CyberSecurity MALAYSIA

MOSTI

e-Security

Volume 20 - (Q3/2009)

The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice. Even with oversight the policies and procedures may not be effective: **my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures** that were in place for years before I compromised them successfully.

Kevin Mitnick

Contributors

ISSN 1985-1995

9 771985 199003

Best Brand Internet Security

KDN License number: PP 15526/10/2009 (023300)

From the Editor's Desk

maslina@cybersecurity.my

Hi to everyone and Selamat Hari Raya Aidil Fitri to all muslim readers!

So, what do we have in this issue; product certification, BCM, email header analysis, memory analysis of gmail forensic and many more technical write-ups, but of course they are those the interesting ones!

Next quarter? Without we realize it, time passed so fast and next quarter will be the last quarter of the year. Please utilize your budget for the trainings offered by CyberSecurity Malaysia and get the best deal before the year ends!

For this last quarter, you will see more training on wireless security and security essentials. Do check our website for more details if you want to attend the training and sit for the CISSP and SSCP.

Our CEO highlighted the social networking abuse. While there are various ways to protect from social media hacker attacks, but still education and awareness remains the essential factor to curb it. Thus, please convey the significance of not disclosing personal details in the cyber world to your colleagues, friends and family. It is not only happening to adults, but our kids are at risk too. For all parents, please ensure you know what your kids are doing on the net.

I would like to thank our contributors for this publication and hope for security professionals and practitioners out there to share their experiences and know-how with us.

Do email us if you wish to contribute.

Happy reading!

Best Regards

Maslina

Maslina binti Daud
Editor

A Message from the Head of CyberSecurity Malaysia

Welcome to the third edition of eSecurity Bulletin for 2009 and a belated Eid-ul Fit al-Mubarak to all our Muslim readers.

In the past quarter, there were quite number of stories on social networking websites being attacked such as Facebook and Twitter, rather than conventional attacks through email. If previously, phishing attacks usually targeted financial websites, now phishers are expanding it, luring Internet users to accidentally expose their sensitive information through social networking sites. This latest development causes real threats to organizations as employees do access social networks at workplace. Thus, it is imperative for organizations to ensure proper measures including social network policy to be in place to avoid sensitive data being leaked out unnecessarily.

It is without a doubt, the weakest part of security lies within the organization itself. Disgruntled employees, terminated employees can be a source of enemy to exploit vulnerabilities within the system that can surprise the organization. Strong security policy with security awareness instilled amongst employees able to alarm possible danger by internal perpetrators.

Therefore, CyberSecurity Malaysia is trying various ways to inculcate security awareness be for organizations as well as for public. On 9 August 2009, His Honourable Tuan Haji Fadillah Yusof has officiated our new CyberSAFE portal. In general, CyberSAFE portal is our new commitment to propagate our cyber security messages with new updated information and outlook pertaining to the cyber security awareness to the public. This portal consists of CyberSAFE Website (www.cybersafe.my) and CyberSAFE Web Zine.

Again, I would like to stress educating people and organizations are fundamental in building a strong pillar to secure our cyberspace.

Finally, I would like to take this opportunity to thank our contributors who have given their time and support to make this bulletin a success. New contributors are always welcomed!

Thank you.

Best Regards
Lt Col (R) Husin Jazri (Retired) *CISSP*
CEO
CyberSecurity Malaysia

Table of Contents

PUBLISHED BY
CyberSecurity Malaysia (726630-U)
Block A, Level 8, Mines Waterfront Business Park
No 3, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

PRODUCED BY
Equal Media (1590095-D)
Block D-10-3, Plaza Kelana Jaya
Jalan SS7/13A, 47301 Petaling Jaya
Selangor Darul Ehsan, Malaysia
Tel / Fax : +603 2274 0753

PRINTED BY
Percetakan Tujuh Lapan Enam Sdn Bhd (564108-K)
No18, Lengkungan Brunei
55100 Pudu, Kuala Lumpur
Tel: +603 2732 1422
KKDN License Number: PQ 1780/3724

e-Security News Highlights for Q3, 2009

Survey: Half of businesses don't secure personal data (September 24, 2009)
"Around 55 percent of all businesses acknowledge that they secure credit card information but not Social Security numbers, bank account details, and other personal data, according to a survey of more than 500 companies released Wednesday by Imperva and Ponemon Institute.."

http://news.cnet.com/8301-1009_3-10360639-83.html

Three of Four Charges Dismissed In Terry Childs Case (August 24, 2009)
"Terry Childs, the San Francisco network administrator who kept some rather important passwords to himself last summer, is now facing a considerably shorter list of accusations. A judge has dismissed three of the four charges that were brought against him.."

http://www.securitypronews.com/news/securitynews/spn-45-20090824ThreeOfFourChargesDismissedInTerryChildsCase.html

Cyber virus targets online banking log-ins (September 21, 2009)
"CYBER criminals have created a highly sophisticated Trojan virus that steals online banking log-in details from infected computers. The Clampi virus, which is spreading rapidly across hundreds of thousands of computers in Britain and the United States, infects computers when users visit websites that host a malicious code.."

http://www.theaustralian.news.com.au/business/story/0,28124,26102544-5017997,00.html

Woman falls victim to identity thief (September 9, 2009)
"PETALING JAYA: Swashna (not her real name) wondered why strangers kept sending requests to add her as a friend on their profile at a popular social networking site. The 25-year-old company executive is normally careful about who she adds to her own profile, so she was surprised to find total strangers claiming to know her…"

http://star-techcentral.com/tech/story.asp?file=/2009/9/9/technology/20090909100203&sec=technology

Cyber-thief Sold Stolen Domain to NBA Player, Police Charge (August 4, 2009)

"A 25-year-old man is charged with stealing a company's domain name and selling it to NBA player Mark Madsen for $111,000. New Jersey State Police say they believe the arrest marks the first time the state has charged someone with stealing a domain name…"

http://www.eweek.com/c/a/Security/CyberThief-Sold-Stolen-Domain-to-NBA-Player-Police-Charge-411195/

10 Ways to Protect Your Company from Social Media Hacker Attacks (September 24, 2009)

"News Analysis :Social networks can be scary places that cause many companies to debate whether to continue supporting social network access for employees at the office. But keeping a company safe from potential security issues isn't as hard as it might appear. Here are 10 ways to make social network access safer.."

http://www.eweek.com/c/a/Security/10-Ways-to-Protect-Your-Company-from-Social-Media-Hacker-Attacks-595134/

Cyber criminals may target Olympics (July 8, 2009)
"International organised criminal networks are already preparing to target the London 2012 Olympics, one senior police officer has warned. Scotland Yard Deputy Assistant Commissioner Janet Williams said officers are probing a series of front companies that could be used in complex frauds.."

http://www.channel4.com/news/articles/science_technology/cyber+criminals+may+target+olympics/3255757

Teenagers blamed for 40% of game crimes in Korea (September 26, 2009)
"About 40 percent of online game-related crimes were committed by teenagers last year, according to a report by the National Police Agency.A total of 76,141 game-related crimes occurred in 2006-2008 and 61,886 or 81.3 percent of the offenders were apprehended, showed the report unveiled by a ruling party lawmaker…"

http://www.asiaone.com/News/AsiaOne+News/Crime/Story/A1Story20090926-170070.html

Researchers: Attacks on US, Korea sites came from UK (July 15, 2009)
"The denial-of-service attacks launched on Web sites in South Korea and the United States earlier this month appear to have come from a master server in the United Kingdom, according to security researchers in Vietnam.."

http://www.zdnetasia.com/news/security/0,39044215,62056041,00.htm

New York Times website hit by malicious adverts for scareware (September 14, 2009)
"The website for the New York Times was hit by malicious adverts over the weekend. A note was posted to the home page on Sunday that warned of a pop-up message warning users that their computer had been infected, and urging them to install fake anti-virus software.."

http://www.scmagazineuk.com/New-York-Times-website-hit-by-malicious-adverts-for-scareware/article/148862/

Time for social networks to take security seriously (July 22, 2009)
"Last week, a hacker who gained access to a Twitter employee's personal email account was able to infiltrate the company's Google Apps account to steal confidential documents, which were then published by some websites.."

http://www.mxlogic.com/securitynews/web-security/time-for-social-networks-to-take-security-seriously694.cfm

Twitter warns of direct-messaging worm (September 24, 2009)
"Social-networking service Twitter warned users on Wednesday that a link sent by direct message redirects users to a malicious site that attempts to steal their account credentials…"

http://www.securityfocus.com/brief/1016

MyCERT 3rd Quarter 2009 Summary Report

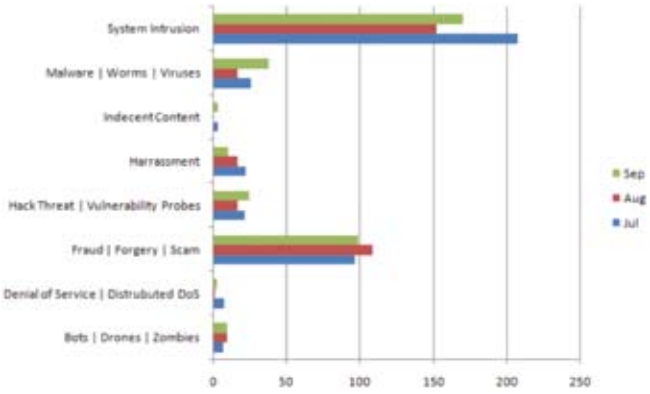
Introduction

This quarterly summary provides an overview of activities related to Cyber999 (computer security incident handling service) and trends observed from the research network. The summary provides users with high-level statistics of incidents handled by MyCERT in quarter three (Q3) of 2009, security advisories published, and events participated by MyCERT staff. Do take note that the statistics provided reflect only the total number of incidents handled by MyCERT. They do not represent nor reflect the financial value and impact of the incidents to the victims. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and international organizations to resolve computer security incidents.

Incidents Trends Q3 2009

From July to September 2009, MyCERT, via its Cyber999 service, handled a total of 1087 incidents. These incidents were referred to MyCERT by members in it's constituency and security teams from abroad, in addition to MyCERT's proactive monitoring efforts.

The following graph shows the total incidents handled by MyCERT in Q3 2009.



Incident Breakdown by Classification in Q3 2009

In Q3 2009, system intrusion and fraud recorded high number of incidents representing 50% and 29% of total incidents handled respectively. System intrusion incidents are generally attributed to web defacement. MyCERT observed that the main cause of defacements were due to unpatched and misconfigured web applications. There was a slight surge of web defacements in July and August due to political events where attackers target shared hosting servers in carrying out mass defacements.

Fraud related incidents handled by MYCERT comprise of mostly phishing sites of local and foreign brands. In Q3 2009, MyCERT handled 165 phishing related incidents involving 125 unique phishing sites that target various brands. The majority of phishing sites were targeting local financial institutions. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the affected Internet Service Providers (ISPs). There were instances where MYCERT was able to recover the drop email accounts used by attackers and the database containing users credentials. Details of those information are normally escalated to responsible parties for their further action.

MyCERT has also observed that a targeted phishing attack is normally coupled with 'money mule' recruitment emails. Basically once users credentials has been obtained via the phishing sites, the criminals will need somebody who has an account at the same bank to assist them in transferringthe money out. The following is an example of money mule recruitment email. Take note of the requirement of "Only Maybank Account (Malaysia) "

Hello,

Would you like to work from home and get paid every day?

HOW MUCH WILL YOU EARN?
At the beginning your fee will be 10% per each operation, though in future it will increase up to 18%!

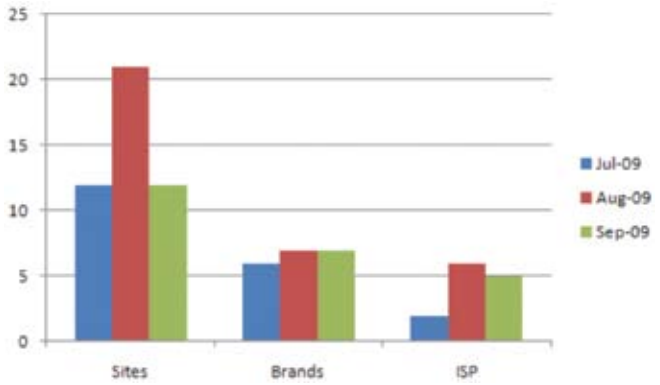
MAIN REQUIREMENTS
#18 years or older
#Legally capable
#Responsible
#Ready to work 3-10 hours a week
#E-mail and internet experience
#Only MayBank Account (MALAYSIA)

If you are interested in our proposition please respond to this message by e-mail!

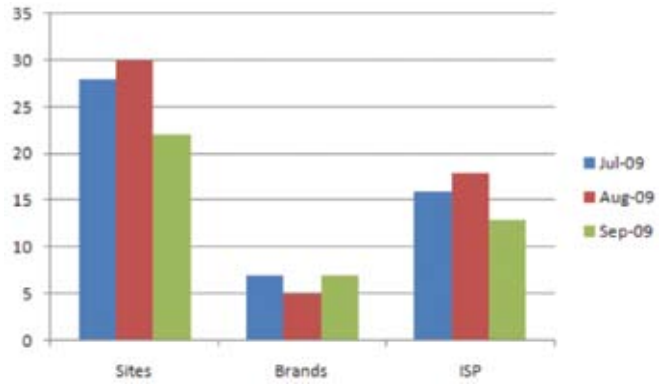
Best Regards

William Svent,
Payments Management!
Constanta, Romania, 920000
E-mail: xxx@live.com

The following graph gives an overview of phishing incidents handled by MyCERT in Q3 2009.

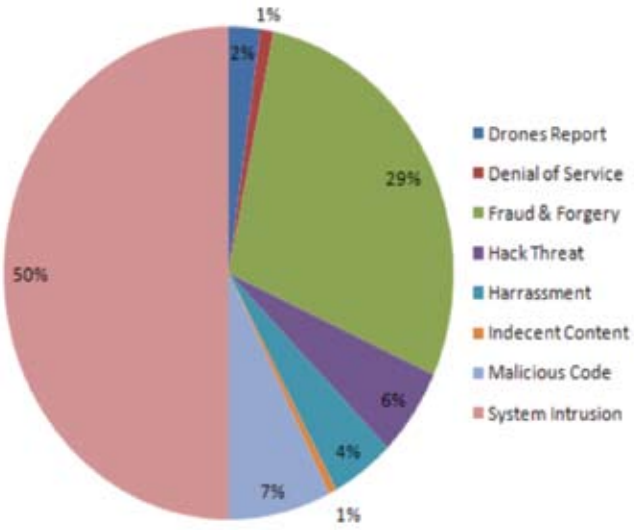


Unique Foreign Brands Phishing Websites July to Sept 2009



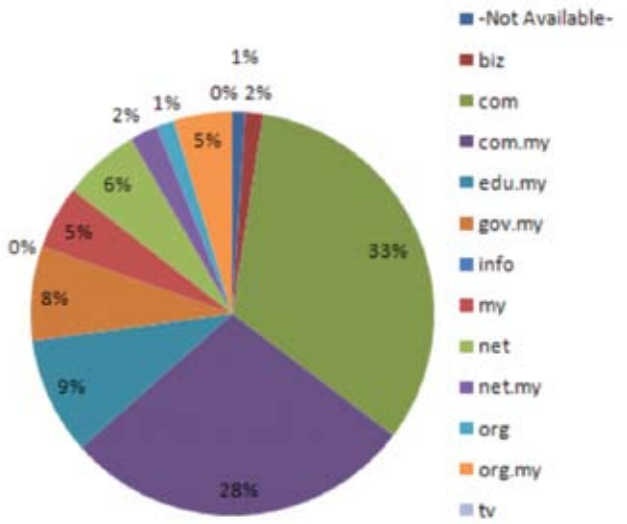
Unique Local Brands Phishing Websites July to Sept 2009

In Q3 2009, drones and malicious codes related incidents represent 9% of total incidents handled by MyCERT. Drones or 'zombies' are computers infected with malicious codes that connect to the command and control (C&C) servers. Other examples of incidents within these categories are active botnet controller and hosting of malware or malware configuration files. In Q3 2009, MyCERT has handled about 251,341 IP addresses in Malaysia that has been infected by conficker worm. There is still significant infection of Conficker and its variant out there.



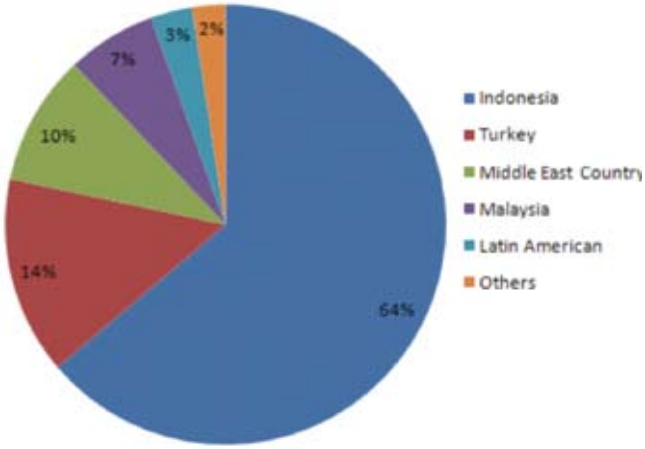
Percentage of Incident Q3 2009

The following graph shows the breakdown of domains defaced in Q3 2009. Out of the 490 websites defaced in Q3 2009, 61% of them are those with com and com.my extensions. Defacers generally target web applications that are prone to SQL injection or sites that are not secured or patched with latest updates.



Web Defacement By Domain Q3 2009

In Q3 2009, MyCERT has observed that the majority of defacers originate from Indonesia, representing 64% as shown in the below graph. The activities of defacers from this origin, mainly involves mass defacements of websites hosted on single virtual hosting server.



Percentage of Defacer Origin For Q3 2009

Advisories and Alerts

In Q3 2009, MyCERT had issued a total of 25 advisories and alerts for its constituency. Most of the advisories in Q3 are related to popular end user applications such as Adobe PDFReader, Adobe Flash, Microsoft Office Power Point, Mozilla Firefox and Microsoft Internet Explorer. Attacker often compromise end users computersby exploiting vulnerabilities in users' application. Attacker uses various social engineering techniques to trick users to open a specially crafted file (i.e. a pdf document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT in 2009.

http://www.mycert.org.my/en/services/advisories/mycert/2009/main/index.html

CyberSecurity Malaysia Research Network

Apart from the Cyber999 service, MyCERT also observed activities on its research network and conduct analysis on internet threats and trends. The overall objectives of this initiative are as follow:

- To observe the network for suspicious traffic simultaneously monitor for the occurrence of known malicious attacks.
- To observe attacker behaviours in order to learn new techniques being deployed
- To determine the popular techniques that is currently being used as well as to confirm the continued use of old and well known attack techniques.
- To compile and analyze sufficient relevant information of which the results can be used to alert the community at large to the possibility of imminent cyber attacks on local networks.

Malware Tracking

Malware, a portmanteau from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software. Malware is not the same as defective software, that is, software which has a legitimate purpose but contains harmful bugs.

MyCERT have seen that most vulnerabilities being exploited in Windows systems were through automatic methods, without direct involvement of the attacker. The known vulnerabilities are automatically being exploited by malware which updated with recent or famous exploit code.

Beside of exploiting common vulnerabilities, MyCERT has observed that cyber criminals also take advantage on some popular events such as H1N1 and the passing of Michael Jackson, the 'King of Pop'. MyCERT spotted and learned a few malicious spam links, videos and emails about Michael Jackson's death and H1N1. The modus operandi for this attack relies so much on social engineering technique. Out of total 16275 binaries collected in Q3 2009, 727 are unique (based on MD5 hash).

In the following plot, one can see the the global distribution of binaries downloaded by Nepenthes sensors in the third quarter of 2009.

Different antivirus products might reflect different name for one particular malware. As grouped by MD5 hash, here are the top 10 malwares collected in Q3 2009:

1822	524bc0f75c12683f73ce0ceed70faab8	OK	W32/Backdoor2.FEHI	WORM/Rbot.cyj	OK
1144	7dc73bfa4d78284155dd5101991eeb34	OK	W32/Backdoor.BAE	BDS/Small.EO	FSG V1.3x SN:1637
1000	98eb0fdadf8a403c013a8b1882ec986d	OK	W32/Trojan5.DCW	WORM/Rbot.147456.27	OK
816	1f8a826b2ae94daa78f6542ad4ef173b	OK	W32/Trojan5.DCW	WORM/Rbot.147456.27	OK
727	e269d0462eb2b0b70d5e64dcd7c676cd	OK	W32/Trojan5.DCW	WORM/Rbot.147456.27	OK
674	2fa0e36b36382b74e6e6a437ad664a80	OK	W32/Trojan5.DCW	WORM/Rbot.147456.27	OK
626	14a09a48ad23fe0ea5a180bee8cb750a	OK	W32/Trojan5.DCW	WORM/Rbot.147456.27	OK
473	1d419d615dbe5a238bbaa569b3829a23	OK	OK	OK	OK
444	1bbf323c6560ffa2a00285f26947e084	OK	W32/Kolab.Q	TR/Crypt.XPACK.Gen	OK
429	a2bf71ed94580d2e957b550c9aae1490	OK	W32/Trojan5.DCW	WORM/Rbot.147456.27	OK

Top 10 Binary Hash

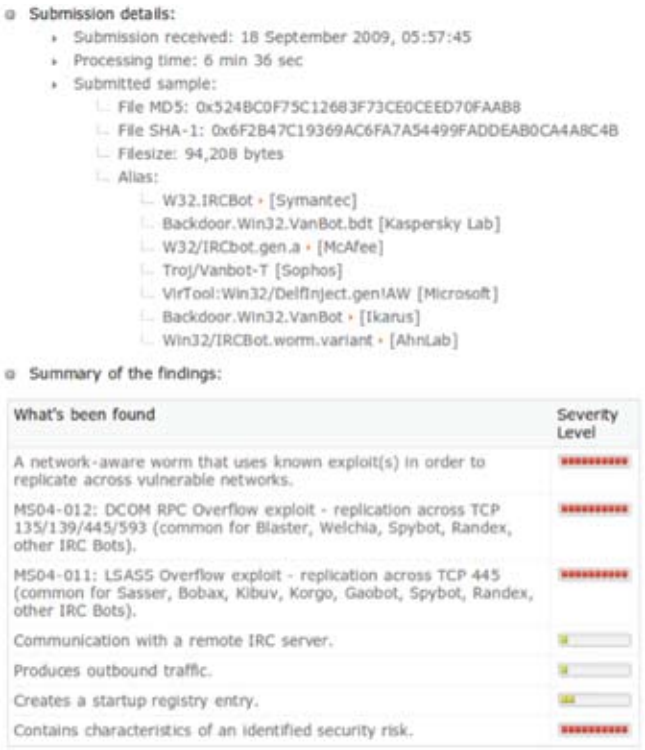
Based on MD5 hash, among the top malware collected in Q3 2009:

- 524bc0f75c12683f73ce0ceed70faab8
- 7dc73bfa4d78284155dd5101991eeb34

Analysis from Threat Expert

From the above, two MD5 hashes, and some other samples, one could observe and might conclude that most malware that MyCERT has collected in Q3 2009 share the following summaries:

- Family of network-aware worm. Uses known exploit(s) in order to replicate across vulnerable networks.
- Exploit MS04-012 vulnerability: DCOM RPC Overflow exploit - replication across TCP 135/139/445/593.
- Exploit MS04-011 vulnerability: LSASS Overflow exploit - replication across TCP 445.
- Communicate through a remote IRC server.
- Contains characteristics of an identified security risk.



Other Activities

MyCERT staff had been invited to conduct talks and training in various locations in Q3 2009.The following is a brief list of talks and trainings conducted by MyCERT in Q3 2009:

- September 2009 – Talk on Global Threats Updates at F-Secure Lab.
- August2009 –Incident Response Training for Egypt CERT in Cairo, Egypt.
- August 2009 – Cyberspace Security; Current Trends and Threats, Client Side Security; Minggulnovasi, Sarawak.
- August 2009 – Presentation on Hacking Anatomy at INSTUN, Tronoh,Perak.
- July 2009 -Security Awareness Talk atBulan ICT, SIRIM Berhad.
- July 2009 – Training on TCP/IP at INSTUN, Tronoh, Perak.
- July 2009 – Presentation on Hacking Anatomy at CGSO Internet Security Awareness.
- July 2009 – Hacking Demo at ILKAP DPP Prosecution Course.

Conclusion

In Q3 2009, neither crisis nor outbreak was observed. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. MyCERT encourages Malaysian Internet users to be constantly vigilant of the latest computer security threats.

MyCERT can be reached for assistance at:

Malaysia Computer Emergency Response Team (MyCERT)
E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999 (Office Hours)
Phone: (603) 8992 6969 (Office Hours)
Fax: (603) 8945 3442
Phone: 019-266 5850 (24x7)
SMS: 019-281 3801
http://www.mycert.org.my/

Please refer to MyCERT's website for latest updates of this Quarterly Summary.

Business Continuity Management: From Information Security Management System (ISMS) Perspective

Background

Information security (IS) in its broader definition as described by the ISO/IEC 27001:2005 is, *"The protection of information from a wide range of threats in order to ensure business continuity, minimize risk and maximize return on investments and business opportunities"*. To ensure this, a suitable set of controls, policies, organizational structures, procedures and other related functions must be implemented along with other business management processes.

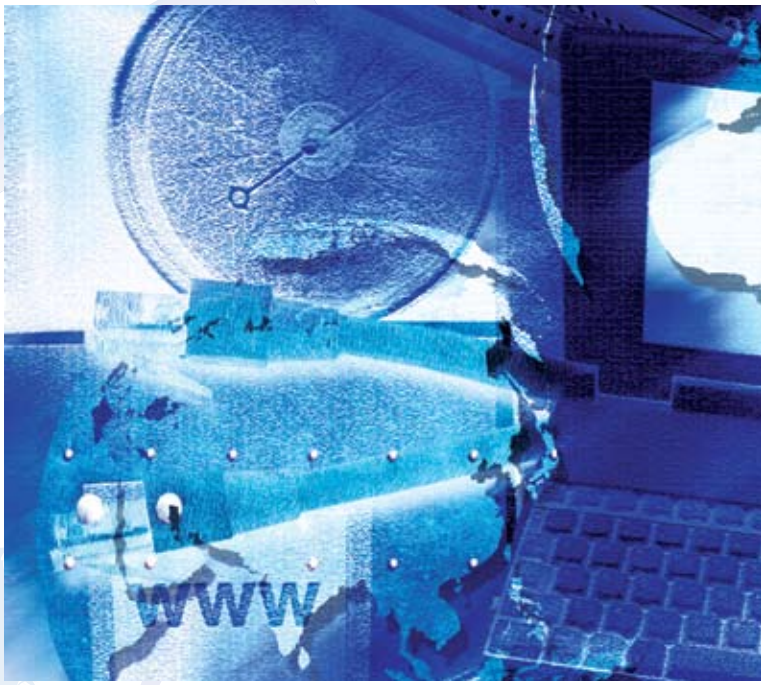
ISO 27001 is an information security management standard developed to help organizations establish, implement, operate and monitor an Information Security Management System (ISMS). In other words, ISO 27001 is also an ISMS development methodology which explains how to develop ISMS. However, this standard alone does not elaborate on the elements that construct ISMS, which is where ISO 27002 comes in.

The ISO 27002, previously known as ISO/IEC 17799:2005, lists the generally accepted information security management practices that make up ISMS. There are 15 controls covered and Business Continuity Management (BCM) is one of the main ones. Although, BCM is often considered to be a subject by its own, in terms of standards BCM is an integral part of it. Being an essential part of IS, this is obviously stated in section 14 of ISO 27002 where BCM is clearly emphasized. ISO 27002 includes useful advice and guidance on how to include IS controls within the business continuity process. As for organizations undergoing the ISMS certification, having to comply to ISMS requirements is an indirect requisition to have BCM in place all at the same time.

Content

As stated in the ISO/IEC 27002:2005(E) Information Tech - Security techniques – Code of Practice for Information Security Management , the information security aspects of BCM is to counteract interruptions to business activities, protect critical business process from the effects of major failures of information systems or disasters and ensure their timely resumption. To ensure this, organizations should implement business continuity (BC) process to reduce the impact as well as to recover from loss of information assets at an acceptable level.

Overall there are 5 subsections within the BCM area. Subsection 14.1.1 stated that IS should be included in the BCM process. The control that should be implemented for this subsection is to develop and maintain a managed



process for BC to address organizations' IS requirements. Similarly, this is to establish a business continuity process for information. In doing so, the implementation guidance that can be followed stated the process to have these BCM key elements ; understanding the risks in terms of likelihood and the impact caused by IS incidents and establishing the business objectives of information processing facilities; identifying all the assets in critical business processes; possibility to purchase suitable insurance as part of the overall BC process or part of operational risk management; identifying and considering the implementation of additional preventive and mitigating controls; identifying sufficient financial, organisation, technical and environmental resources to address the identified IS requirements; ensuring personnel safety and protection of information processing facilities and property; formulating and documenting BC Plans for IS requirements to be in line with the agreed business strategy; regular testing and updating of the plans and processes; and ensuring the management of BC is included in the organizations' overall processes and structure.

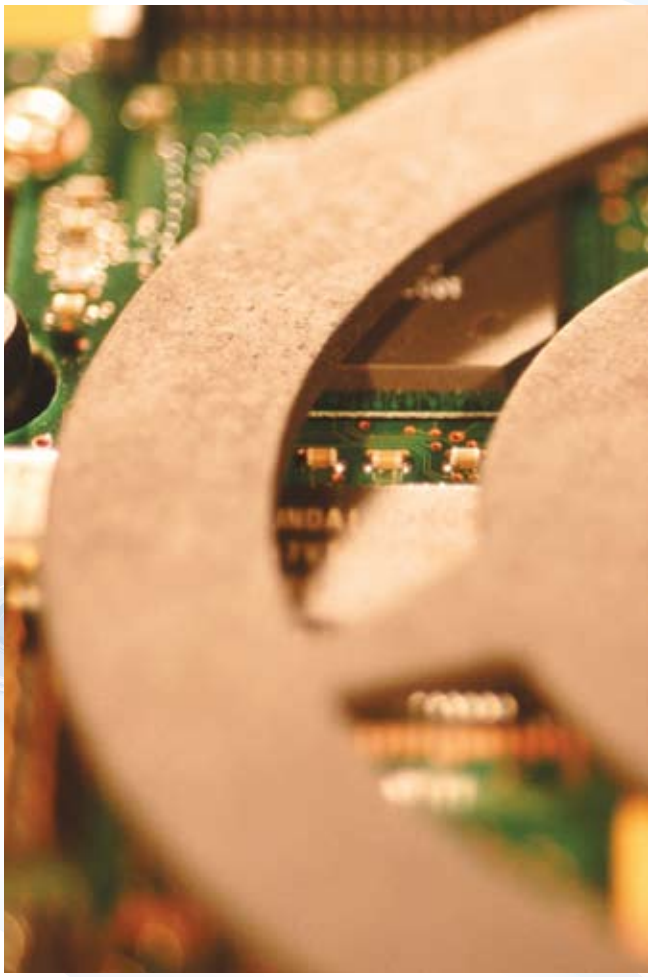
Subsection 14.1.2 stated that the IS aspects of BCM is to identify the events that could interrupt business for which

risk assessment comes into place. The control that should be implemented for this subsection is to identify events causing interruptions to business process along with the impact and probability of such interruptions and their consequences for IS. The implementation guidance for this are stated herein; IS aspects of BC should be based on events that may cause disruptions to the organization business processes; risk assessment to be carried out to determine probability and impact of interruptions to all business processes and include results specific to IS; Based on the result business continuity strategy is to be developed and endorsed by management and subsequently

plan created and again endorsed by management prior to implementation. IS aspects of BCM in Section 14.1.3 is to develop and implement continuity plans. For this subsection the control that should be in place is to develop and implement plans to restore operations and ensure availability of information at required level within required time after an interruption or failure of critical processes. The implementation guidance highlighted that the BC planning process should consider the following ; identification and agreement of all responsibilities and BC procedures; identification of the acceptable loss of information and services; implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; operational procedures to follow pending completion of recovery and restoration; documentation of agreed procedures and processes; staff education in agreed procedures and processes including crisis management; testing and updating of the plans.

Section 14.1.4 is mainly on establishing a BC planning framework. The control emphasizes on maintaining a single framework of BC plans to ensure consistency in all plans, to attend to IS requirements and to identify priorities for testing and maintenance. In general the implementation guidance stated on the approach for each BC plans to ensure information system availability, security, specification of the escalation plan and conditions for activation. Responsibilities to execute plans shall also be considered. All the plans shall be included within the organization change management programme and amended accordingly to cater for changes. Specific owner shall own the BC plans and be responsible for their respective plans.

Section 14.1.5 is on testing, maintaining and re-assessing of BC plans. The control for consideration is to have periodic test and regular updating of BC plans to ensure its effectiveness. On top of all, the implementation guidance stated that it is important for all recovery team members and other relevant staff to be aware of the plans and their responsibility and role when the plan is invoked. On the other hand, test schedule ought to indicate how and when each element of the plan should be tested. Various techniques may be used to ensure plans are executable during crisis. Amongst these are table top testing, simulations, technical recovery testing and testing at an alternate site, test of supplier facilities and services and complete rehearsal or full simulation that integrates all processes and resources to ensure continuity of business for an organization Results should be recorded and changes to be incorporated accordingly and actions taken to improve existing plans.



Audit & Implementation

In the context of BCM implementation, while undergoing the ISO 27001 certification process, among the first items the auditors will look at the existence of a BC plan. In retrospect, during the BCM business impact analysis phase where critical business functions are identified, it is crucial to integrate the organizations' operations, staffing, materials , transport and facilities with the IS requirements as well as other continuity requirements . In BIA exercise, the impact for consequences of disasters, loss of service and availability and security failures are also considered. The auditors will check on the consistency of the reports created and are updated accordingly.

The same goes for the risk assessment stage, where BCM practitioners' should also include controls to identify and reduce the risks. This is to ensure that information required for business processes is readily available. Above all, the main thing that is vital to the auditors is consistency in the plans across the organization and the plans fit into a single high level framework as stated in clause 14.1.4. As for clause 14.1.5, the existing continuity plans need to be tested thoroughly to ensure the plans are working as expected and results of the test can be used to enhance the continuity plans. Isolated components testing can be done in the earlier phase but must be followed by an overall full test simulation that links all the components and ensuring interdependencies are also addressed and tested.

On a different note, although the implementation guidance is referred and followed, the basic thing that needs to be looked at is ensuring all the BCM related documents are reviewed, approved and recorded accordingly following the ISMS procedures and policies by the appropriate management level. It is also important to ensure consistent usage of terms and reference throughout all the related documents.

To conclude, ISO 27001 implementation not only helps to ensure effective security management practices, but also streamlines compliance with BCM. Although BCM is covered in more detail within the BS 25999 standard, but ISO 27002 nonetheless includes additional structural approaches that may strengthen and increase consistency in the BCM overall process and implementation.

References

1. ISO/IEC 27002:2005(E) Information Tech – Security techniques – Code of Practice for Information Security Management

2. An Introduction To Information, Network and Internet Security - Aspects of BCM *http://secutity.practitioner.com/introduction/infosec_7_13_3.htm*

3. The Business value of ISO270K- A case Study by Gary Hinson, CEO of IsecT.Ltd. *http://iso27001security.com/ISO27k_the_business_value_of_ISO27k_case_study.pdf*

4. ISO 27000 NEWSLETTER – ISSUE 14 & 19

EnCase 101: How EnCase Looks at the Time of the Evidence File? [Part 1]

Abstract

Some may wonder the reason we need to find out the suspect's computer time zone setting before we start an analysis. Unlike in the US that observes various time zone setting because of the geographical area and size, Malaysia has only one time zone setting. Nevertheless, there is always a possibility that the suspect's computer's time zone setting may be changed accidentally or purposely. Apart from that, do you know that even the examiner's machines can sometimes change the time zone of an evidence file? Time zone is important because it changes the Modified, Access, Create (MAC) of the evidence file. We know that Operating System, logs most of the user's activities that includes the time when the activities are carried out. It is of great importance that the time of the evidence file is identified, as the suspect may claim he or she is innocent. In this article, what I would like to highlight how examiner's machines can affect the time zone of an evidence file.

Background

This research started based on the report generated from EnCase Forensic Software having an hour difference on the same evidence file, which triggered, the experiment on the software. The case started when a suspect posted a seditious or defamatory comment on a blog and a report was lodged to the police. The police investigated and through the IP address, they managed to locate the suspect, seized his computer and handed it over to me for analysis. The time and date posted on the comment was recorded at 13 February 09 06:45:45PM.

The objective of the case was simple: To find any trace of evidence in the suspect's computer that matched the comment posted on the blog and at the same time matched the given time and date of the incident. During a keyword search, a html file (i_background[2].html) that contained some part of the comment was found. However, the time did not match. It registered an hour earlier than the actual incident time. The BIOS time of the suspect machine was studied and found to have an offset of a few seconds compared to the current time. How do we justify an evidence file that content matches the original post but the MAC time was all offset by an hour? The mystery remained unsolved until two days later when the client called to request for some other evidence from the suspect's hard disk. Another report was re-extracted from the software but the same evidence file now matched the given time of the incident.

Experiment

In order to solve the mystery, an experiment was carried out, which uses the concept of daylight saving time. The basic idea behind DST is to gain more light out of the day by advancing clocks by one hour during the summer. During DST, the sun appears to rise one hour later in the morning.

The only thing that can trigger that kind of setting is time zone setting. For experiment purposes, three machines containing three different time zone settings and the same version of the EnCase Forensic Software were set up. Each was labeled as:

- Machine A: (GMT + 07:00) Bangkok, Hanoi, Jakarta
- Machine B: (GMT +8:00)Kuala Lumpur, Singapore
- Machine C: (GMT +8:00) Beijing, Chongqing, Hong Kong, Urumqi

Target Evidence: An image hard disk containing a windows based OS with a target evidence file named i_background[2].html created under time zone GMT+8:00 Kuala Lumpur on 13 February 09 06:45:45PM

In machine A, a write blocker was attached to prevent data from being written to the original evidence and ran EnCase Forensic Software. The following information was taken from the evidence:

SECTION	i_background[2].html
File Type	html
Full Path	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content. IE5\7MWYJWPL\i_background[2].html
File Created	02/13/09 05:45:45PM
Last Written	02/13/09 05:45:51PM
Last Accessed	02/13/09 05:46:40PM
Entry Modified	02/13/09 05:45:51PM

Then machine A was replaced with machine B and all the steps were repeated. The following result was obtained:

SECTION	i_background[2].html
File Type	html
Full Path	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content. IE5\7MWYJWPL\i_background[2].html
File Created	02/13/09 06:45:45PM
Last Written	02/13/09 06:45:51PM
Last Accessed	02/13/09 06:46:40PM
Entry Modified	02/13/09 06:45:51PM

And then with machine C:

SECTION	i_background[2].html
File Type	html
Full Path	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content. IE5\7MWYJWPL\i_background[2].html
File Created	02/13/09 06:45:45PM
Last Written	02/13/09 06:45:51PM
Last Accessed	02/13/09 06:46:40PM
Entry Modified	02/13/09 06:45:51PM

	Original Sample Setting (GMT+8:00) Kuala Lumpur, Singapore	A (GMT +07:00) Bangkok, Hanoi, Jakarta	B (GMT+8:00) Kuala Lumpur, Singapore	C (GMT +8:00) Beijing, Chongqing, Hong Kong, Urumqi
Create	02/13/09 06:45:45PM	02/13/09 05:45:45PM	02/13/09 06:45:45PM	02/13/09 06:45:45PM
Accessed	02/13/09 06:46:40PM	02/13/09 05:46:40PM	02/13/09 06:46:40PM	02/13/09 06:46:40PM
Modified	02/13/09 06:45:51PM	02/13/09 05:45:51PM	02/13/09 06:45:51PM	02/13/09 06:45:51PM
Last Written	02/13/09 06:45:51PM	02/13/09 05:45:51PM	02/13/09 06:45:51PM	02/13/09 06:45:51PM

Of all the three machines, only machine A showed difference in results.

Conclusion

Based on the experiment, we concluded that EnCase Forensic Software shows the time of the evidence based on the examiner's machine time zone setting. Therefore, it is important before starting the investigation to know the time zone setting of the evidence examined before starting the analysis.

Reference

EnCase ®Computer Forensic II-v6.10pvi(03.16.2009) Copyright ©2009, Guidance Software,Inc.

Why ICT Product Developers and Consumers Should Support the Certified ICT Products

Introduction

- **The Dilemma of ICT Product Developers and Consumers**

  In current Information Technology world, no entity is immuned from being announced in the next "The Breach of Information Security" headline. There is no assurance in the security protection that is blending within the ICT product. Indeed, without this assurance, there would be serious economic risks for information processing systems which are vitally essential in the day to day life such as payment cards for the banking activities, SIM card in the world of mobile telecommunications, health card, and protection of the networks. As of July 2009, according to the incidents reported to Malaysian Computer Emergency Report Team (MyCERT), there was 1971 number of cases reported based on the general incident classification like denial of service, fraud and forgery, vulnerability probing, malicious code, system intrusion, etc. From such scenario, it shows that no one can escape from these 'virtual' deceases.

  On the other hand, many ICT consumers lack of knowledge, expertise, or resources necessary to judge whether their confidence in the security of the IT products or systems is appropriate, and they might not wish to rely solely on the assertions of the developers. Therefore, consumers might choose to increase their confidence in the security measures of an ICT product or system by acquiring an analysis of its security. So how does one prevent data security breaches?

  Reflecting from this situation, the government has made a wise and efficient step by commencing the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme as a way to enhance the National cyber security. Certified products provide grounds for confidence that they: will meet consumer security needs; function as specified; have adequate guidance; can be operated securely; have been built correctly; have been delivered as requested; has been thoroughly tested; and have reduced the potential for exploitable vulnerabilities in their implementation. However, it does not mean that the evaluated and certified product is totally free from exploitable vulnerabilities. There remains a residual level of risk that exploitable vulnerabilities remain undiscovered in the TOE's claimed security functionality. This residual risk is reduced as the certified level of assurance increases for the ICT products and systems.

- **Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme**

  The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme is a systematic process for evaluating and certifying the security functionality of ICT products and systems against ISO/IEC 15408 standard which is known as Common Criteria (CC). The usage of the recognise ISO standard ensures that MyCC Scheme certified products which can be found in MyCC Scheme Certified Products Register (MyCPR) at *www.cybersecurity.my/mycc/mycpr.html* will become the world standard in security specifications and evaluations. In addition, it helps the developer to improve the competitiveness of their ICT products in the global ICT market.

Security evaluation of ICT products and systems is conducted by the licensed and accredited evaluation facilities which are known as Malaysian Security Evaluation Facilities (MySEFs). MySEF can be a commercial or government entity that is independent from the product developers. MySEF shall be operated in an independently accredited environment based on MS ISO/IEC 17025 and within the MyCC Scheme rules. The

main role of MySEF is to conduct a specific and a well-mannered plan of the security evaluation on Target of Evaluation (TOE) which is the ICT product or a consumers' specification which is call Protection Profile (PP).

In addition, MySEF may also provide consultancy services on how CC standard is to be applied in the development environment and how consumers' requirements can be communicated to developers. This will ensure that all development documentation, and the evaluation scope are determined based on CC requirements. The evaluation process is completely independent and conforms to a methodology which is known as Common Evaluation Methodology (CEM) or ISO/IEC 18045. During the evaluation process, the evaluator team works on the product, and documentation to find whether it is internally consistent, properly functioned and performed like what has been claimed by the developer. The results of the evaluation are recorded in the Evaluation Technical Report (ETR) and will be submitted to the MyCC Scheme Certification Body or what we call Malaysian Common Criteria Certification Body (MyCB) for the certification process before the evaluation process closed.

MyCB is an impartial body within the MyCC Scheme that is responsible for carrying out certification and for overseeing the day-to-day operation of MyCC Scheme. The certification process includes the acceptance of the products to be evaluated and certified under the MyCC Scheme, oversee the evaluation process, and certifying the evaluation results.

Benefits to the Consumers

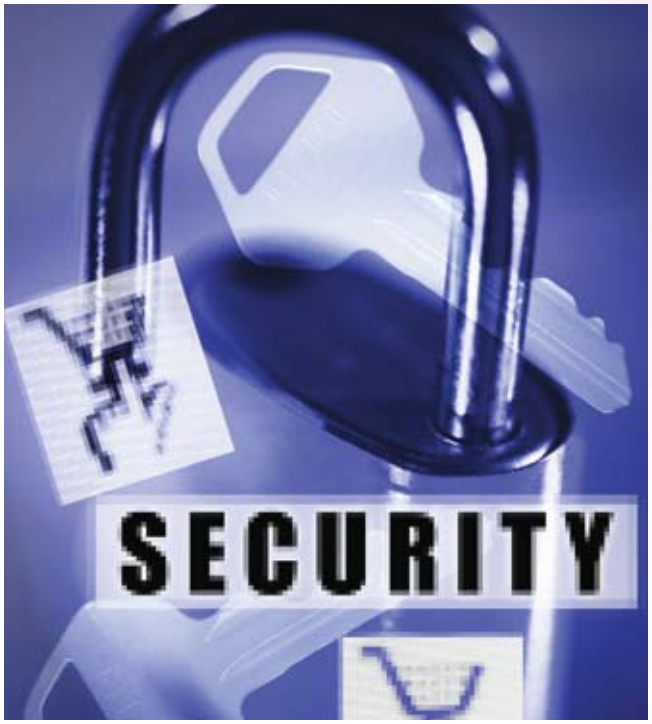
The Common Criteria provides a mechanism for ICT consumers to express their security needs to developers for a type of ICT products such as firewall, operating system and others in an unambiguous manner. This is what we call a Protection Profile (PP). A PP develops by a consumer defines a minimum set of security functionality that must be implemented in a type of product. The PP needs to be evaluated and certified to ensure that it is complete, consistent, and technically sound and suitable for use as a template on which to build another PP or a type of an ICT product.

During acquisition, consumers need to check whether an ICT product has been successfully evaluated, and whether it is developed based on the consumer's requirements or PP. By using a PP, the customers can make the right decision in procuring the right ICT products. It also builds the consumers' confidence towards the quality and security of ICT products and systems through rigorous independent security evaluation. By getting the certification, the user would get the answers on queries such as the safety and the suitability of the product for the user.

Benefits to the Developers

The main goal of an independent security evaluation to the developers is to validate the security claims of their ICT products or systems. CC allows the security evaluation of an ICT product or system to obtain a level of confidence that the security functionalities claim by the developer. The developers could fulfil their customers' needs by producing the ICT product or system based on the PP. First, they need to develop a document that includes the security needs for a specific identified product or system. This document is called Security Target (ST). The Security Target contains a summary specification, which defines the specific measures taken in the product or system to meet the security requirements. Security Targets is actually designed to answers questions such that revolves around the developer capability to produce such product, the way product is tested and its evaluation processes. Furthermore, by constructing the ST, the developer has a guideline to produce a secure ICT product or system that meets the consumers' needs.

The developers will also use the CC to determine the scale for measuring assurance level for their ICT product or system which is called the Evaluation Assurance Levels (EALs). EALs consist of an appropriate combination of the assurance components as describe in Part 3 of the CC. Basically, there are seven hierarchically ordered EALs defined in the CC, where higher EAL represents more assurance than the lower EALs. The complexity of evaluation process increased based on the EAL, evaluation scope and complexity of the product or system. Most of the developers have chosen to contribute until EAL4+ evaluation because there is no standard and recognize methodology for EAL5 and above.



Independent security evaluation and certification will help the developer to gain access to new markets and make their product different from other similar type of products. Moreover, the ICT products or systems produced are more robust because the security flaws discovered during the evaluation are rectified.

Conclusion

Malaysian consumers and developers will gain a lot of benefits from the MyCC Scheme certification. Besides obtaining the global recognition and acceptance, the security engineering practices for the ICT product or system development will be improved. Certification shows that the security functionalities of an ICT product or system has been evaluated based on the defined scope, and verified that it met the developer's claim. Therefore, the deployment of certified products or systems based on the Certification Report and Security Target can increase the confidence level of consumer that they: will meet consumer security needs; function as specified; have adequate guidance; can be operated securely; have been built correctly; have been delivered as requested; has been thoroughly tested; and have reduced the potential for exploitable vulnerabilities.

References

1. Part 1: Introduction and General Model, Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3, July 2009, *http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf*
2. MyCC Scheme Policy (MyCC_P1), version 1, May 8, 2009, *http://www.cybersecurity.my/mycc/document/MyCCP1.pdf*
3. Reported Incidents based on General Incidents Classification Statistic 2009, MyCERT Statistic July 2009, *http://www.mycert.org.my/en/services/statistic/mycert/2009/main/detail/625/index.html*
4. Motoshi Saeki, Haruhiko Kaiya "Using Common Criteria as Reusable Knowledge in Security Requirements Elicitation", 2008, *http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/paper09.pdf*
5. Ariffuddin Aizuddin "The Common Criteria ISO/IEC 15408 The Insights, Thoughts, Questions, and Issues", *http://www.cybersecurity.my/data/content_files/13/68.pdf?.diff=1176418091*
6. Common Criteria and Protection Profile: How to Evaluate Information, 2003, *http://www.sans.org/reading_room/whitepapers/standards/common_criteria_and_protection_profiles_how_to_evaluate_information_1078*
7. Thuy D. Nguyen, Timothy E. Levin, and Cynthia E. Irvine, "High Robustness Requirements in a Common Criteria Protection Profile", *http://cisr.nps.edu/downloads/06paper_highrobust.pdf*
8. Ross Anderson, "Why Information Security is Hard - An Economic Perspective", 2001, *http://www.acsac.org/2001papers/110.pdf*
9. Richard E. Smith, "Trends in Government Endorsed Security Product Evaluations", October 2000, *http://www.cryptosmith.com/docs/evaltrends.pdf*
10. Jennifer deJong, "Common Criteria or Common Confusion - Misperceptions about the global security standard abound", June 2005, *http://www.ghs.com/ download/articles/GHS_common_criteria_060105.pdf*

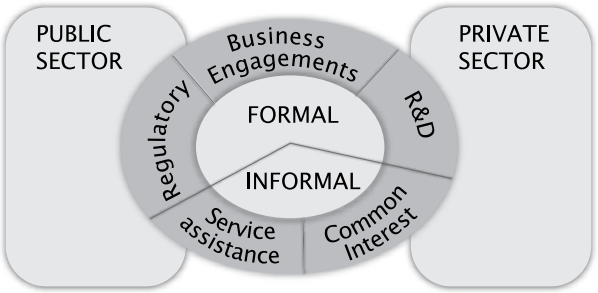
Towards an Effective and Efficient Public and Private Cooperation Within The Critical National Information Infrastructure

Introduction

The National Cyber Security Policy (NCSP), a policy endorsed by the government to protect the Critical National Information Infrastructures (CNII), defines the country's CNII as real or virtual assets. These systems and functions are vital to the nation that their incapacity or destruction would have a devastating impact on the national economic strength, image, defense and security, government capabilities to function, and the public health and safety. The NCSP has identified ten critical sectors as the CNII, namely National Defense & Security, Banking & Finance, Information & Communication, Energy, Transportation, Water, Health Services, Government, Emergency Services, and Food and Agriculture.

The complexity and interdependency of the CNII is becoming more visible and unavoidable. It is observed that Malaysia's critical information infrastructures are mainly operated by private stakeholders due to Malaysia's privatization policy. As a result, the situation requires an effective Public Private Cooperation (PPC) among the CNII operators and the government to ensure that the CNII are adequately protected.

There are a number of issues with regards to the cooperation between the private and the public sector. These issues include the unwillingness of agencies and organizations to share sensitive information such as information on cyber security incidents and system vulnerabilities. This is due to the perception and belief that by exposing such information, it will have negative impacts on their organizations. Another relevant factor that can be considered as a restrictive factor in nurturing the cooperation between both sectors is the different level of understanding on information security itself.
To overcome these issues, five models of the PPC have been proposed by the NCSP as shown in the diagram below.



The formal PPCs are the Regulatory PPC Model, the Outsourced PPC Model, and also the Research & Development (R&D) Cluster PPC Model. While the Information Security Assistance PPC, and the Common Interest Group PPC Models are the informal PPCs. These PPC models are expected to foster the joint cooperation efforts in protecting the CNII, at the same time building trust in sharing information and resources between the public and the private sectors.

The Regulatory PPC Model

This model recommends that there should be a "sector lead" empowered with regulatory authority and governed by legislations to lead the cooperation efforts between both the public and the private sectors. The sector lead has to identify the private sectors that fall under its jurisdiction. The model requires cooperation within the industry or each sector to practice good governance in their decision making process. Information sharing, awareness, co-formulation of policies and guidelines and capacity building are some possible areas of cooperation. Examples of sector leads in Malaysia would be the *Bank Negara* for the Banking and Financial sector and the Malaysian Communications and Multimedia Commission for the Information and Communication Sector.

The Outsourced PPC Model

This model proposes that government agencies to outsource certain services to the private sector service providers. These include consultancy services, security audits, or technical support both in hardware or software. These service providers are paid for the services rendered and there should be some guidelines in order to ensure the protection of secrecy and privacy.

The R&D Cluster PPC

This model refers to the cooperation between research institutions, universities and the public and private sectors. By utilising funding from various sources, it promotes collaborative research in information security. Some incentives from the government could foster an R&D culture among researchers. An example is MIMOS Bhd, the R&D organisation that functions as an advisor to the Malaysian Government on technologies, policies and strategies relating to technology development, is a good example of this model with the aim to nurture research and development in information security.

The Information Security Assistance PPC Model

This model is driven by the Not for Profit (NFP) organisations, where the Information Security Assistance PPC Model is mainly supported by the government. The services are widely open to the public, private and also the community. CyberSecurity Malaysia is the best example of this type of PPC Model. With 'Securing Our Cyberspace' as its tagline, the organisation has a number of services to offer. These services are open to be employed by the community.

The Common Interest Group PPC Model

Infosec.my, a knowledge sharing session organised by CyberSecurity Malaysia, is a good example to illustrate this model, where parties (from the public and private sectors) or a community with a common interest gather in meet to discuss and share their knowledge and experience pertaining to information security matters. Another example is the SIRIM national technical committee on information security standards (TC5), which monitors and participates in the international (ISO) information security standards, setting process and recommends adoption or adaptation of such standards for Malaysia. Members of these committees, such as TC5, comprise of representatives from the public and private sectors, promoting a high level of consultative process in reviewing standards and guidelines.

These foregoing PPC Models were designed with the aim to foster joint cooperation efforts in protecting the CNIIs and building trust in sharing information and resources between the public and private sectors. Since the majority of the nation's critical infrastructure is operated and owned by the private sector, the public-private cooperation has been identified as one of the key initiatives in protecting the CNII. However, this can only be successfully accomplished and achieved if the government, which has the responsibility of protecting the national critical infrastructure, can offer a trusted, well-organized, efficient and reliable networking platform to the private sector, covering all relevant aspects from battling misdemeanors and early warnings, to standards development, knowledge sharing, technical expertise and support.

In conclusion, the cooperation between the private sector and the public sector is essential as both sectors are dependent on each other to ensure the nation's critical information infrastructure is protected. The most important element in the cooperation is that trusted information sharing should be instituted between the public and private sectors, exchanging information such as specific threats, awareness raising, exercises, recommendations and so forth. The information sharing exchange would be effective and efficient if the public and private sectors are willing to collaborate more and trust one another. If this can be done, the CNII of the country would be more resilient in the future.

Reference

Ministry of Science, Technology and Innovation (2006). A Study on the Development of the National Information Security Policy

The Curious Case of Service Packs Effects on Vulnerability Scanning for Windows 2003

Background

Despite the availability of newer Windows operating system, a lot of corporate environment is still running Windows 2003, serving web pages, hosting databases, running web applications and email services, not to mention DNS and other network infrastructure services. Although, it is not the latest Microsoft Windows server operating system, the number of corporations that still runs it and has not upgraded to Windows 2008, makes this version of Windows a very relevant target for vulnerability assessment study.

Objective

We set out to find the vulnerabilities that are present on a newly installed Windows 2003 with no service packs, no extra applications installed, and no firewall running on the machine, which will be our baseline or reference installation in the future.

Our objective is to find out any decrease (or increase) in the number of detected vulnerabilities after applying Service Pack 1 and Service Pack 2 on the target Windows 2003 machine.

We have to pick a vulnerability scanner for the test and Nessus was a natural choice. Nessus is a popular security auditing tool used by professional security testers and novices alike. It comes in two types, the free so called Homefeed version and the paid by subscription Professional Feed. We were curious whether there is any significant difference between vulnerabilities found by Nessus vulnerability scanner with Homefeed (free) and Professional Feed (paid by subscription).

The Scenario

First, we set up a virtual machine running Windows 2003 SP0 with no installed applications as the target. A second virtual machine with BackTrack 3.0 and Nessus 3.2 installed serves as the penetration tester's machine. BackTrack is a Linux distro with a collection of security assessment tools pre-installed. Unfortunately, Nessus did not come as a standard install.

When everything is ready we ran Nessus vulnerability scanner against the Windows 2003 virtual machine and the results were analyzed for high risk or critical vulnerabilities.

What we tested

First, we used Nessus vulnerability scanner with the free home-feed type plugins and updated just prior to running the scan. All plugins were selected including the unsafe checks. The aim was to throw everything at the Windows 2003 target without worrying about bringing the machine down. Both Microsoft patches check scan and the default complete scan were used.

Subsequently, Service Pack 1 was applied to the target and Nessus vulnerability scanner was once again run against it.

Next, the same test was repeated after Service Pack 2 was applied to the target.

We entered the administrator password into Nessus vulnerability scanner configuration to enable local checks to be performed and each scan was run twice to enhance confidence and ensure repeatable results.

When we were done with the free home-feed plugins the whole scan was repeated again using the Professional feed.

The Result

The results came back with some expected findings and a few unexpected ones too. The table below contains our findings.

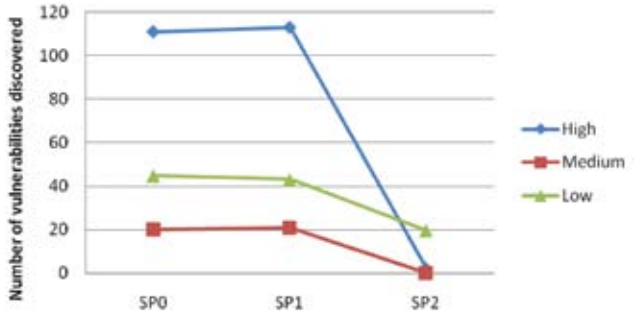
Scan Type	Windows 2003 SP0 number of vulnerabilities found	Windows 2003 SP1 number of vulnerabilities found	Windows 2003 SP2 number of vulnerabilities found
Nessus Home Feed (Microsoft Patches scan)	High: 111 Medium: 20	High: 113 Medium: 21	High: 2 Medium: 0
Nessus Home Feed (Default scan)	High: 111 Medium: 20	High: 113 Medium: 21	High: 2 Medium: 0
Nessus Professional Feed (Microsoft Patches scan)	High: 111 Medium: 20	High: 113 Medium: 21	High: 2 Medium: 0
Nessus Professional	High: 111	High: 113	High: 2
Feed (Default scan)	Medium: 20	Medium: 21	Medium: 0

The scan results are consistent for high and medium vulnerabilities across all scan types (Microsoft patches and default scans) and across plugin feed types (home-feed and professional feed). The results also show, there was no direct relation between the scan results and the types of vulnerability scanner applied.

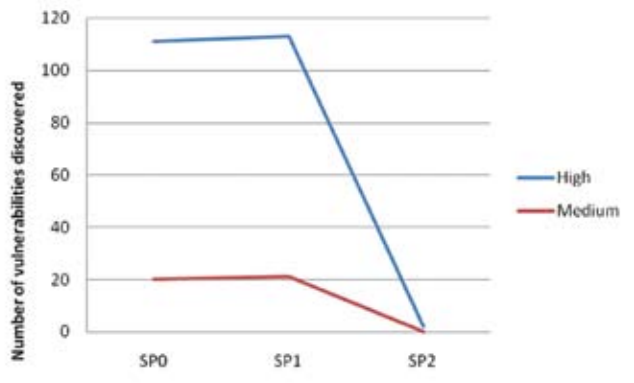
The effect of applying service packs on the number of high and medium vulnerabilities is not very noticeable going from SP0 to SP1. In fact, from our observation, the number of high vulnerabilities increases by two and medium vulnerabilities increases by 1 if you upgrade to SP1 from SP0. The scenario illustrates that not only will you not improve your security by applying SP1, you will actually be worse off than if you have chosen to remain with SP0.

The security improvements after applying SP2 is very noticeable if you look at the number of high and medium vulnerabilities discovered after the upgrade. The high and medium vulnerabilities have decreased sharply to 2 and 0, respectively.

The following chart shows these results.



There are minor variations in the number of low vulnerabilities discovered. To simplify the analysis and for the purpose of easy comparison, the number of low vulnerabilities has been averaged out across different scan types and plugin feed types in the chart below.



Conclusion

It can be concluded from this vulnerability scan results analysis that a significant reduction in the number of high and medium vulnerabilities can be achieved if an installation of Windows 2003 server is applied with service pack 2. In addition, the result also shows, it is not advisable to apply service pack 1 because the number of vulnerabilities will increase after the upgrade, which is indeed puzzling.

Reference

http://www.nessus.org/nessus/

Email Header Analysis

Introduction

Nowadays, everyone has his or her own personal email address. Emails are used for personal and professional communication. Email can be sent through application based such as Mozilla Thunderbird, Microsoft Outlook, Lotus Notes or through web based email client like Gmail, Yahoo, Hotmail, and Operamail. Almost all web based email clients are free for registration and this leads to the increasing of the email users in the world, which can potentially translate to more illegal activities such as spamming, phishing, slanderous emails, etc. There are two components when a person sends out an email, email header and message body (the content of the email).

What is email header?

When you send an email, extra information will be included in the email itself. The information is stored in the upper section of the email, which we call an email header. The email header contains details of the sender, route or path the email took and the receiver. This information is useful especially when we want to trace the information about the sender such as the IP address and the time, which the e-mail was sent out.

```
Delivered-To: fauzixxxxxxxx@gmail.com
Received: by 10.142.bbb.aa with SMTP id v15cs452525wfg;
        Wed, 3 Jun 2009 01:33:20 -0700 (PDT)
Received: by 10.100.bbb.a with SMTP id g8mr728457anc.66.
        Wed, 03 Jun 2009 01:33:09 -0700 (PDT)
Return-Path: <fauzixxxxxxxx@yahoo.com>
Received: from web57613.mail.re1.yahoo.com (web57613.mai
        by mx.google.com with SMTP id 5si737382ywd.45.2C
        Wed, 03 Jun 2009 01:33:07 -0700 (PDT)
Received-SPF: pass (google.com: domain of fauzixxxxxxxx
Authentication-Results: mx.google.com; spf=pass (google.
Received: (qmail 52248 invoked by uid 60001); 3 Jun 2009
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=
DomainKey-Signature:a=rsa-sha1; q=dns; c=nofws;
  s=s1024; d=yahoo.com;
  h=Message-ID:X-YMail-OSG:Received:X-Mailer:Date:From:S
  b=uOMTNZHXQfP8qsf+xENLevXyL1YRQFnVIhioC1xVS1KK1zeinPPt
Message-ID: <237846.50609.qm@web57613.mail.re1.yahoo.com
X-YMail-OSG: w5cSt_kVM1kIsD5N.hovjhODrY3Lw8shFB22WjzIwmr
Received: from [61.6.bbb.aa] by web57613.mail.re1.yahoo.
```

Figure 1: Basic Concept of Quantum Cryptography System.

Figure 1 above shows a typical email header of Gmail. In an email header, it is mandatory to have these four fields:

- FROM – the sender's name and email address
- TO – the recipient's name and email address
- DATE – the date when the email was sent
- SUBJECT – the subject of the email

Although these four fields are mandatory but they can easily be spoofed. In year 2003, a worm code name *W32.Sobig.F@mm* successfully altered the FROM field by using ***admin@internet.com*** as the sender and sent emails to all contacts found in the victim's address book. Then the recipient of the infected email sent emails to all the contacts found in that computer and this process followed suit producing a massive chain-reaction.

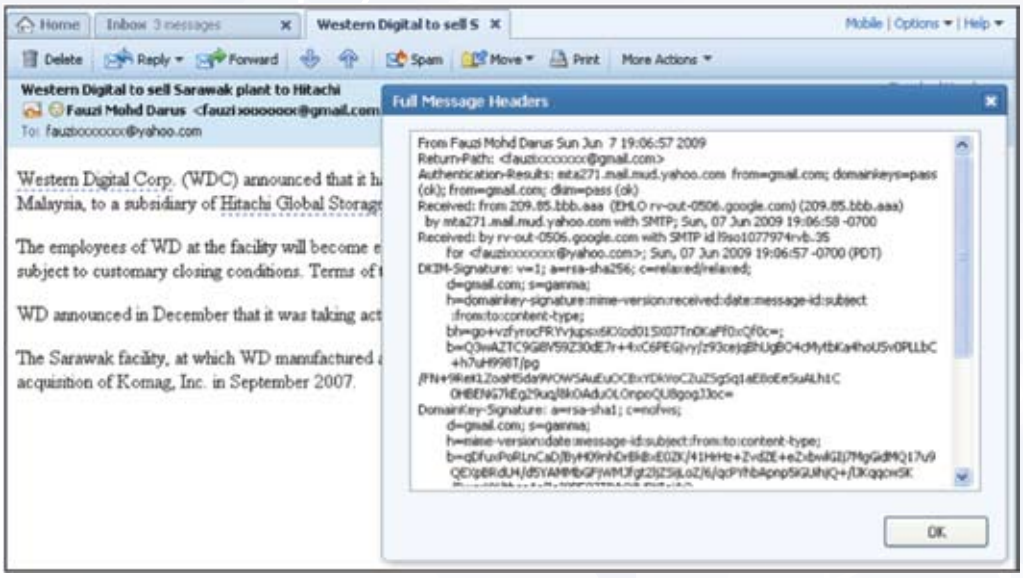


Figure 2: Message Body and Message Header of an Email

Other than these four fields, sending time stamps and receiving time stamps by the email agents that have received and sent the email are also included in the email header. This information is automatically inserted by the email agents.

The time stamp field also can be spoofed. However, the detection of timestamp spoofing is fairly easy.

The analysis

Let's use the email header in Figure 3 as our example of analysis. The highlighted lines (lines begin with the "Received:" tag) will help us to trace the sender of the email. To read the email header, we start from bottom to top as the last time stamp was inserted at the top of the email before it is delivered to the receiver.

Figure 3: Email Header Analysis

As we can see in the Figure 3 above, there are four lines that show the time stamps that where inserted by the email agents when received and forwarded it to next email agent until it reached to the receiver.

The first time stamp shows the email was sent from IP address 61.6.bbb.aa, which is the IP of the ISP of the sender and received by Yahoo mail server, web57613.mail.re1.yahoo.com (66.196.bbb.aa). We believe that the email was sent from a web browser based on the "HTTP" at the end of the line.

Then in the second line, Yahoo mail server forwarded the email to cybersecurity.my (192.228.bbb.a). From cybersecurity.my the email was then forwarded to another mail server, 172.20.b.aaa. Finally, the email was delivered to the recipient from mail server with IP 172.20.b.aaa.

Furthermore, you can see another tag in the email header called "X-Originating-IP". This tag indicates the real IP address of the email sender.

In short, the email route can be summarized as below.

From: fauzixxxxxxx@yahoo.com
To: helloworld@cybersecurity.my
IP: 61.6.bbb.aa
Date: Wed, 3 Jun 2009 01:33:07 -0700 (PDT)

Mail Server: web57613.mail.re1.yahoo.com [66.196.bbb.aa]
Received From: 61.6.bbb.aa
Delivered To: cybersecurity.my
Date: Wed, 03 Jun 2009 01:33:07 PDT

Mail Server: cybersecurity.my [192.228.bbb.a]
Received From: web57613.mail.re1.yahoo.com 66.196.bbb.aa]
Delivered To: 172.20.b.aaa
Date: Wed, 03 Jun 2009 01:33:07 -0700 (PDT)

Mail Server: 172.20.b.aaa
Received From: cybersecurity.my [192.228.bbb.a]
Delivered To: helloworld@cybersecurity.my
Date: Wed, 03 Jun 2009 01:33:09 -0700 (PDT)

Delivered To: helloworld@cybersecurity.my
Date: Wed, 3 Jun 2009 01:33:20 -0700 (PDT)

Figure 4: Email Route Information

References

RFC5335 - Internationalized Email Headers

http://email.about.com/cs/spamgeneral/a/spam_headers.htm

http://www.emailaddressmanager.com/tips/header.html

File Deletion in Linux

Introduction

Nowadays, Linux is becoming more popular as it is an operating system which is more reliable and secure compared to Windows. However, for new computer users, Windows is still much easier to use as users do not have to bother to know about the source code of the operating system when using Windows. On the other hand, those using Linux need to know some commands even to delete a file.

In this article, targeted for Linux beginners, the discussion will revolve around the process of deleting a file or directory and what happens to the file or directory after the deletion.

Files can be deleted from the Linux/ Unix console by using the 'rm' (short for remove) command. By default, this command deletes a file without confirmation from user.

$ rm filename
This command immediately deletes a file in the current directory without prompting.

$ rm filename1 filename2
This command allows user to delete more than one file at once.

$ rm -r directory
The -r flag is used to recursively remove directories and subdirectories in the argument list. The directory will be emptied of files and removed. The user is normally prompted for removal of any write-protected files which resided in the directory. This -r flag actually is a permission for rm to delete directories, their files and their subdirectories.

$ rm -f filename
Another rm flag is -f, which will remove all files in a directory whether it is write-protected or not and it will remove all your files without prompting the user.

$ rm -i filename
The -i flag is used to ensure that rm prompts for confirmation before removing any file.

Be careful with the rm command, since the multi-user nature of Linux does not have an undo command. Once you have deleted a file, it will be gone for good, unless you use the recovery software.

What happens after deletion?

- **File Deletion under EXT2/3**

What happened to the files after being deleted? In Windows, all the deleted files go straight into the Recycle Bin. However, in Linux only files that had been deleted from the GUI will go to the Trash folder. In actual fact, the files are not lost unless they are overwritten, which includes the rm command file. Before I the discussion goes any further, it's better for you to understand the important data structures in Linux.

By default, Linux use EXT3 as its file system, but it also uses EXT2. EXT3 is the new version of EXT2 with journaling mechanism. Journaling keeps track of the major steps taken during the last sessions with a file and it also can be booted up to the last configuration and recover it to the point of crash.
The boot record in Linux is called Superblock. Linux divides the drive into block groups and a copy of the Superblock is frequently found at the beginning of these block groups.
Linux also distributes information fairly evenly across the drive (it does not use a first-come-first-serve file allocation method).

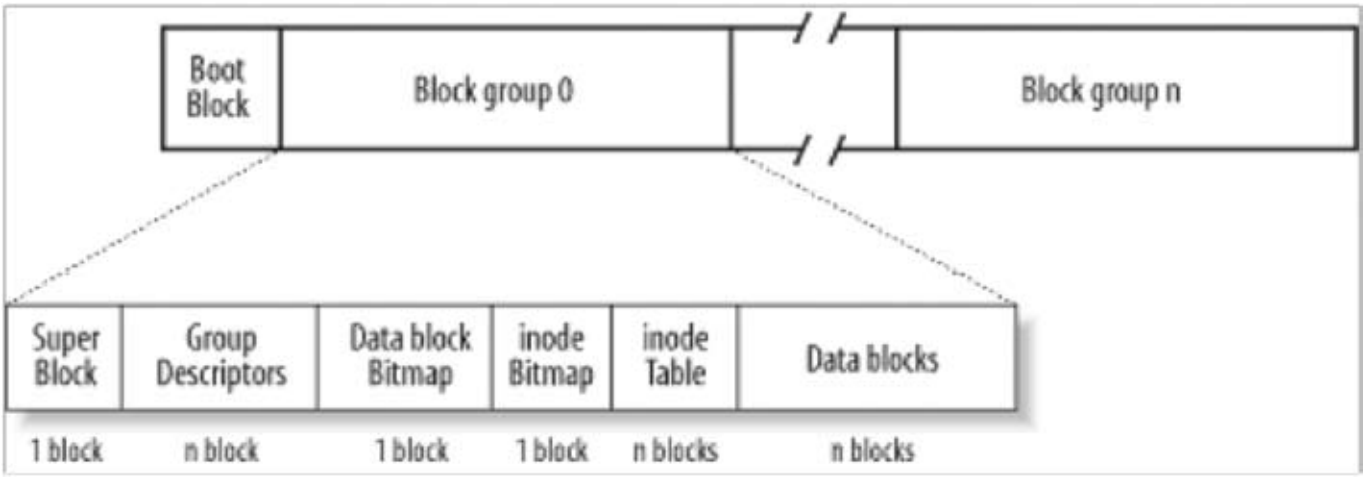


Figure 1

- **Superblock**
  The first logical drive which stores information about the number of free blocks, inodes, block size and other information related to file system.

- **Group Descriptors**
  Includes information of each group, located after the Superblock. Each group descriptor describes one group.

- **Blocks Bitmap**
  The block bitmap keeps track whether each block is in use or not.

- **Inode Bitmap**
  The inode stores all information about a file. A fixed number of blocks are usually allocated for storing the inode Table, which stores all the file inodes. The in odes also contain pointers to disk blocks where the actual files are stored. The inodes bitmap is provided to check for allocated blocks and free them when files are deleted from the system.

- **Inode Table**
  Inode Table contains Meta information about the file. This information includes the filename, the filesize, a pointer to the disk blocks containing the file, the file creation, access and modification times, the number of links to the file, as well as the user and group ids of the file.

"The inode contains 15 pointers to blocks where the first 12 are direct pointers to content blocks. Another pointers will have 1 indirect pointer to data and the next one points to `a block of pointers' to `blocks of pointers' to a double indirect. Indirect and double indirect block pointer will be used to support larger files. Refer figure 2."

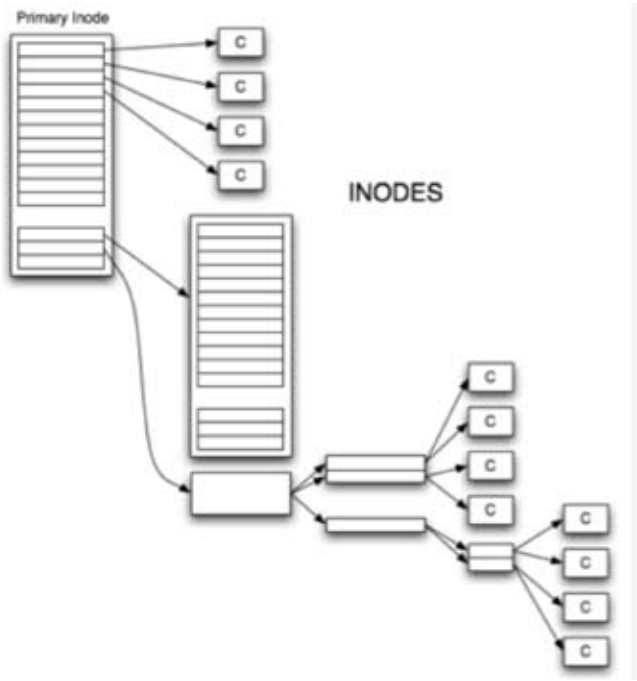


Figure 2

When you delete a file, the inode status is set to zero. If a process has a hold of the file, it does not displace the inode. It breaks the link between the directory entry and the inode. That file now can be called an orphan as it does not have a parent anymore. There is an inode orphan list in the Superblock. When you reboot the computer, the orphans will be unallocated.

There's a difference between EXT2 and EXT3 in terms of unloading an inode. EXT3 will wipe the inodes, so block number will be lost while EXT2 doesn't wipe the inodes (similar to FAT). EXT2 will adjust previous directory entry length to obscure deleted record. Refer figure 3.

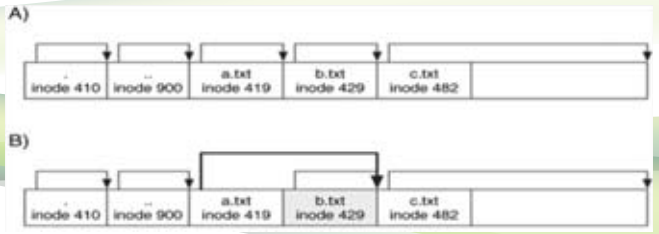


Figure 3

Conclusion

Unlike Windows, Linux operating system drivers clean the part of inode information after file is deleted and fills it with zero object size, object type information and object allocation information. This means after a file is deleted, the software knows nothing about it. But, recovery is still possible as there are a set of recovery methods that could help with file recovery, but none can give 100% assurance that the deleted files can be recovered.

References

http://thinkdifferent.typepad.com/edulog/computer_forensics_i/

http://lowfatlinux.com/linux-delete-files-rm.html

http://www.computerhope.com

Malicious Macromedia Flash File Analysis

Introduction

Macromedia Flash File Format (SWF) is designed to deliver vector graphics and animations over the internet through web browsers. Unfortunately, the availability of SWF files playing perfectly on any platform's browser has brought the attention of the malware writers. In 2008, antivirus companies and security research centers including SecurityFocus [1], McAfee [2], and SANS [3] have reported in-the-wild exploitation of the SWF vulnerability. For details on this vulnerability could be witnessed in CVE-2007-0071 [4]. According to Mark Dowd, IBM Internet Security Systems researcher, Adobe Flash Player version 9.0.115.0 and earlier, are prone to memory corruption issue when processing a malicious Shockwave Flash (SWF) file. The successful attack will allow arbitrary code to run through an exploitable NULL-pointer dereference and compromise the infected computers. This document shows the in-depth process of analyzing malicious SWF files.

Useful Tools for Analysis SWF File

In this section, the useful tools for conducting analysis process will be listed. The analysis machine installed with the tools is as below:

- SWFTool [5] – Collection of utilities for working with Adobe Flash files (SWF files)
- IDA Pro - Disassembler for static analysis
- OllyDbg - Debugger for dynamic analysis
- Hex Workshop for hex view

Overview

A lot of malware writers from China abused the Adobe Flash Player vulnerability to develop their own exploit generators resources. These exploit generators can be kept by the writers for personal usage or sale in the underground black market forum. Figure 1 shows the example of a SWF File Exploit Generator for Adobe Flash Version Win9, 0,115,0ie.

Figure 1: Flash Exploit Generator

The malware writers uploaded and ran the malicious SWF files in the vulnerable web server – so called malicious server. The attack started with injecting the embedded Uniform Resource Locator (URL) into third party domain's web pages through SQL injection [7] or IFrame Injection [8]. The embedded link will automatically redirect victim to the malicious server, which hosts the malicious SWF files. Then the link will exploit the vulnerability and install the trojan or backdoor in victim's computers if the victim is using vulnerable Adobe Flash Player.

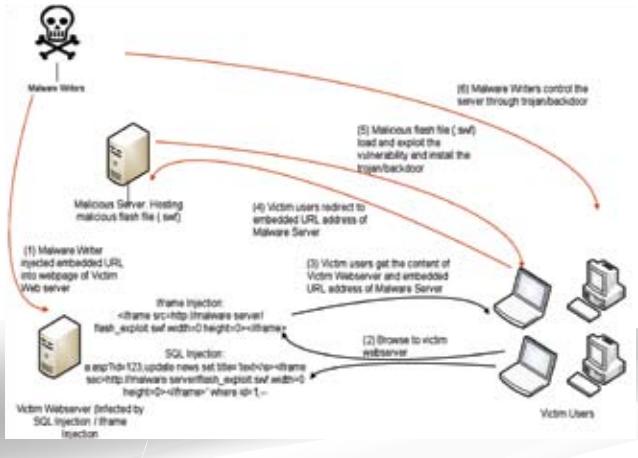


Figure 2: Flash Exploitation Attack through SQL Injection / IFrame Injection

In this section, the useful tools for conducting analysis process will be listed. The analysis machine installed with the tools is as below:

- Malware writers launched an attack to the victim's web servers and planted an embedded URL that is linked to malicious server through SQL injection or IFrame Injection attack.
- Once the users browsed the web server, the browser will redirect to the embedded URL hosting malicious SWF files.
- The malicious SWF files will be downloaded and exploit the vulnerable Adobe Flash Player application and install Trojan or Backdoor into the victim's computer.
- Malware writers will able to connect and compromise victim's computer through the installed backdoor or trojan.

Analysis of Malicious SWF File

The analysis is divided into two parts. The first part will explain the steps on extracting embedded SWF file and locating the decryption routine of the shellcode. The following steps will describe the decryption of obfuscated shellcode and its payload. Figure 3 shows the original screenshot of malicious SWF file in hex view.

- **Extracting Malicious Code from SWF File**

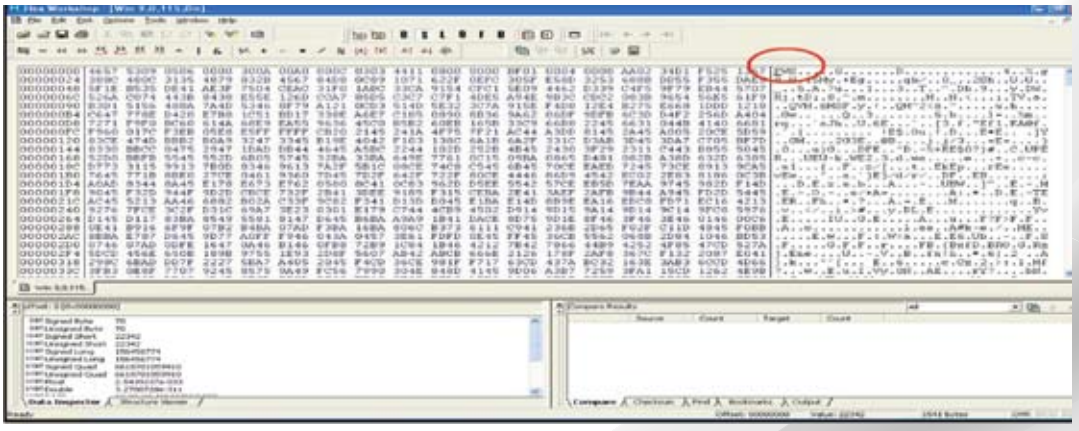
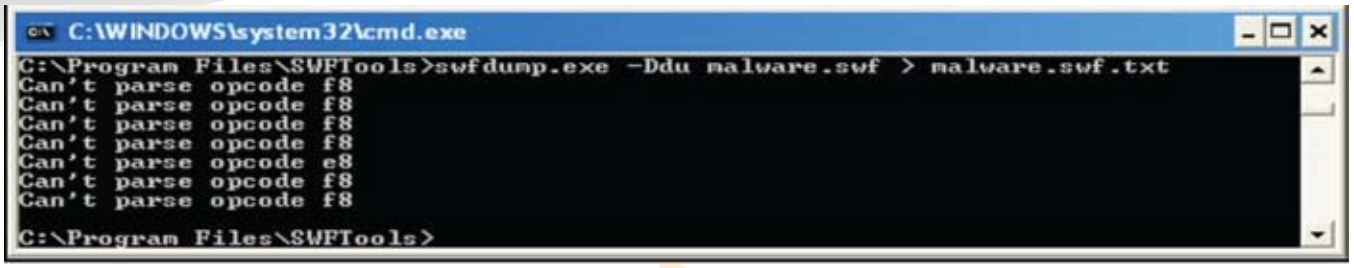


Figure 3: Original Screenshot of Malicious SWF File

The complete SWF binary structure [9] as shown below:

[FWS/CWS] [Version] [Length] [Header] [Tag Code + Length] [Tag Contents] […..[0]

The SWF file starts with string FWS. An FWS signature indicates an uncompressed SWF file [10] but it is still unreadable. The software - swfdump.exe can be used to see the tag and DEFINEBITS section where the obfuscated shellcode is located [11].



DEFINEBITS section indicates the starting opcode and end opcode of the obfuscated shellcode as shown in Figure 4 and Figure 5.

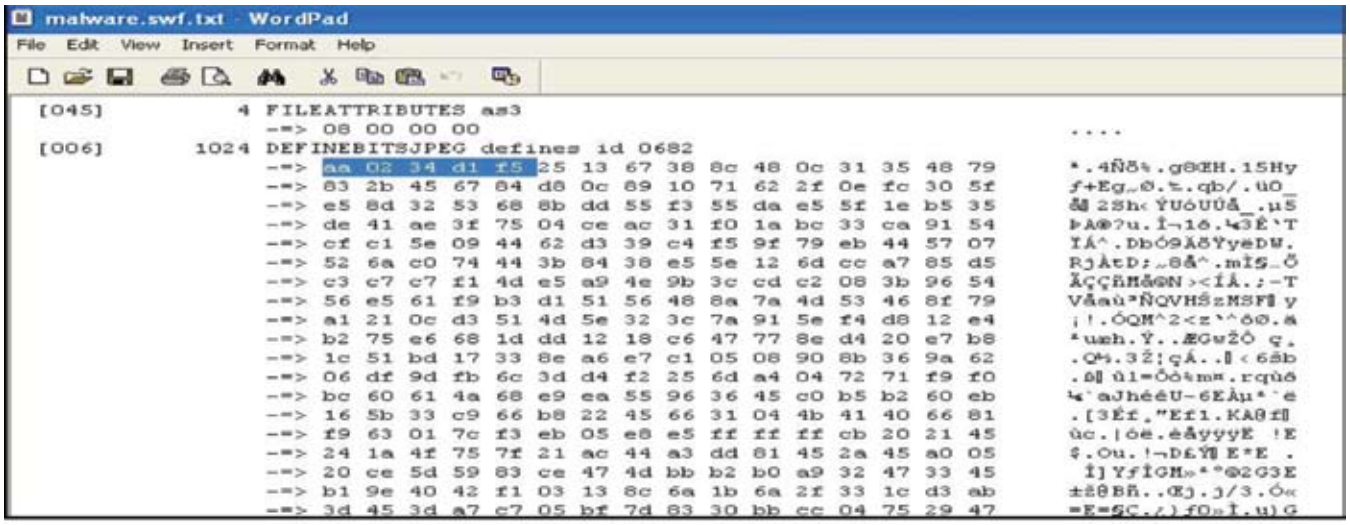


Figure 4: Starting Opcode of the Obfuscated Shellcode

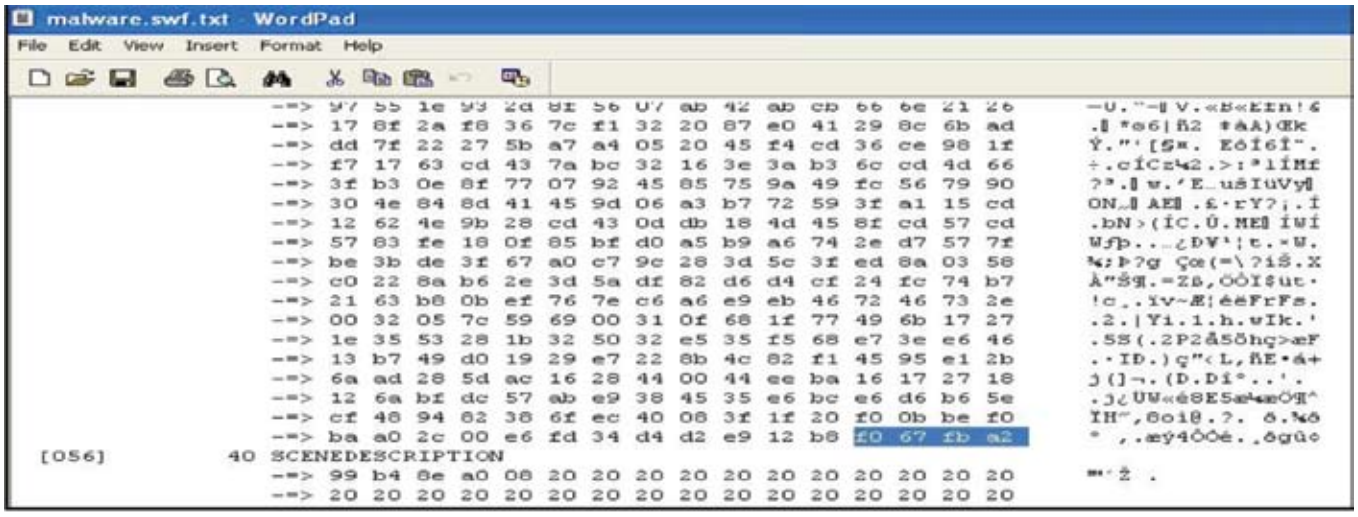


Figure 5: End Opcode of the Obfuscated Shellcode

Obfuscated shellcode was copied starting from opcode **AA02 34D1** (Highlighted in Figure 4) until opcode **F067 FBA2** (Highlighted in Figure 5) by using Hex Workshop and saved it as different filename; in this case, we named it as **shellcode.bin.**

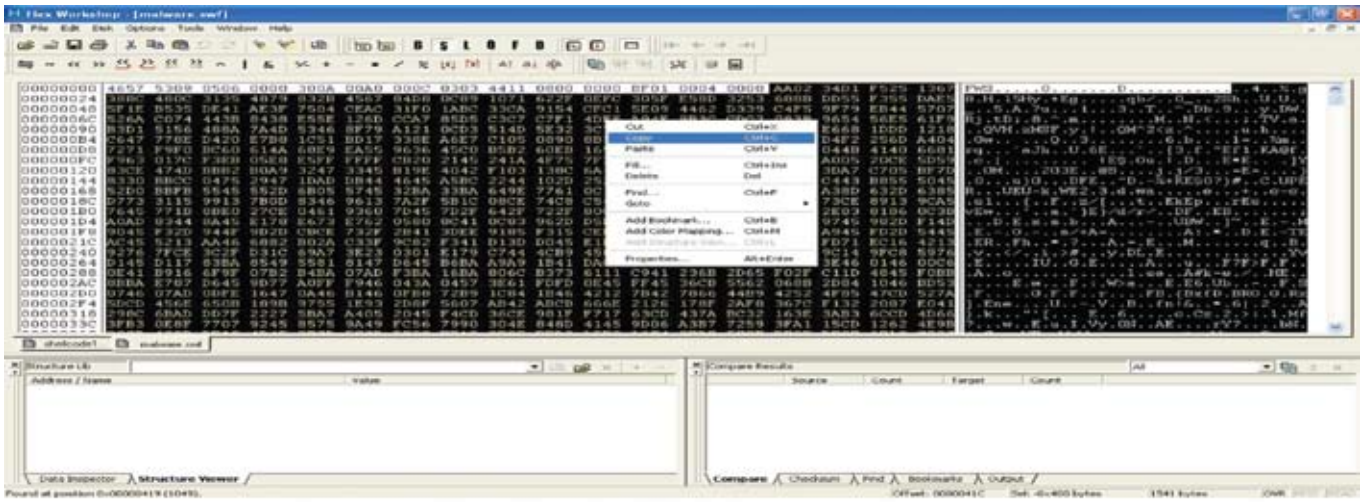


Figure 6: Copy the Obfuscated Shellcode from Malicious SWF File

- **Shellcode Analysis**

The following step is looking at the decryption routine of obfuscated shellcode. First, load the **shellcode.bin** with IDA Pro and 32-bit disassemble mode is chosen. The full code analysis can be done by choosing **force conversion of the selected byte to instruction** option.

- Select and highlight all the codes
- Press C and select option Force analysis

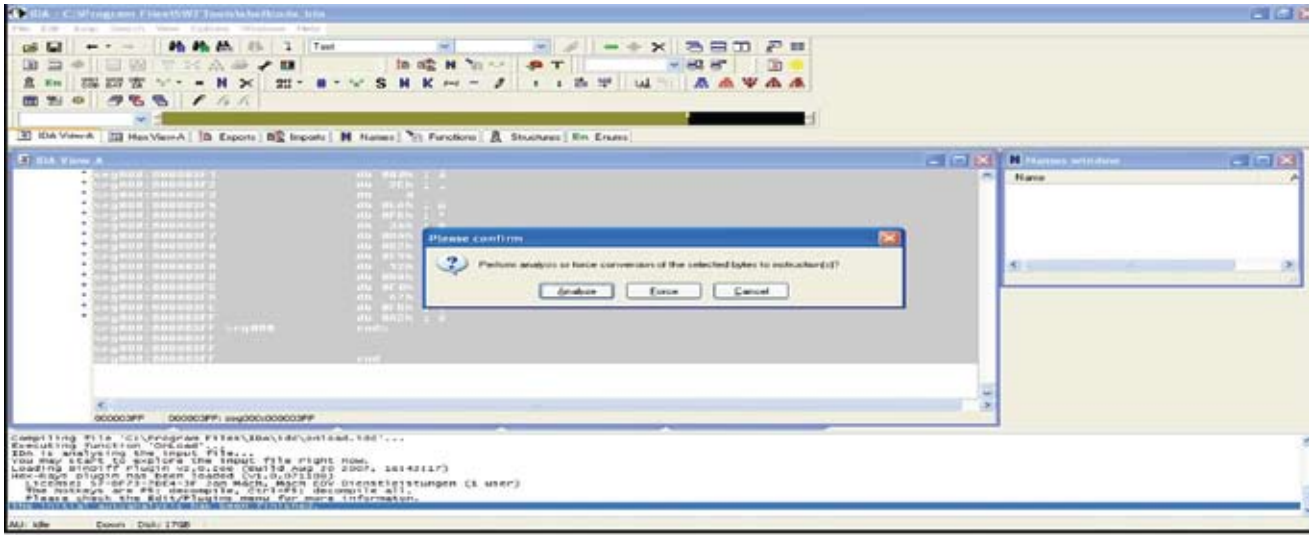


Figure 7: Conversion of the Selected Byte to Instruction

Figure 8 shows the result of obfuscated shellcode and its decryption routine.

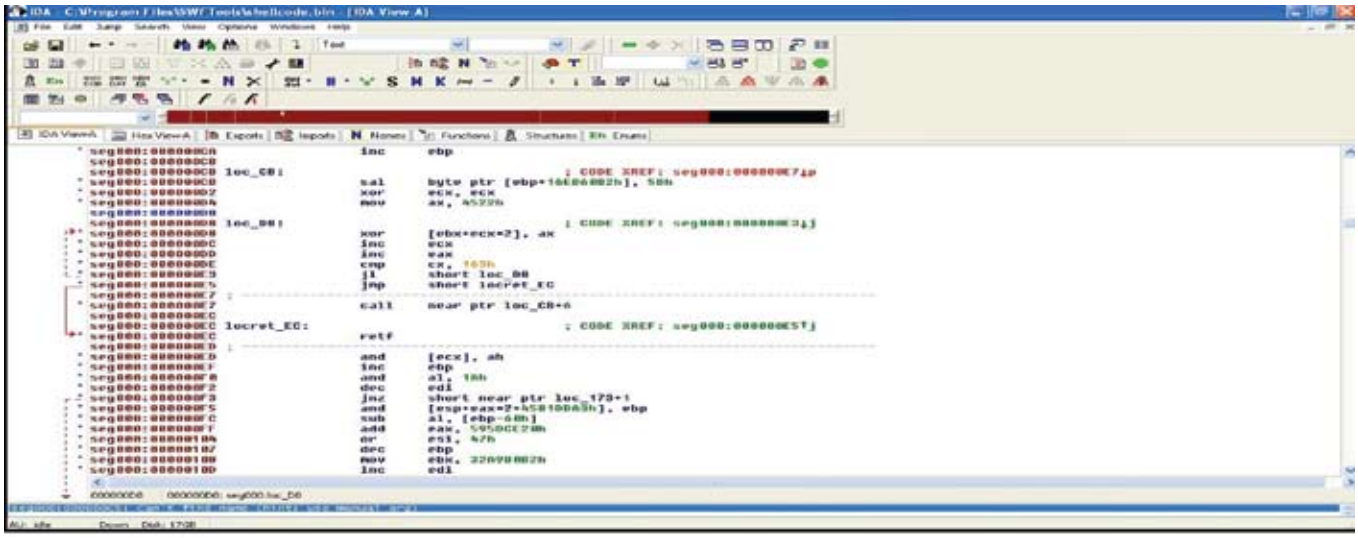


Figure 8: Decryption Routine of the Shellcode

"The obfuscated shellcode will call the decryption routine before executing the payload. In this exercise, the starting of the decryption code located at offset **0000 00D8**. The details of the coding can refer to the comments (Refer Figure 9).

```
seg000:000000D2    xor     ecx, ecx                ; Initialize ecx to zero. ecx as the
counter
seg000:000000D4    mov     ax, 4522h               ; Load 4522h as a key into ax
seg000:000000D8
seg000:000000D8 loc_D8:
seg000:000000D8    xor     [ebx+ecx*2], ax         ; Start decrypt shellcode using the
value in ax
seg000:000000DC    inc     ecx                     ; Increment the counter by one
seg000:000000DD    inc     eax                     ; increment the key by one
seg000:000000DE    cmp     cx, 163h                ; Check if the counter is equal to 163h
seg000:000000E3    jl      short  loc_D8           ;Jump to decryption routine again if less
than 163h
seg000:000000E5    jmp     short  locret_EC        ;Decryption process done
seg000:000000E7
seg000:000000E7    call    near  ptr  loc_CB+6
```

Figure 9: Hex View of **shellcode.bin** File

Since the opcode for **shellcode.bin** part was found, the same steps can be applied to the original **malware.swf** file. As shown in Figure 10, the **malware.swf** file was loaded with Hex Workshop and the offset for opcode **6631 044B** is **0000 00F4**. Again this is the offset for the beginning decryption routine which was used to decrypt the rest of the obfuscated shellcode.

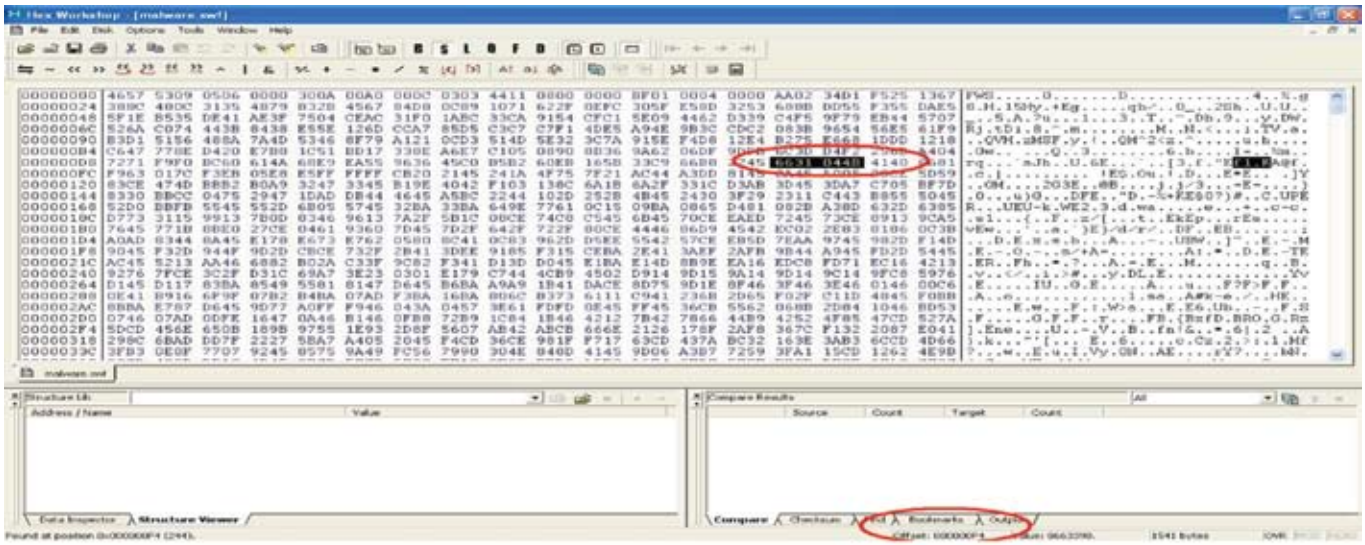


Figure 10: Starting Offset of the Decryption Routine

INT3 instruction will be set to call the interrupted function at debugger by modifying the opcode of **6631 044B** to **CC31 044B** then save it as **malware1.swf**. It is very important to do the setting as below in OllyDbg before starting with the dynamic analysis:

1. Enable the option **Make OllyDbg just-in-time debugger**. Start the OllyDbg → **Options** → **Just-in-time debugging** → **Make OllyDbg just-in-time debugger**

malware1.swf file will be loaded with Internet Explorer. The Internet Explorer will crash and ask for debug option. Debug option will be select and wait for **malware1.swf** file load with OllyDbg.

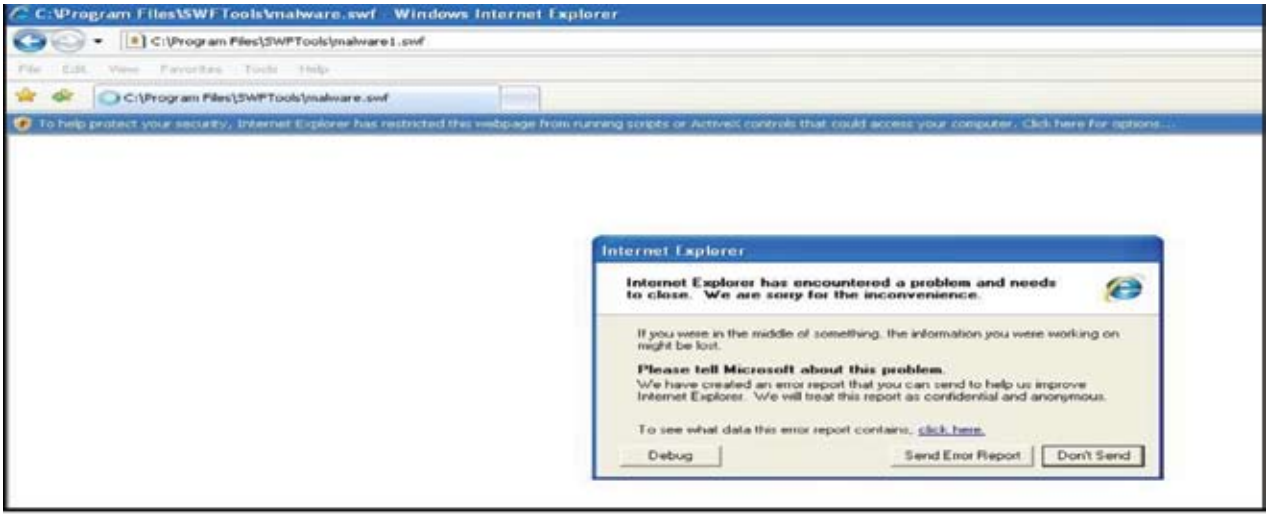


Figure 11: Malicious SWF File Crash the Internet Explorer

The loading process of **malware1.swf** with OllyDbg will stop at offset **04ED 669C**. Then, modify the opcode at offset **04ED 669C** to the original value.

1. The current landed offset is **04ED 669C**.
2. **Right Click → Binary → Edit**
3. Edit the opcode CC to original opcode **66**

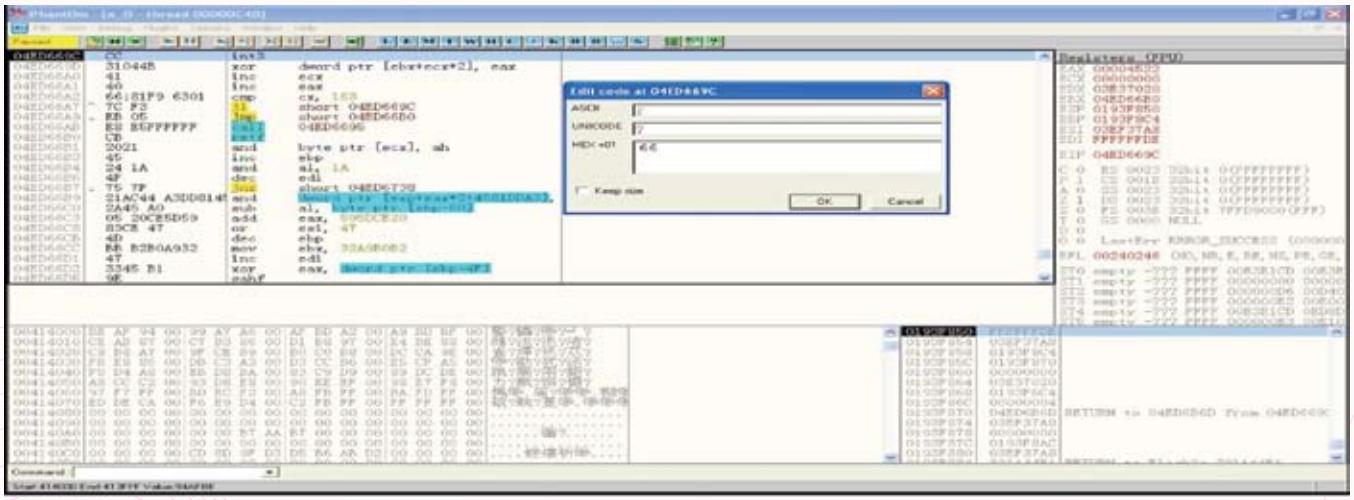


Figure 12: Original Opcode

The following instruction is to decrypt the shellcode and dump the content of the payload after the decryption routine.

1. After modifying the opcode, keep hitting the F7 until the OllyDbg landed at offset **04ED 669C** where the decryption routine starts.
2. Set the breakpoint at offset **04D2 6B21** by pressing F2. Let the OllyDbg continue running by pressing F9.
3. Now OllyDbg landed at address **04D2 6B21**. Start by dumping the content of payload with **right click →Follow in Dump → Selection**

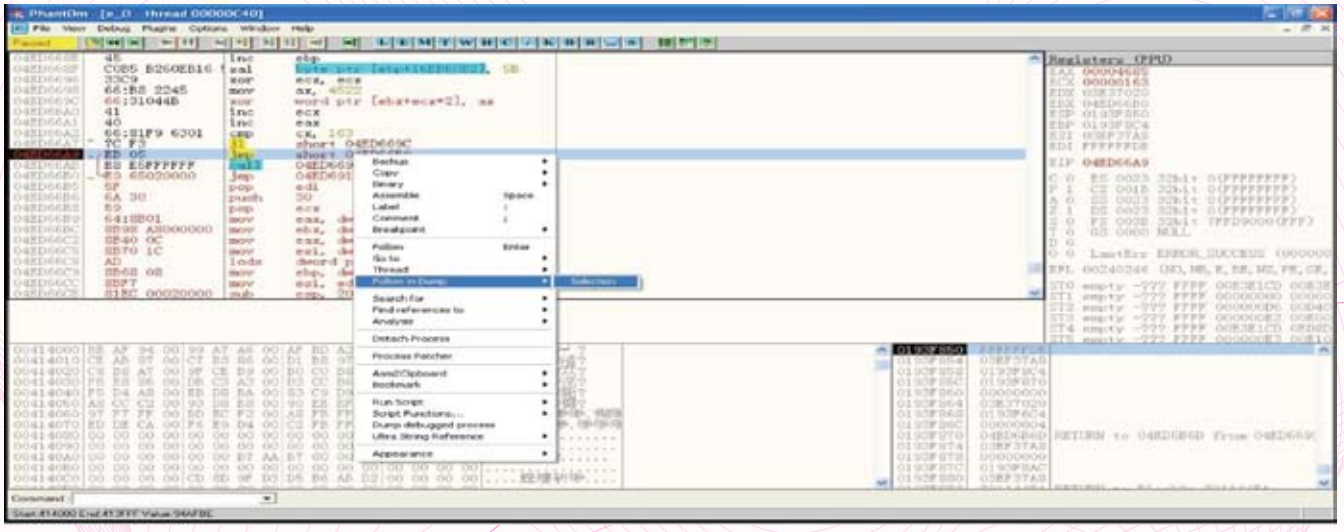


Figure 13: Dump the Content of the Payload

The circled part shows in Figure 14 indicate that the malicious SWF file that connected to http://www.xxxx.cn web site and downloaded test.exe into victim's computers.

Figure 14: The Content of the Payload after Decryption

Other Utilities

In light of growing security problem in Adobe Flash Player, there are a few new tools available to assist the security researcher in reverse engineering and analysis malicious SWF file.

1. WEPAWET [12]
2. Version test for Adobe Flash Player [13]
3. SWFIntruder [14]
4. Jswiff [15]
5. Flare [16]
6. Flashblock (For Firefox users) [17]

Conclusion

Analysing malicious SWF files is a tedious and new process. Numerous tools for decompiling, disassembling and analysis are available, but most of the static tools for analysing SWF were not developed to be used for security testing and analysis. In general, there are no known official guidelines for malicious SWF file security analysis. There are also some important steps that should be taken to limit the damage from the attack of malicious SWF files. The users are recommended to upgrade the Adobe flash player to the latest version or install Flashblock [17] to block all flash content from loading without permission.

References

1. SecurityFocus. Retired: Adobe Flash Player SWF File Remote Code Execution. Website: *http://www.securityfocus.com/bid/29386*

2. Craig Schmugar. Flash Player Exploit Update. Website: *http://www.avertlabs.com/research/blog/index.php/2008/05/27/flash-player-exploit-update/*

3. Adrien de Beaupre. Adobe Flash Player Vulnerabilities. Website: *http://isc.sans.org/diary.html?storyid=4465*

4. Common Vulnerabilities and Exposures. CVE-2007-0071. Website: *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0071*

5. SWF Manipulation and Generation Utilities. Website: *http://www.swftools.org*

6. Wikipedia. SQL Injection. Website: *http://en.wikipedia.org/wiki/SQL_injection*

7. Niyaz PK. Hidden IFrame Injection Attacks. Website: *http://www.diovo.com/2009/03/hidden-iframe-injection-attacks*

8. Fukami and Ben Fuhrmannek. SWF and the Malware Tragedy: Detecting Malicious Adobe Flash Files. OWASP: Application Security Conference, 19-22 May 2008.

9. Adobe Systems Incorporated. SWF File Format Specification version 9. Published June 2007, April 2008. Website: *http://www.adobe.com/devnet/swf/pdf/swf_file_format_spec_v9.pdf*

10. Mark Dowd. Application-Specific Attacks: Leveraging the ActionScript Virtual Machine. April 2008.

11. Web Engine to Protect from and Analyze Widespread and Emerging Threats (WEPAWET). Website: *http://wepawet.iseclab.org*

12. Version test for Adobe Flash Player. Website: *http://www.adobe.com/go/tn_15507*

13. SWFIntruder. Website: *https://www.owasp.org/index.php/Category:SWFIntruder*

14. Jswiff. Website: *http://www.jswiff.com*

15. Flare. Website: *http://www.nowrap.de/flare.html*

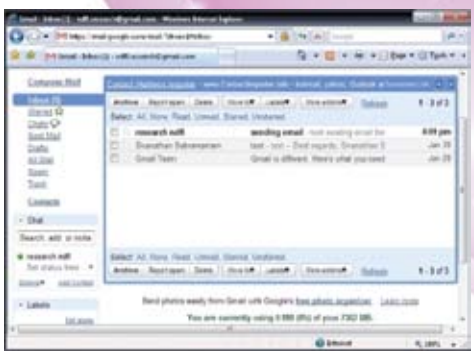
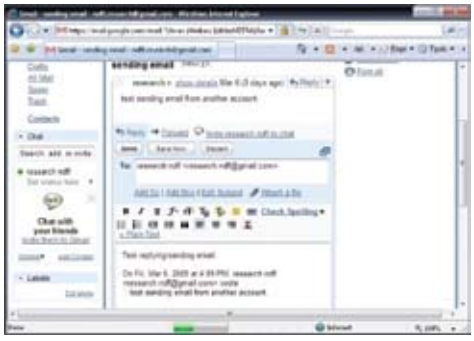
16. Flashblock. Website: *http://addons.mozilla.org/en-US/firefox/addon/433*

Gmail Forensic (Memory Analysis) – Part 2

On the previous article, we have elaborated on the first part of Gmail Forensic. In this second part of the article, we shall concentrate on the findings and analysis of the memory dump to look for remnants of Gmail content.

Findings

The findings of eight (8) tests performed can be summarized as below:

Test	Screenshot of each test	Finding of IE process dump + PDGmail.py command	Finding of entire memory dump + PDGmail.py command
1. Login into Gmail account		Emails (message header and message body) in the inbox found in the memory	Emails (message header and message body) in the inbox found in the memory
2. Receive new email but it was not opened or read		The old and new email (message header and message body) found in the memory	The old and new email (message header and message body) found in the memory
3. Read new email received		The old and new email (message header and message body) found in the memory	The old and new email (message header and message body) found in the memory
4. Compose new mail but not send		No remnants of the newly composed email	No remnants of the newly composed email

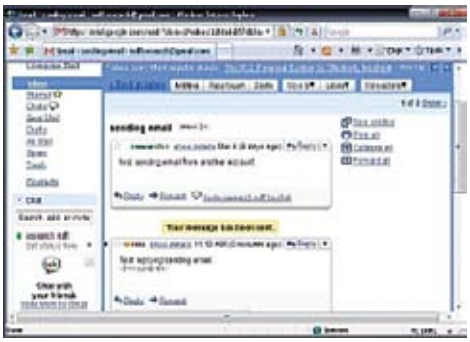
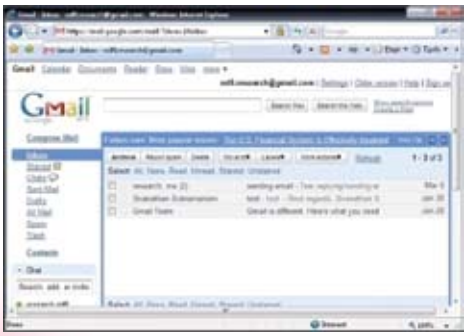
5. Send new mail	 	No remnants of the newly sent email	No remnants of the newly sent email
6. Logoff Gmail but IE still running		Remnants (message header) of the old, new and newly sent email found in the memory	Remnants (message header) of the old, new and newly sent email found in the memory
7. Exit IE	-	-	Remnants (message body) of the old, new and newly sent email found in the memory
8. Restart IE		No remnants of Gmail account found in the memory	No remnants of Gmail account found in the memory

Table 1: Summary of findings

Analysis

In Test 1, partial output from PDGmail.py command can be depicted in Figure 8. *(Note: Only partial output is put in this article).*

Figure 1: Partial output of PDGmail.py command on data collected in Test 1

In Figure 1, highlighted in box 1, we found information the Gmail account which is *ndfl.research@gmail.com*. We also found information about the timestamp of the last access and the most recent access to the Gmail from the memory. The interesting part is that the timestamp is based on the Gmail server time but has been converted to the local GMT time, in this example Gmail account was recently accessed on March 06, 2009 at 15:40:18 GMT+8 (Malaysia local time).

Further down, there were repetitious message headers found. Looking at two unique message headers highlighted in box 2, we concluded that there were only two emails in the inbox (based on the unique message id in the "ms" tag; *"11f262b9bc278ab2" and "11f1bc71eb3a82bb"*). The sender of the emails was *"Sivanathan Subramaniam <siva@cybersecurity.my>"* and also *"Gmail Team <mail-noreply@google.com>"*. In box 2, we can also see snippets of both emails; the first email contains *"test --Best regards, Sivanathan Subramaniam (MSc, GCFA) Senior Digital Foren..."* and the second email contains *"Messages that are easy to find, an inbox that organizes itself, great spam-fi..."*.

Finally, in box 3, the message body of the email can be found. As depicted, email content received from *"Sivanathan Subramaniam <siva@cybersecurity.my>"* is readable from the memory itself. Further analyzing the memory, we also found the email content received from *"Gmail Team <mail-noreply@google.com>"*.

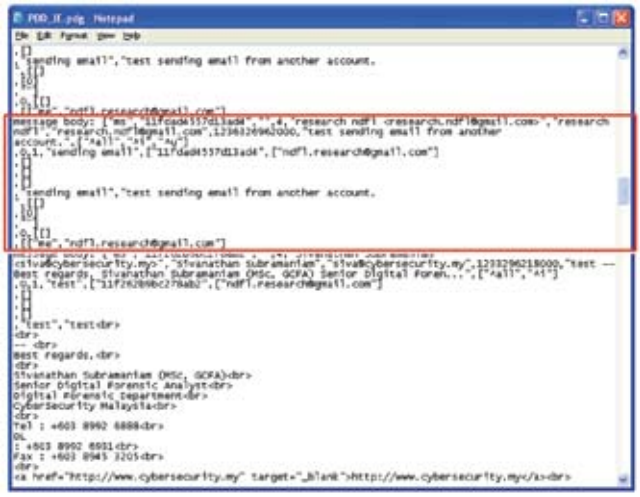


Figure 2: Partial output of PDGmail.py command on data collected in Test 2

In Test 2, we found all findings as in Test 1, with additional data on the new email received. In Figure 2, highlighted in the red box, the message body of email received from *"research ndfl < research.ndfl@gmail.com>"* was found in the memory. We also found message body of all previous mails; from *"Sivanathan Subramaniam <siva@cybersecurity.my>"* and *"Gmail Team <mail-noreply@google.com>"*. Similar findings were found in Test 3 as well. Meanwhile, in Test 4 and Test 5, no remnants of the newly composed email were found in the memory. From Test 1 until Test 3, we can summarize that by login into the Gmail account, at least, information about emails contained in the Inbox can be carved out from the memory without going through the hassle to click and read each individual email.

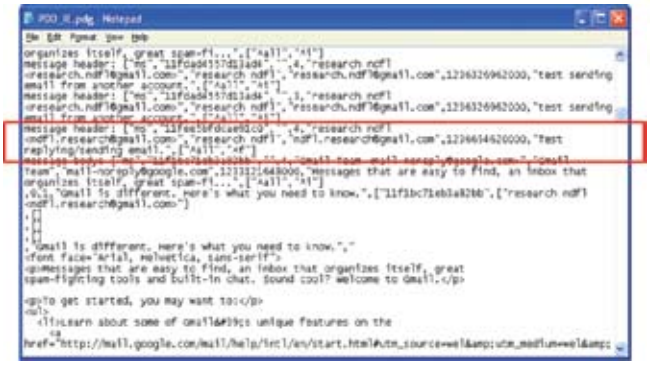


Figure 3: Partial output of PDGmail.py command on data collected in Test 6

Interestingly, in Test 6, we found message header of the newly sent email in the memory. In Figure 3, highlighted in the red box is the message header of the new email that was composed and sent from the Gmail account. However, the message body of the email was not found either in the IE process dump or the full memory dump.

The message body of the new composed and sent email was found in Test 7 (full memory dump). As depicted in Figure 4, only the message body of the new sent email was found. All message header and message body of other previous emails were not found in the memory. Meanwhile,

in Test 8, no remnants of Gmail were found in the memory. From Test 6 and Test 7, we can summarize that there is a possibility to discover remnants of Gmail account in the memory even after a user logoff his/her account or even exit the internet browser.

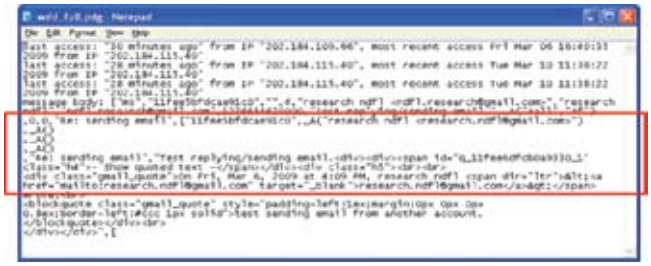


Figure 4: Output of PDGmail.py command on data collected in Test 7

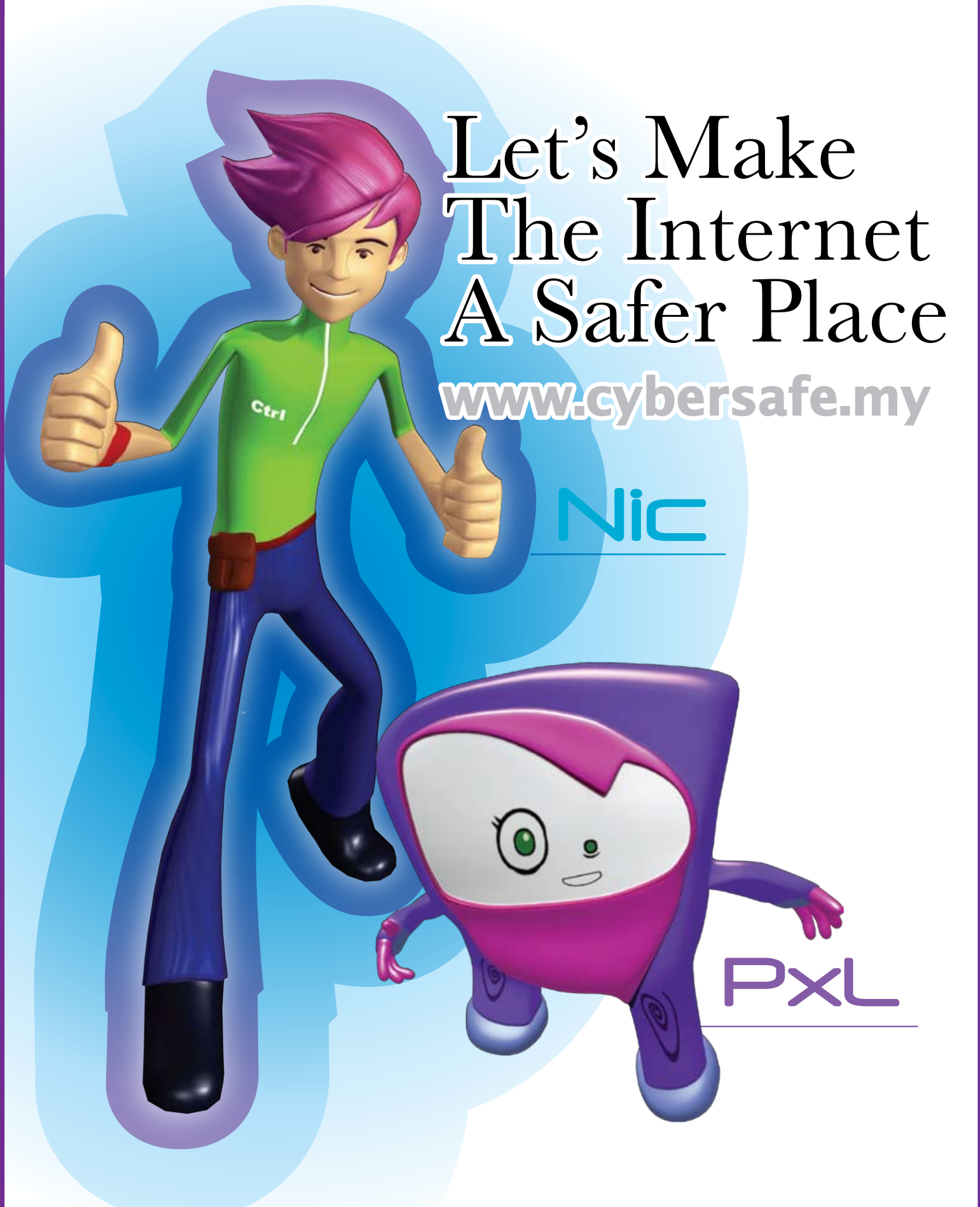
Conclusion

What we found from the analysis of the memory is interesting and very useful for investigators. It is indeed amazing what computer memory can contain. From a computer forensic view, it is very important to be able to secure the memory at the crime scene prior to seize any computers as there is ample information in the memory that definitely can assist the investigators in their work. Based on the findings of each test conducted, it is indeed very critical especially for First Responders (officers responsible in processing a crime scene) to realize the importance of acquiring the memory of a running computer as this valuable information will be lost if the computer is shut down.

References

1. Forensic Gmail Artifact Analysis, *https://blogs.sans.org/computer-forensics/2008/09/19/forensic-gmail-artifact-analysis/*

2. pdgmail: new tool for gmail memory forensics, *https://blogs.sans.org/computer-forensics/2008/10/20/pdgmail-new-tool-for-gmail-memory-forensics/*



CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Bussiness Park,
No 3, Jaalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan.
Tel: 03-89460999 Fax: 03-89460888

www.cybersecurity.my

CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI