015.

Case studies of impersonation and spoofing for commercial fraud done via email as a medium

Figures 1 and 2 display the steps involved in the method of operation for impersonation and spoofing via email as a medium:

a. The victim company requests a purchase order from the supplier and waits for a proforma invoice from the supplier.

b. The victim company will receive a fake proforma invoice from the perpetrator via email allegedly from the supplier, with a fake account number to which to transfer the payment.

c. Inexperienced and untrained staff will process the forged invoice and make payment to the fake account.

d. The supplier will inform the victim company that payment has not been made and the victim company will say that payment has already been made.

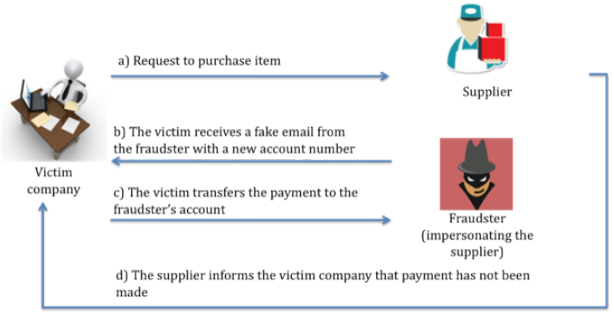


Figure 1: Method of a fraudster impersonating a supplier

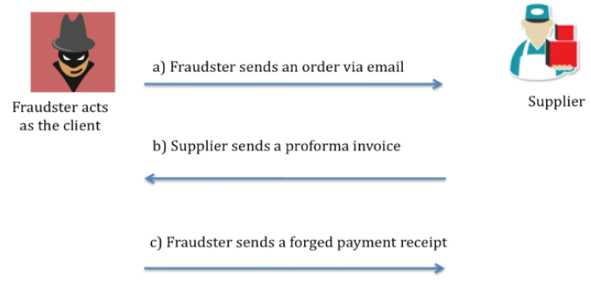


Figure 2: Method of a fraudster impersonating a client

a. The fraudster sends an order request to the supplier.

b. The supplier sends a proforma invoice to the fraudster.

c. The fraudster sends a forged payment receipt to the supplier.

d. Inexperienced and untrained staff will process the forged invoice and ship the items to the fraudster.

e. The supplier realizes the payment receipt is forged.

Best Practices

- Be wary of suspicious activities or emails from known or unknown persons. Check with the right parties the validity of the information received.

- The user may refer to registered companies for Malaysian products at Malaysia External Trade (MATRADE):

  Malaysian Exporters: http://www.matrade.gov.my/en/for-malaysian-exporters

  Foreign Buyers: http://www.matrade.gov.my/en/for-foreign-buyer

- The user may refer to registered companies in Malaysia via: https://www.ssm-einfo.my/

- Get proper confirmation directly from the supplier on their account number before making any payments. Confirmation can be done via a telephone call for instance.

- Check/verify the email including the full email header, email features (spelling) and email content (invoice, address, document copy, payment method).

- Call your bank immediately if you realize the transfer has been made to a fake account number.

- Employers are highly encouraged to train and provide security awareness for their employees.

- Lodge a police report at a nearby police station with details or evidence for further police investigation.

Impacts of Impersonation and Spoofing Fraud Reported

The impacts of the impersonation and spoofing fraud incidents reported are listed below:

1. An attacker may attempt to harvest records of targeted information (financial data, personal info) via various hacking or social engineering techniques in order to steal data.
2. An attacker may attempt to sell the stolen data to third parties or underground channels.
3. Impersonation attacks are increasingly tied to organized crime. This is because the profitability of impersonation attacks has global implications not only for individuals but also enterprises.
4. Impersonation and spoofing attacks can also destroy financial security and financial outcomes.

Conclusion

By Q4 2015, 22 incidents were reported on impersonation and spoofing fraud. The most incidents reported for impersonation and spoofing fraud in Q4 2015 were done using email as a medium to impersonate victims. Organizations and regular users must be aware and concerned with impersonation and spoofing fraud that may occur in daily activities. The repercussions from impersonation and spoofing can have high impact on the affected organization or user, even from a small mistake such as misunderstanding email content or an email address. As such, organizations and regular users must always make sure to adhere to the best security practices to prevent data from being stolen that might be used for malicious fraud activity.

References

1. http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/799/index.html

2. https://zeltser.com/media/docs/impersonation-attacks.pdf

3. http://www.mysecurityawareness.com/article.php?article=384&title=what-is-impersonation-in-social-engineering#.VYd_mKbkaf4

4. http://techterms.com/definition/spoofing

5. https://www.mycert.org.my/en/services/advisories/mycert/2015/main/detail/1130/index.html

Keselamatan Siber Anak-Anak : Akujanji Ibu Bapa Siber

By | Zaleha Abd Rahim, Yuzida Md Yazid

Di zaman kecanggihan teknologi kini, pengaliran maklumat di dunia siber tiada siapa dapat mengawalnya. Beribu-ribu laman web telah dibangunkan hampir setiap hari demi untuk menyalurkan maklumat walau dimana juga kita berada. Betapa mudahnya hidup di zaman ini, dengan hanya satu 'klik', serta-merta kita mampu menerokai dunia tanpa batas sempadan. Maka tidak hairanlah jika kanak-kanak seawal usia 3 tahun sudah didedahkan dengan gajet-gajet dan aplikasi-aplikasi seperti iPhone, iPAD, Notebook, Facebook, Twitter, Instagram, YouTube dan lain-lain lagi.

Justeru itu, adalah wajar ibu bapa memupuk nilai integriti yang tinggi, jati diri dan akhlak yang mulia dalam diri anak-anak mereka agar gejala-gejala negatif dapat dihindari. Statistik yang dikeluarkan oleh Malaysian Computer Emergency Response Team (MyCERT) jelas menunjukkan angka peningkatan dalam jenayah siber seperti *cyberbully, cyber flirt, scam, cyberstalking* dan lain-lain lagi. Oleh yang demikian, ibu bapa perlu memainkan peranan yang lebih aktif dalam memastikan keselamatan siber anak-anak mereka terjamin dan dipelihara. Komunikasi tanpa sempadan kadangkala boleh merosakkan akidah dan sahsiah anak-anak. Bukanlah sesuatu yang menghairankan andainya seseorang anak yang pada zahirnya kelihatan baik di depan mata ibu bapa, akhirnya terjebak dalam perangkap masalah sosial di alam siber, akibat kurangnya perhatian..

Sebagai orang yang terdekat dengan anak-anak, ibu bapa seharusnya memainkan peranan penting dalam membantu mengawasi dan memantau keselamatan anak-anak mereka ketika berada di alam siber. Berikut adalah beberapa akujanji yang perlu diambil oleh ibu bapa bagi memastikan keselamatan dan kesejahteraan anak-anak mereka. Maka dengan ini saya berjanji akan melaksanakan perkara-perkara berikut:

1. Walau pun saya kurang pengetahuan tentang Internet, saya akan mengambil masa untuk mempelajari bagaimana menggunakannya agar saya boleh memantau dan mengawasi apa yang dilayari oleh anak-anak saya.
2. Saya akan mengajar anak saya supaya menghormati privasi orang lain sama ada dalam dunia realiti dan digital
3. Saya akan menerangkan kepada anak saya tentang pembelian barang secara dalam talian dan saya akan menunjukkan kepadanya *website* yang selamat dan dipercayai untuk membeli barang secara dalam talian. Saya juga akan menunjukkan kepadanya bagaimana untuk mencari dan menentukan pembelian yang terbaik.
4. Saya akan mengajar anak saya tentang tatasusila penggunaan teknologi komunikasi atas talian. Saya juga akan menerangkan bahawa komunikasi secara bersemuka adalah juga penting
5. Saya akan menerangkan kepada anak-anak tentang keperluan budi bahasa dan tingkah laku yang sopan semasa berkomunikasi dengan orang lain dalam talian. Jika mereka mahu dihormati, mereka juga perlu menghormati.
6. Saya akan cuba mengenali rakan-rakan Internet anak-anak saya dan akan memastikan mereka adalah rakan-rakan Internet yang sah dan selamat.
7. Saya akan memberitahu anak-anak bahawa ada sesetengah maklumat dalam talian adalah milik orang lain yang tidak boleh dicerobohi atau diambil tanpa kebenaran.
8. Saya akan memastikan anak-anak ada had masa yang tertentu untuk melayari Internet agar mereka tidak ketagihan teknologi dan berkemungkinan mengalami masalah kesihatan.
9. Saya akan meluangkan masa mengajar anak-anak saya bagaimana untuk melindungi data-data peribadi mereka
10. Saya akan memberitahu anak-anak bahawa pencegahan adalah lebih baik dari pemulihan. Justeru, saya akan menunjukkan cara install perisian seperti antivirus, *spyware* dan *adware*.
11. Saya akan menjadi 'role model' terbaik untuk anak-anak dengan memberikan contoh sebagai pengguna Internet yang baik.

12. Saya akan membuat pemeriksaan *(spotcheck)* ke atas gajet yang digunakan anak-anak agar mereka lebih berhemah dalam penggunaannya.

Menjadi ibu bapa kepada generasi siber sememangnya mencabar. Di samping berikrar untuk melakukan perkara-perkara di atas, ibu bapa juga harus menerapkan dan memberikan didikan agama yang sempurna sejak awal usia anak-anak. Tidak dinafikan, agama merupakan benteng yang paling kukuh untuk menghalang perkara negatif yang dibawa dari alam siber. Didiklah anak-anak tentang dosa dan pahala sepanjang melayari Internet. Apabila anak-anak memahami konsep Tuhan sentiasa melihat apa yang mereka lakukan, dengan sendirinya kegiatan mereka di alam siber akan lebih terkawal.

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

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

Best Brand Internet Security 2008 & 2009

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

STANDARDS MALAYSIA
MS ISO/IEC 17025 TESTING
SAMM NO. 456
(MyREF LABORATORY)

MSC MALAYSIA
Status Company

Best Child Online Protection Website