CyberSecurity MALAYSIA

e-Security

MOSTI

Volume 17 - (Q4/2008)

"The mantra of any good security engineer is: 'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together" *Bruce Schneier*

Contributors

MyCERT 4th Quarter 2008 Summary Report
MyCERT
CyberSecurity Malaysia

DFLive 2008: Your Swiss Army Knife in Digital Crime Scene
By Mohd Izuan Effenddy Yusof &
Mohd Zabri Adil Talib
Digital Forensic Dept
CyberSecurity Malaysia
fendy@cybersecurity.my
zabri@cybersecurity.my

Defending Yourself at Wireless Hotspots
By Mohamad Nizam Kassim
Security Assurance Dept
CyberSecurity Malaysia
mnizam.kassim@cybersecurity.my

Data Protection: Software Encryption vs Hardware Encryption
By Ahmad Dahari Bin Jarno
Security Assurance Dept
CyberSecurity Malaysia
dahari@cybersecurity.my

Taking Information Security Governance to the Next Level
By R.Azrina R.Othman
Chief Technology Officer
CyberSecurity Malaysia
azrina@cybersecurity.my

9 Security Predictions for 2009
By Derek Manky
Security Research Engineer
Fortinet
georginatan@fortinet.com

Internet Safety
By Tan Tze Meng
Multimedia Development Corporation (MDeC)
tmtan@mdec.com.my

Botnet 101 for the rest of us mortals
By Syahrir Mat Ali
Cyber Media Research Dept
CyberSecurity Malaysia
syahrir@cybersecurity.my

Information Security Best Practices Series: How to avoid becoming a victim of Cyberstalking?
By Raj Kumar
Security Management and Best Practices
CyberSecurity Malaysia
raj@cybersecurity.my

Risk Management within ISMS
By Nor Aza Ramli
Security Management &
Best Practices Dept
CyberSecurity Malaysia
aza@cybersecurity.my

The Reality of Cyber-Threats Today
By Zahri Yunos
Chief Operating Officer
CyberSecurity Malaysia
zahri@cybersecurity.my

ISSN 1985-1995

9 771985 199003

ISMS
SIRIM
UKAS
074
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4806

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

From the Editor's Desk

maslina@cybersecurity.my

I hope it is not too late for me to wish all readers a very good Christmas and Happy New Year! This edition sees great contributions; a good mix of technical and management articles on information security. Thanks to everyone who contributed to this bulletin.

For year 2008, CyberSecurity Malaysia has been aggressively promoting security awareness throughout the country to different target audience. Year 2008 also observed the country's initiative in the Information Security standards development at the international platform where CyberSecurity Malaysia through Standard Malaysia, has proposed a new ISO standard in the area of Digital Forensic.

Anticipating more security breaches in 2009 due to economic turmoil, organizations are expected not to take any risks on any possibilities for security within their organisation to be compromised; subsequently affecting their critical information assets and stakeholders' interest. Thus, it is absolutely vital for organisations to have dedicated staff with the necessary expertise and technical know-how in various information security domains.

For that, CyberSecurity Malaysia has produced a training calendar comprises competency building courses for information security professionals. Please see our Training Calendar for 2009 at the last page of this bulletin.

Lastly, to keep abreast with the latest threats, security events, and advisories, we do encourage readers who have not yet subscribing to our mailing list, please do so. Again, thanks to all contributors for their time and efforts. We do hope you will find this issue fruitful and please share it with your friends and colleagues. Happy New Year!

Best Regards

Maslina

Maslina binti Daud
Editor

A Message from the Head of CyberSecurity Malaysia

Greetings to all readers! Another year has come to an end. It has been another exciting 12 months where events and activities related to enhancing security measures were held by CyberSecurity Malaysia.

Many new threats have been discovered in 2008. New malware variants have emerged consisting of threats that mutate as they spread and infect computers. Spam activities and phishing attacks continue to be active despite measures being put in place by many organisations. While antispam filters have become more sophisticated, spam threats have dissipated indicating that spammers are not giving up! Phishing attackers have been grabbing opportunities from big events to make their 'baits' more convincing and by employing advanced techniques. We had seen many trusted websites become a target conduit for attackers to carry out their malicious activities. With the current global economic climate, data loss prevention is becoming more crucial in protecting sensitive information of organisations where mergers and acquisitions are common.

We offer various information security training and awareness programmes for end-users and organisations. We have organised an inaugural Professional Critical Infrastrucure Protection (PCIP) programme with the Critical Infrastructure Institute (CII), USA for selected candidates from various Critical National Information Infrastructure (CNII) sector organisations in Malaysia. This programme being first of its kind conducted in the country, specifically addresses the security needs and issues faced by critical sectors. Services offered by these sectors are vital as any disruption to its services will create a huge economic and societal impact.

For the upcoming year, it is anticipated that there will be great challenges ahead in the information security world. The global economic crisis can create opportunity for new attacks like new forms of phishing attacks, financial scam for mortgage, unemployment related scams. We may experience new and emerging threats on websites as well as explosion of new malware variants. Information security professionals will be expected to play bigger roles in meeting the demand for a more secure cyberworld.

I would like to thank our contributors who have given their support to make this bulletin a success and new contributors are always welcomed!

Happy New Year!

Thank you.

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

Table of Contents

READER ENQUIRY
Security Management and Best Practices
CyberSecurity Malaysia
Ministry of Science, Technology and Innovation (MOSTI)
Email: smbp@cybersecurity.my

PUBLISHED BY
CyberSecurity Malaysia (726630-U)
Level 7, Sapura@Mines
7, 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 Q4 2008

MySpace Suicide Case Verdict: Three Misdemeanor Convictions

(November 26 & 28, 2008)

Lori Drew, the Missouri woman who perpetrated an Internet hoax that prompted a 13-year old neighbor to kill herself, was convicted of three misdemeanor offenses of accessing computers without authorization; a federal jury acquitted Drew of three felony counts of accessing computers without authorization to inflict emotional harm.

http://www.securityfocus.com/brief/863

Group Raises Privacy Concerns About RFID Chips in Identification Docs at Borders

(December 1, 2008)

The Association of Corporate Travel Executives (ACTE) wants the US to stop using a system that reads RFID tags in government issued identification documents at border crossings, pending a review of the security issues the system poses.

http://www.theregister.co.uk/2008/12/01/rfid_scanning_under_fire/

Koobface Virus Hits Facebook

(December 4, 2008)

The Koobface virus is spreading through the messaging system of the social networking site Facebook. The malware attempts to harvest sensitive financial information, such as credit card numbers.

http://www.usatoday.com/tech/news/computersecurity/2008-12-04-facebook-virus_N.htm?csp=34

Just Two Percent of PCs are Fully Patched

(December 3 & 4, 2008)

According to statistics gathered by Secunia, 98 percent of PCs are running at least one unpatched program. The results were extrapolated from a sample of 20,000 PCs scanned by the company's Personal Software Inspector 1.0 over the past week.

http://www.scmagazineuk.com/Report-Nearly-all-computer-users-running-insecure-programs/article/121946/

Trojan and Keystroke Logger Dropzone Study

(November 18, 2008)

A research team assembled by Thorsten Holz from the University of Mannheim (Germany) examined banking Trojans, keystroke loggers and dropzones for both types of malware. Their study found more than 33 GB of log files in the dropzones of 70 separate pieces of malware.

http://www.heise-online.co.uk/security/Keyloggers-under-the-microscope-news/112288

Phone Hacker Sticks Computer Company with CA $52,000 Bill

(December 19, 2008)

Manitoba (Canada) Telecom Services is insisting that a Winnipeg-based company is responsible for the cost of phone calls a hacker made to Bulgaria through its phone system. Someone broke into the HUB Computer Solutions system in late November and over a period of two-and-a-half weeks made calls totaling CA $52,360 (US $43,023)

http://www.scmagazineuk.com/IT-company-hit-with-52000-bill-after-hacker-used-system/article/123156/

Virtual casanovas cashing in on Malaysian women

(December 22, 2008)

They choose their victims via Internet social networking sites and pretend to be cyber casanovas who start showering their victims with virtual gifts such as flowers, jewellery, plants, pets and even cars.

http://thestar.com.my/news/story.asp?file=/2008/12/22/nation/2866819&sec=nation

RBS WorldPay Data Breach Affects More than 1 Million Customers

(December 23, 24 & 29, 2008)

Attackers broke into the computer system at RBS WorldPay, a payment processing services provider, compromising personally identifiable information of more than one million customers. The compromised data include financial account information and Social Security numbers (SSNs).

http://www.theregister.co.uk/2008/12/29/rbs_worldpay_breach/

For latest news, please visit **http://www.cybersecurity.my**

MS-145.102008: MyCERT Quarterly Summary (Q4) 2008
Original Issue Date: 07th January 2009

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during the quarter. This report highlights statistic of attacks or incidents reported to MyCERT, as well as other noteworthy incidents and new vulnerabilities information.

MyCERT believes these numbers are only the tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order for us to assist those who are affected and escalate the matter to our partners.

Finally, this summary also directs to resources in dealing with problems related to security incidents.

Incident Reports

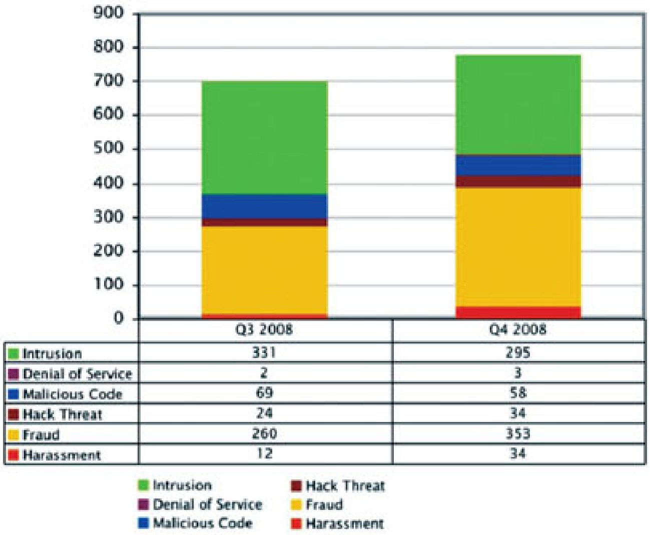
In the fourth quarter of 2008 (Q4), a total of 33036 incidents, inclusive of spam incidents, were reported to MyCERT representing a 52.51% increase of incidents compared to Q3 in 2008 . The majority of the incidents reported this quarter is contributed by spam reports. There was a tremendous increase in fraud incidents which mainly involving phishing, cheatings, and Nigerian scams. No critical outbreaks in terms of malware or exploitation that had raised red alert or crisis in our constituency were reported this quarter. Most categories of incidents reported to MyCERT had increased. However, malicious code and intrusion incidents had decreased in this quarter.

Attached is the Table of Figure showing the comparisons between number of reports received in Q3 2008 and Q4 2008.

	Q3 2008	Q4 2008	%
Harassment	12	34	183.3
Fraud	260	353	35.77
Hack Threat	24	34	41.67
Malicious Code	69	58	-15.94
Denial of Service	2	3	50
Intrusion	331	295	-10.88
Spam	20963	32261	53.89
Total	**21661**	**33036**	**52.51**

Table of Figure for Q3 2008 and Q4 2008

The following is the graph showing number of incidents handled according to the different categories in Q3 2008 and Q4 2008:

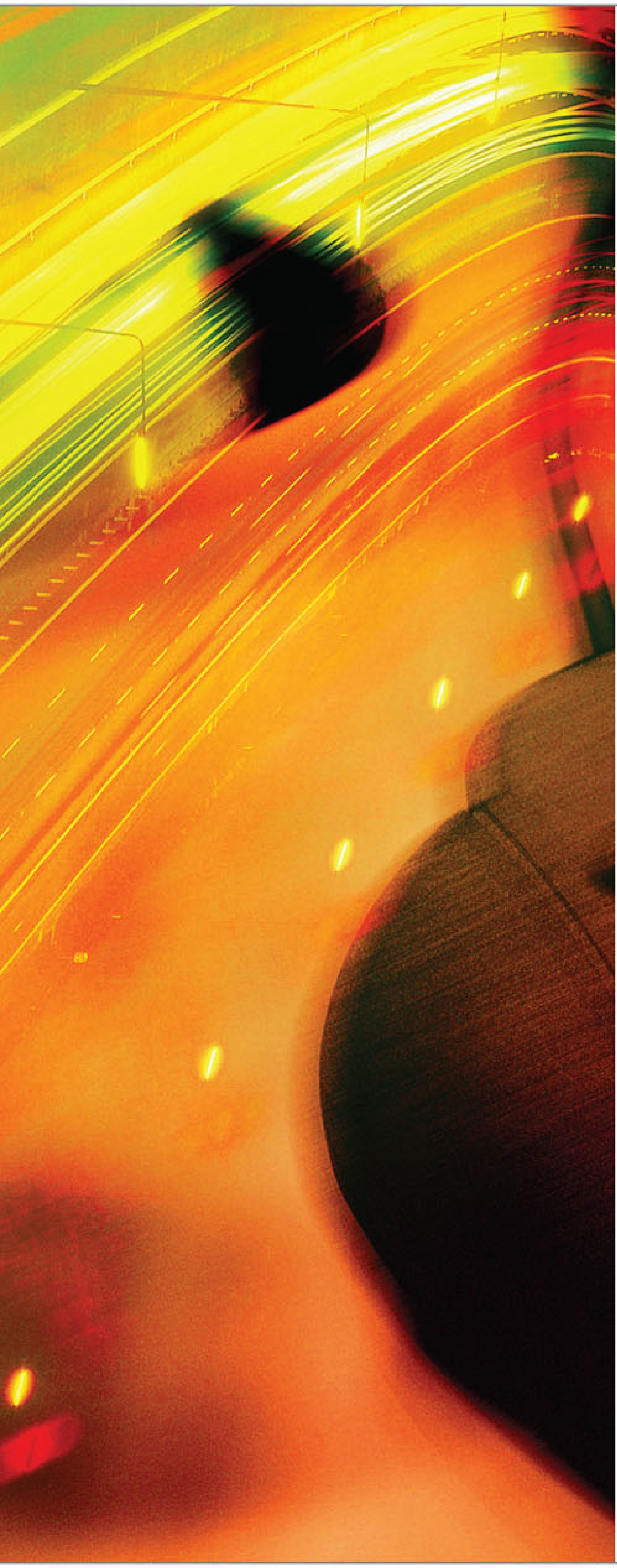


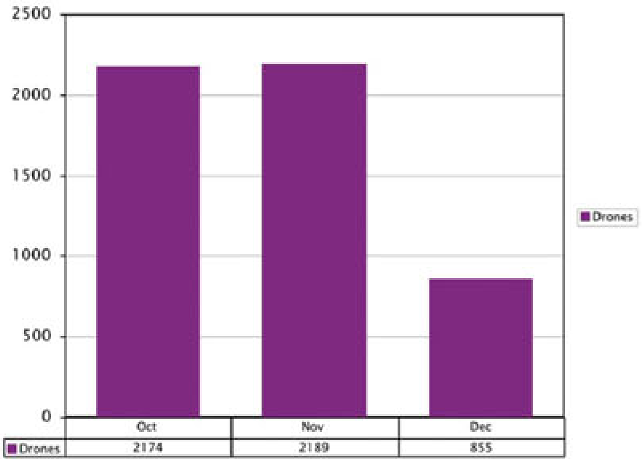
	Q3 2008	Q4 2008
🟩 Intrusion	331	295
🟪 Denial of Service	2	3
🟦 Malicious Code	69	58
🟥 Hack Threat	24	34
🟨 Fraud	260	353
🟥 Harassment	12	34

Comparison of incident statistics between Q3 2008 and Q4 2008

Malicious Codes

A total of 58 incidents related to malware were reported to MyCERT. In this quarter, we received several reports from foreign Computer Emergency Response Teams (CERTs) and security organizations regarding bots infected machines (drones), command & control server of botnets and malicious files hosted on computers in Malaysia. Some of these reports contained IP addresses, most of which are on home users network, which had been reported to us previously. In all of the instances, MyCERT had notified and assisted the respective ISPs on bot removal and mitigation strategies. These bots or zombies are normally used to carry out malicious activities such as spamming, executing denial of service attacks, hosting phishing sites and spreading malware.





	Oct	Nov	Dec
■ Drones	2174	2189	855

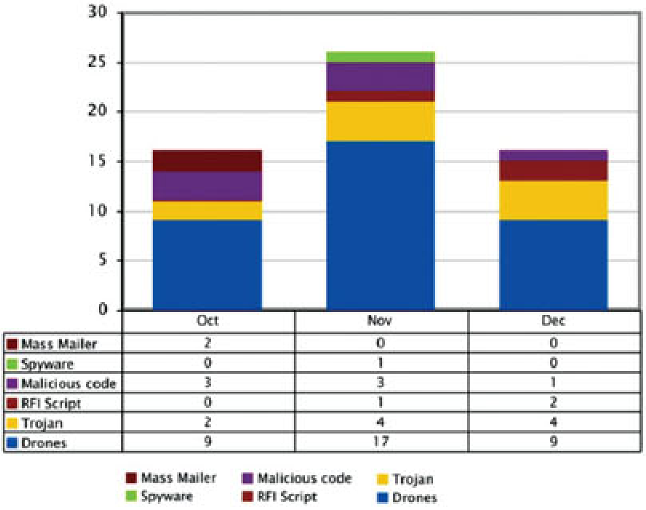
Statistics on total Malaysian IPs running Drones for Q4 2008

In this quarter, MyCERT received reports of 5218 IP addresses that were believed to be infected with malicious files and being used as drones of one or more botnets. The graph on the following page shows the number of IP addresses running drones belonging to Malaysian constituency in Q4, 2008.

MyCERT received 6 reports from a foreign CERT regarding some details found on a server which was used by a Trojan to log keystrokes. The keylogger Trojan, named the Nethell Trojan, had successfully captured keystrokes of usernames/passwords belonging to various internet accounts in our constituency, which includes accounts belonging to internet banking, web mails, entertainment sites, e-commerce and other online services. MyCERT had notified the respective parties for immediate rectifications on the compromised passwords.

In this quarter we also received several reports regarding machines within our constituency that hosting RFI scripts. We had advised the respective computer's Administrators to clean up and rectify the affected machines.

The following graph shows breakdown of malware incidents received in this quarter:



	Oct	Nov	Dec
■ Mass Mailer	2	0	0
■ Spyware	0	1	0
■ Malicious code	3	3	1
■ RFI Script	0	1	2
■ Trojan	2	4	4
■ Drones	9	17	9

Breakdown of types of malware incident in Q4 2008

Hack Threat

MyCERT received 34 reports for the category of hack threats in this quarter which represents 41.67% increase compared to previous quarter. Most of the hack threat reports were received from foreign security organizations where the sources of the attack are from Malaysian IP addresses. Some of the common attacks observed are similar to attacks reported in previous quarter which are SSH brute-force attacks, port scanning and other malicious or suspicious activities that had triggered alerts.

MyCERT's findings for this quarter, as was in previous quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21) and HTTP (TCP/ 80).

Denial of Service

In this quarter, MyCERT received 3 reports on denial of service which is slightly higher than in previous quarter. The denial of service attack consists of sending huge traffic, continuously to a system, causing the system to slowdown or choked. In distributed denial of service attacks, the source of the attacks mostly come from various spoofed multiple IP addresses and majority of denial of service attacks originate from 1 single IP address. The majority of denial of service attacks were successfully handled or stopped by blocking the source of the attacks at the customers' upstream router.

Intrusion

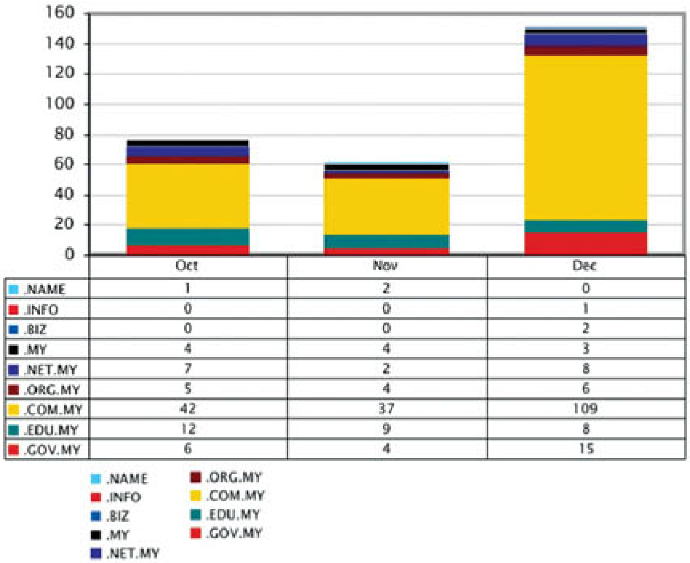
MyCERT had received 295 reports related to intrusion in this quarter, which represents a 10.88% decrease compared to previous quarter. The majority of the incidents in this category were web defacements (or re-defacements in some incidents) of .my websites hosted in Malaysia that belonged to various sectors and running on various platforms.

Based on our analysis, majority of these defacements were caused by web application vulnerabilities such as remote file inclusion, SQL injection and unpatched third party add-ons.

MyCERT was able to contact the respective Administrators of the websites and advised on recovery and mitigations. In the previous quarterly report, MyCERT had discussed possible workarounds to prevent these kinds of attacks and can be viewed at:

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/564/index.html

MyCERT had also produced a statistic on breakdown of defaced .MY sites by domains, as attached below:



	Oct	Nov	Dec
.NAME	1	2	0
.INFO	0	0	1
.BIZ	0	0	2
.MY	4	4	3
.NET.MY	7	2	8
.ORG.MY	5	4	6
.COM.MY	42	37	109
.EDU.MY	12	9	8
.GOV.MY	6	4	15

Breakdown of web defacements reported in Q4 2008

Harassment

MyCERT had handled 34 incidents under the category of harassment this quarter which represents a more than 100% increase. The nature of the harassment cases includes email threats to defamatory messages/ pictures/photos on internet forums and social networking websites. In this quarter, we observed a surge on harassments using stolen social networking IDs for malicious purposes such as using stolen IDs to post defamatory and threatening messages and pictures on websites against a particular individual, group and religion. In majority of cases, MyCERT managed to communicate with the respective social networking sites to get the defamatory and threatening messages and pictures to be removed. In some cases, the matter had been referred to the Law Enforcement Agencies.

Fraud

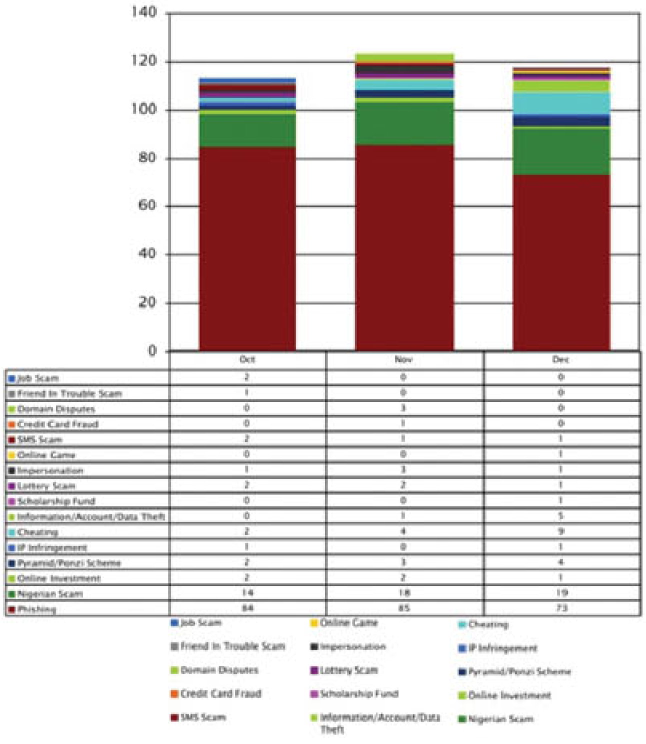
There is an increase in terms of the number of reports involving fraud reported to MyCERT this quarter with an increase to about 35.77%, which comprised of 353 reports compared to 260 reports in previous quarter. Majority of fraud incidents reported were phishing incidents involving local and foreign financial institutions or brands. In this quarter, we observed a surge on phishing reports, with 242 reports, which includes reports on phishing emails and phishing sites impersonating local/foreign financial institutions or brands. Upon reported to MyCERT, the phishing sites were put offline or removed to shutdown within 24 - 48 hours.

As was in previous quarter, we observed phishers actively using the fast-flux techniques for a more advanced and sophisticated phishing tactics. MyCERT had handled the phishing reports by communicating with respective parties and in most instances, the phishing sites were put offline or removed to shutdown within 24 - 48 hours.

Other types of fraud that worth to be highlighted in this quarter are Nigerian scams, cheating and stolen information/data/accounts. Nigerian scams had increased in this quarter with 51 reports mostly from home users. In some cases, users had fall victim to this scam which led to huge monetary loss. MyCERT advise users to be careful when dealing with people who request for cash or bank deposits for a particular transaction. They must not send any money to unknown parties without proper verification.

We also observed an increase on cheatings this quarter with 15 reports. Majority of the cheating cases involved users who paid for products they ordered online but had never received the products. Most of these cases were referred to the Law Enforcement Agencies as well as to the respective banks. MyCERT would like to advise users to be extra careful when they purchase items online to avoid being cheated by fraudsters. It is advisable to purchase items from authorized or licensed online traders who can guarantee the delivery of items to buyers otherwise they should deal offline.

Attached is the graph showing the breakdown of types of fraud incidents that we received in this quarter:



	Oct	Nov	Dec
Job Scam	2	0	0
Friend In Trouble Scam	1	0	0
Domain Disputes	0	3	0
Credit Card Fraud	0	1	0
SMS Scam	2	1	1
Online Game	0	0	1
Impersonation	1	3	1
Lottery Scam	2	2	1
Scholarship Fund	0	0	1
Information/Account/Data Theft	0	1	5
Cheating	2	4	9
IP Infringement	1	0	1
Pyramid/Ponzi Scheme	2	3	4
Online Investment	2	2	1
Nigerian Scam	14	18	19
Phishing	84	85	73

Breakdown on frauds reported in Q4 2008

Vulnerabilities Reported

In this quarter, MyCERT also received 19 reports from various reliable sources regarding web application vulnerabilities found on Malaysian websites. The vulnerabilities include SQL injection, directory listing and weak administrator's passwords. MyCERT had verified the reported vulnerabilities at the said websites and informed the respective owners to fix the vulnerabilities to prevent untoward incidents.

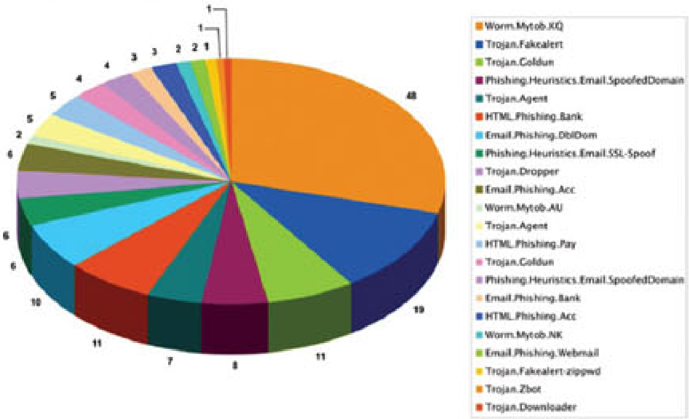
Steps that administrators can implement to fix the above vulnerabilities are available in the MyCERT Q2 Summary Report at:

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/596/index.html

Spam Watch

MyCERT had observed that spam related incidents had increased by 53.89% in this quarter compared to the previous quarter. A total of 32261 incidents were received compared to 20963 reports in previous quarter. Spam incidents remains as the incident with highest number of reports received compared to other incidents.

Based on our observation of the monthly spam statistics, we noticed spam emails were recorded higher with the outbreak of a certain security threat. The top categories of spam emails detected for this quarter are the phishing emails which recorded the highest followed by Trojan emails. Phishing emails mainly involved spoofed domains related to banks. Majority of Trojans are the Trojan.Agent, Trojan.Dropper and Trojan.Goldrun.



Spam payload detected by ClamAV in Q4 2008

Other categories of spam are related to scam emails such as the Nigerian scam, Lottery scam, get rich schemes. Promoting or selling of products/services still remains as one of the main contributors to spam.

There are no perfect techniques or tools to completely eradicate spam, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users email clients. Users are also advised not to respond nor purchase products promoted via spam as this serves only to further propagate spam activities. MyCERT encourages users to report spam so that proper action can be taken against the owner of the computer sending out the spam.

Alerts & Advisories

In this quarter, MyCERT had released 3 alerts related to critical vulnerabilities on Mozilla Firefox and Microsoft Internet Explorer. The alerts are available at:

MA-144.122008: MyCERT Special Alert - Mozilla Firefox Multiple Vulnerabilities (23/12/2008)
http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/621/index.html

MA-143.122008: MyCERT Special Alert - Microsoft Internet Explore 7 (IE7) 0-day Exploit (11/12/2008)
http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/617/index.html

MA-142.122008: MyCERT Special Alert - MS08-067 related malware (03/12/2008)
http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/616/index.html

MyCERT have also forwarded three advisories and alerts from various other sources to your constituency as below:

Microsoft Security Advisory (961509) (30/12/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/624/index.html

Microsoft Security Advisory: Vulnerability in SQL Server Could Allow Remote Code Execution (22/12/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/623/index.html

Apple Updates for Multiple Vulnerabilities (15/12/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/622/index.html

Microsoft Security Bulletin Summary for December 2008 (09/12/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/619/index.html

Sun Releases Updates for Java SE (08/12/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/618/index.html

MS08-068: Vulnerability in SMB Could Allow Remote Code Execution 11/11/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/613/index.html

MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow (11/11/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/614/index.html

Microsoft Security Bulletin Summary for November 2008 (11/11/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/615/index.html

Security Update available for Adobe Reader 8 and Acrobat 8 (04/11/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/612/index.html

US-CERT: Microsoft Windows Server Service RPC Vulnerability (23/10/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/611/index.html

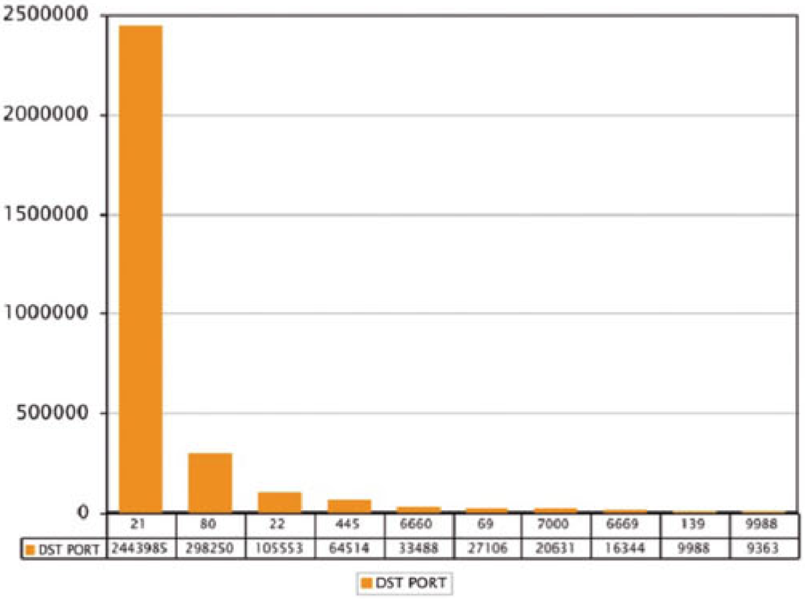
US-CERT: Microsoft Updates for Multiple Vulnerabilities (14/10/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/610/index.html

Activities from Research Network

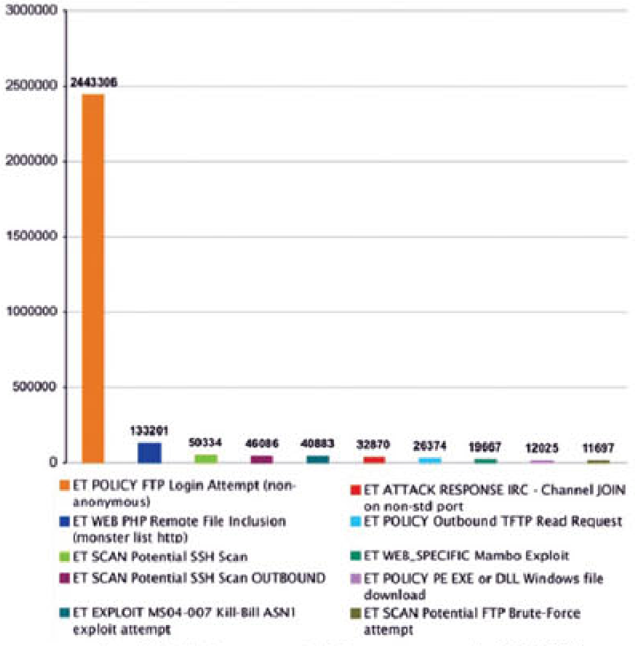
The CyberSecurity Research Network monitoring objectives are:

- To monitor the network for suspicious traffic as well as to monitor for the occurrence of known malicious attacks.
- To observe attacker's behaviour in order to learn new techniques being deployed, determine the popular techniques that are currently being used as well as confirm the continuous use of old and well known attack techniques.
- To compile and analyse relevant information of which the results can be used to alert the community of possible cyber attacks.

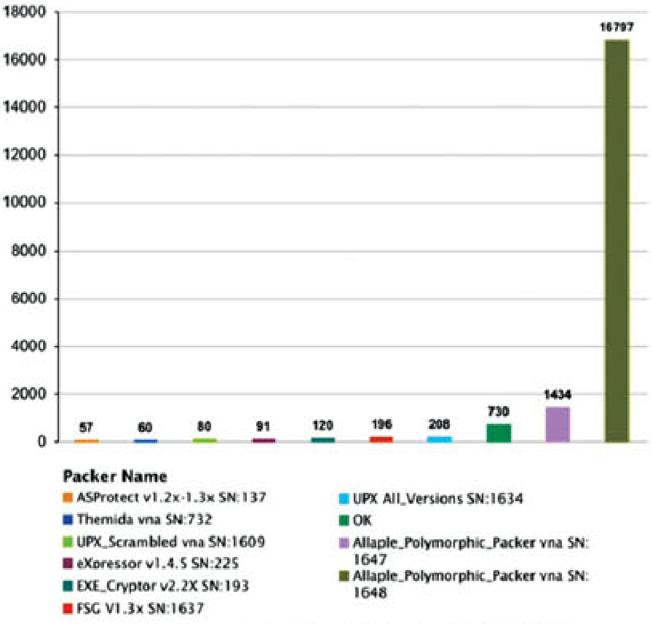
On the following page is a summary derived from MyCERT's research network for Quarter 4 2008.



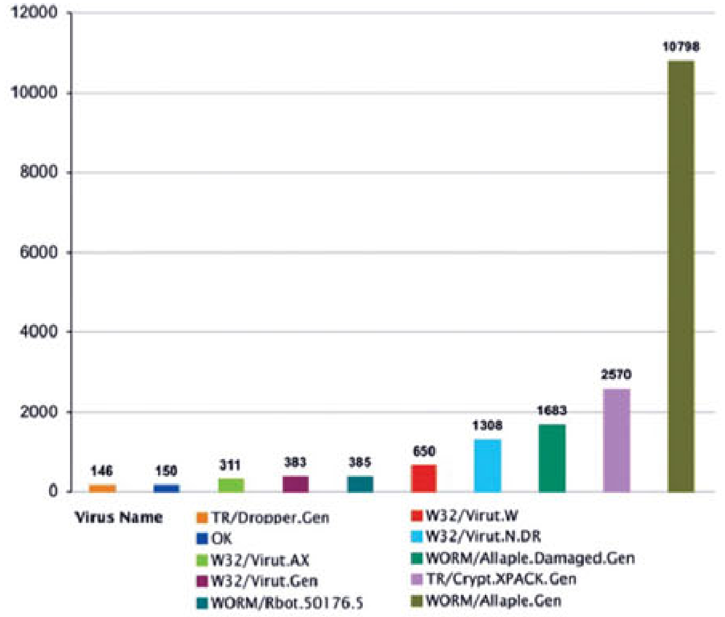
Top 10 destination ports attacked in Q4 2008



Top 10 alerts generated by our sensor in Q4 2008



Top 10 Packer used by Virus (Sigbuster) in Q4 2008



Top 10 Packer used by Virus (Sigbuster) in Q4 2008

Conclusion

Overall, the number of incidents reported to MyCERT had increased to 52.51% compared to previous quarter with incidents mainly contributed from spam incidents. Other reports that contributed highly to the number of incidents received this quarter are fraud, harassment and hack threats. MyCERT would like to advise Internet users and System Administrators to take precautions against the above activities. Neither crisis nor outbreak was observed in this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. MyCERT strongly advises users/organizations to report and seek assistance from MyCERT of CyberSecurity Malaysia in the event of any security incidents.

MyCERT can be reached for assistance at:

Postal Address
Malaysian Computer Emergency Response Team (MyCERT)
CyberSecurity Malaysia
Level 7, SAPURA@MINES
7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor Darul Ehsan
MALAYSIA

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

Phone
+603 - 89926969
(monitored during business hours)

Handphone
+6019 - 2665850
(24x7 call incident reporting)

SMS
+6019 - 2813801
(24x7 SMS reporting)

Fax
+603 - 89453442
(monitored during business hours)

Email
mycert@mycert.org.my or mycert@cybersecurity.my

Any feedback can be directed to MyCERT.

Produced on 06 January 2008 by MyCERT, CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI).

Revision History:
Initial Release
06 January 2008

Please refer to MyCERT's website at http://www.mycert.org.my for latest updates of this Quarterly Summary.

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

DFLive 2008

Your Swiss Army Knife in Digital Crime Scene

DFLive 2008 is a forensics live CD developed by the Digital Forensics Department of CyberSecurity Malaysia. The purpose of this live CD is to perform digital evidence preservation by first responders during digital crime investigation. It is designed to preserve the integrity of the digital evidence in a controlled environment and avoid the evidence from being contaminated or tampered. This live CD is equipped with various tools that can be used to perform evidence preservation procedures on both live and dead systems.

What is a live CD?

Live CD is a computer operating system that is executed upon booting, without installation onto a hard disk drive which contains a complete, functioning and operating system on the distribution medium such as CD-ROM, USB drive and memory. (Source: Wikipedia)

Operating System Specifications

DFLive 2008 is based on Slackware Linux 12.1. Slackware Linux is a highly technical, clean distribution, with only a very limited number of custom utilities. It uses a simple, text-based system installer and a comparatively primitive package management system that does not resolve software dependencies. As a result, Slackware is considered one of the cleanest and least buggy distributions available today - the lack of Slackware-specific enhancements reduces the likelihood of new bugs being introduced into the system. All configurations are done by editing text files. (Source: Distrowatch.com)

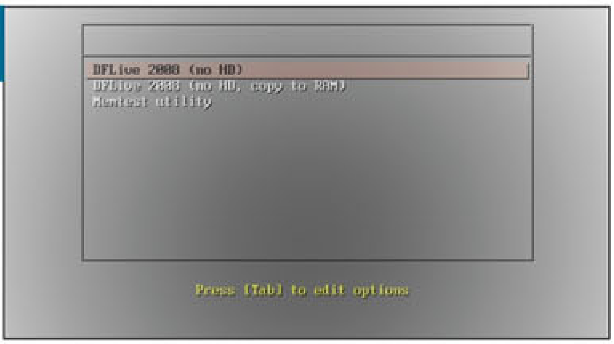
DFLive 2008 uses kernel 2.6.24.3 with SMP support. Desktop display will be auto probe; default resolution is 1024x768 at 75Hz depending on the monitor capability. User will enjoy the pleasant award-winning desktop KDE 3.5.9 as graphical user interface for the system. DFLive 2008 GUI is customised to be simple with clean environment appearance and to add to this excellent feature, it is only 533MB in size.

Boot Options

This live CD provides users with two boot mode options:

a) No HD mode option

This mode option will boot the system from the CD without automatically mounting the hard disk on the PC. It takes approximately 92 seconds from the boot menu to the login screen to appear.

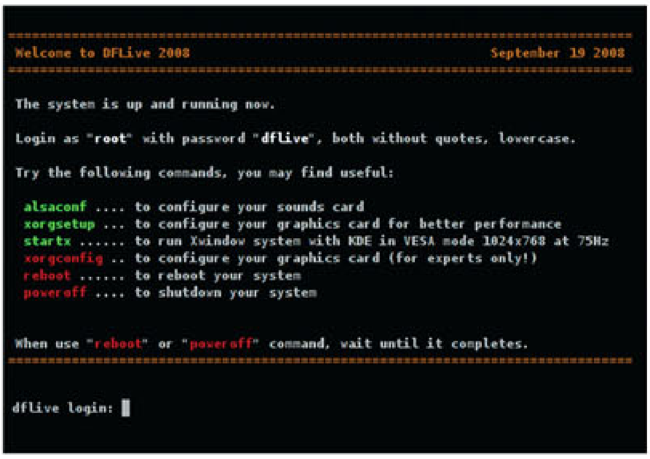


Picture 1: Boot menu.

b) No HD, copy to RAM mode option

This mode option will boot from CD also without automatically mounting the hard disk on the PC and load live system to RAM and automatically eject live CD after all loading processes are done. These mean the CD/DVD-ROM drives are free to be used. This mode takes approximately 256 seconds to load the operating system up.

However this is dependent on the hardware specification of the system being used. The above timing was tested on Lenovo T61, using Intel Core 2 Duo 2.4GHz and 2GB of RAM.

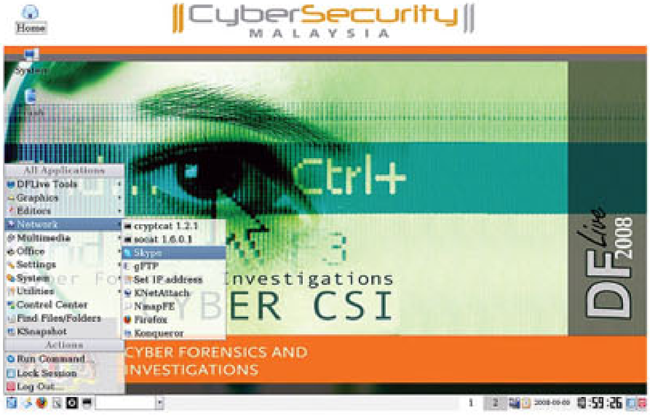


```
===============================================================================
Welcome to DFLive 2008                                        September 19 2008
===============================================================================

The system is up and running now.

Login as "root" with password "dflive", both without quotes, lowercase.

Try the following commands, you may find useful:

 alsaconf .... to configure your sounds card
 xorgsetup ... to configure your graphics card for better performance
 startx ...... to run Xwindow system with KDE in VESA mode 1024x768 at 75Hz
 xorgconfig .. to configure your graphics card (for experts only!)
 reboot ...... to reboot your system
 poweroff .... to shutdown your system


When use "reboot" or "poweroff" command, wait until it completes.
===============================================================================


dflive login: █
```

Picture 2: Login screen, user must read the instructions carefully.

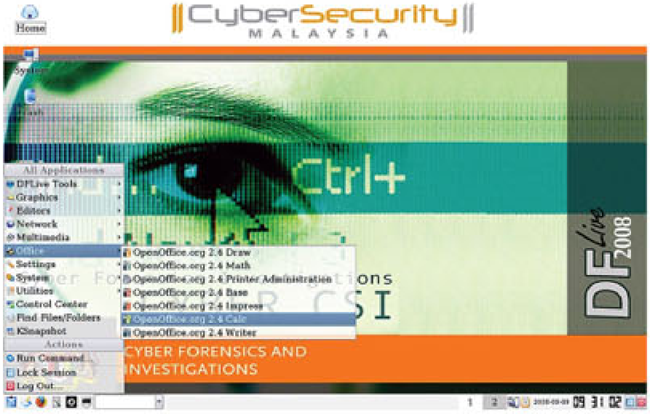
"Copy to RAM" option will provide faster operation compared to running the OS directly from CD-ROM. DFLive 2008 will use approximately 1GB of RAM to function at its optimum speed. It is highly recommended that the machine has more than 1GB of RAM size to operate without any problem.

DFLive 2008 Features



Picture 3: Common network applications for DFLive 2008.

DFLive 2008 supports approximately 120 common manufacturer network devices such as Intel, 3com and D-Link. The internet applications such as Firefox 2.0 (internet browser), Skype 2.0 Linux version (instant messaging) and gFTP (file transfer application) are packaged with this live CD operating system.



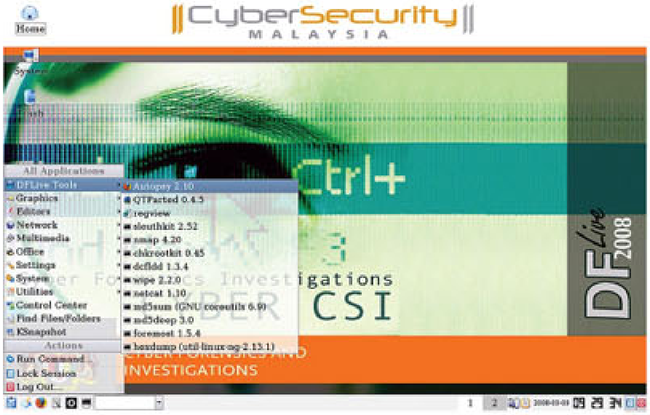
Picture 4: OpenOffice 2.4 is ready, a perfect word processor.

DFLive 2008 is also equipped with OpenOffice 2.4 for any documentation purposes during analysis. Other than that, users have access to multimedia files such as MP3 and AVI. On top of that, this live CD also allows users to have access to VCD and DVD.

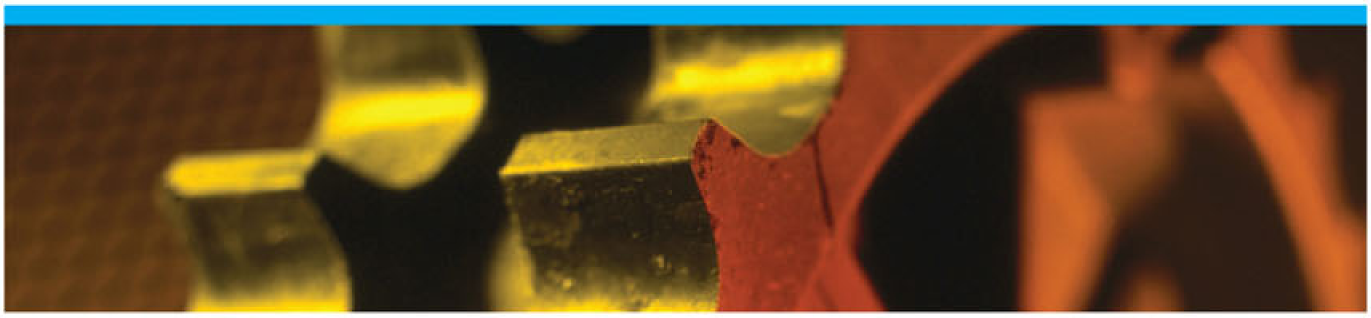
The DFLive 2008 has been tested and validated for working perfectly on any Intel/IBM based processor machines, be it a notebook computer, a desktop computer or a server computer.

Digital Forensics Tools

In this very first release of DFLive 2008, we have packaged together a total of 12 digital forensics tools. Updated version and more tools will be included in the next version of release.



Picture 5: Digital forensics tools features in DFLive 2008.



	Digital forensics tool	Description
1	Autopsy 2.10	The Autopsy is a graphical interface to the command line digital investigation tools in The Sleuth Kit.
2	QTParted 0.4.5	QTParted is a Partition Magic clone written in C++ using the Qt toolkit.
3	RegView 1.0	RegView is a registry editing and System restoring utility.
4	Nmap 4.20	Nmap is a security scanner to discover computers and services on a computer network.
5	Chrootkit 0.45	Chrootkit is a tool to locally check for signs of a rootkit.
6	Dcfldd 1.3.4	Dcfldd is an enhanced version of GNU dd with features that include on-the-fly hashing and status output.
7	Wipe 2.2.0	Block device wiping application.
8	Netcat 1.10	Netcat is a simple Unix utility which reads and writes data across network connections using TCP.
9	Md5sum (GNU coreutils 6.9)	Md5sum is a computer programme that calculates and verifies 128-bit MD5 hashes.
10	Md5deep 3.0	Md5deep is a signature analysis tool to compare hash value of a list of input files to a known hashes.
11	Foremost 1.5.4	Foremost is a console programme to recover files based on their headers, footers and internal data structures.
12	Hexdump (util-linux-ng-2.13.1)	HexDump is a Windows command-line utility which reads a binary file and writes text file with a hexadecimal dump of the contents.

Summary

DFLive 2008 is an open-source tool that is targeted to be used not only by the Law Enforcement officers in their investigation work, but also by IT professionals in responding to any IT security incident and preserving the digital evidence.

CyberSecurity Malaysia believe that the DFLive 2008 will be an alternative to other commercial digital forensics tools available in the market for conducting digital forensics investigation and analysis.

Any request for DFLive 2008 CD copy can be made via email. Comments and feedbacks are highly appreciated and can help improve the live CD in our next release. Please send any inquiry, comments or feedbacks to fendy@cybersecurity.my or zabri@cybersecurity.my.

References

'Slackware', http://slackware.com/, date viewed 10 September 2008

'Distrowatch', http://distrowatch.com/dwres.php?resource=major, date viewed 15 September 2008

'Linux Live', http://www.linux-live.org/, date viewed 4 August 2008

'Autopsy', http://www.sleuthkit.org/autopsy/, date viewed 10 August 2008

'Live CD', http://en.wikipedia.org/wiki/Live_cd, date viewed 1 September 2008

Defending Yourself at Wirel

Public wireless networks often referred to as wireless hotspots that are available everywhere since its introduction into the market in the year 2000. Nowadays, public places such as coffee shops, restaurants, airports and offices provide free wireless network services for Internet as a pulling factor.

Wireless networks provide a great deal of convenience and flexibility and are relatively easy to setup. As a result, more people implement wireless networks with no knowledge of wireless security threats due to

- strictly following quick step-by-step guide with default configurations setting
- do not read manual since some wireless devices have plug-and-play features
- failure to understand security threats that exist in wireless network environment

In this article, we will introduce the defensive countermeasures on how wireless users are able to

- defend their laptops before connecting them to wireless hotspots
- defend their personal data while connecting to wireless hotspots

Defending Wireless-enabled Laptop from Wireless Hackers

Before connecting to the wireless hotspots, it is recommended that wireless-enabled laptop users ensure the following five critical settings in the laptop.

Setting # 1 - Windows Preferred Network List (PNL)

Windows PNL is a standard feature in Windows Zero Configuration (WZC) which is intended to collect all information for all previously connected wireless network. When the wireless adapter is enabled, WZC scans wireless networks based on entries in the Windows PNL. If a wireless network is found, WZC will connect automatically to that wireless network. Otherwise, WZC will scan the nearby wireless networks for wireless users to opt for other wireless connections if there is no wireless networks found based on Windows PNL entries. Therefore, it is recommended to manage these entries in Windows PNL in order to avoid WZC making an automatic wireless connection which is not intended by wireless users. For sake of simplicity, all entries in Windows PNL should be deleted.

Setting # 2 - Wireless Driver

In general, each wireless card is accompanied with wireless driver. This wireless driver interacts with the operating system in order to process the radio communication signal. Recently, wireless hackers developed client-side attack by exploiting wireless drivers such as wireless card denial-of-service and arbitrary code injections. To avoid this potential wireless threat, it is recommended to update wireless driver from wireless card manufacturer accordingly.

Setting # 3 - Antivirus Software, Operating System, Application Software

In order to ensure your laptop is protected wireless, users are expected to update

- antivirus software signatures
- operating system patches
- application software patches

These patches are critical to defend against known vulnerabilities.

Setting # 4 - Personal Firewall

As a standard rule of computer security, personal firewall should be installed and activated. This personal firewall is intended to defend from wired-network attacks as well as an attack that may come from wireless networks. It is recommended that this personal firewall should be activated at all times.

Setting # 5 - Files and Folders Sharing

The most critical threat is when wireless users enable the file and folder sharing option. It gives the opportunity to wireless hackers as well as wireless malware to sneak in. For instance, Windows XP Home Edition manages files and folders sharing and uses the Guest account with a blank password for default access to shared files and folders. Therefore, it is recommended to disable the files and folders sharing option.

ess Hotspots

How to Access Wireless Hotspot Safely?

After defending wireless-enabled laptops, we will focus our attention on practices that are recommended when accessing wireless hotspot in order to ensure security of data and mobile devices. This section also highlights common bad practices that should be avoided.

In order to defend from cyber threats via wireless network, the common critical mistake usually made by wireless users must be avoided. The common critical mistakes are:

1. Tendency to connect to any free available wireless networks.

Usually these types of services have very weak security features due to no encryption or a shared password is used. With these configurations, wireless hackers are able to view all the transmitted wireless data including sensitive information. At any circumstances, do not connect to this type of wireless network if users do not have the sufficient protection settings described earlier.

2. Tendency to connect to weak encryption enabled wireless networks.

WEP encryption (whether WEP-40bit or WEP-104bit) are susceptible to WEP cracking as numerous tools easily crack WEP in less than 1 minute. Similarly, WPA with weak Pre-Shared Key (PSK) is also susceptible to PSK cracking. It is recommended that wireless users must not connect to the WEP-enabled wireless network and only connect to the WPA-PSK (with more than 8 characters in length), WPA - Enterprise and EAP wireless networks.

3. Always turns-on wireless connections.

Most wireless-enabled laptops scan for wireless networks automatically and the connection stays open even if wireless users do not surf internet browser application. If wireless-enabled laptop automatically connects to a wireless network run by potential wireless hackers, they might be able to search your computer for sensitive data, even information that would allow access to their respective corporate network. In order to avoid this unintentional connection to the unknown wireless network, wireless users must turn off wireless when they are not using it.

4. Neglecting which wireless access point, one is connected to.

Wireless users are usually more eager to surf internet and stay connected without considering which access points they are connected. It is recommended that wireless users verify which wireless network they are connecting to, from time to time.

5. Conducting financial transactions at any available wireless network.

Regardless the security features implemented in wireless network, wireless users are not recommended to conduct any financial transaction at wireless hotspot locations unless they are very sure that the application is encrypted and secure.

Conclusion

Wireless networks represent one of the greatest advances in networking in recent years without having to run network cabling through the floors and walls. With flexibility and convenience in implementation, wireless networks are a form of networking of choice. However, wireless networks are often configured insecurely due to lack of understanding in wireless network security implementation.

Wireless LAN Security, 802.11/Wireless LAN Wardriving & Warchalking **http://www.wardrive.net/, 11/02/2008.**

Flickenger, Roger Weeks. **Wireless Hacks, 2nd Edition**, O'Reilly, 2005.

Moerschel, Dreger, Tom Carpenter. **CWSP Certified Wireless Security Professional, 2nd Edition**, Grant McGraw Hill, 2006.

Symantec Enterprise Security, Wireless LAN Security-Enabling and Protecting the Enterprise, **http://www.symantec.com/avcenter/reference/symantec.wlan.security.pdf, 11/02/2008.**

Glenn, Josh. WLAN Security Challenges, 8/03/2005, **http://www.securitydocs.com/library/3534**, 11/02/2008.

DATA PROTECTION

Software Encryption vs Hardware Encryption

Introduction

A while ago, the best platform used to secure data in computers and IT products were several security components such as antivirus and firewall. Then, during the era of spamming and spyware, IT professionals looked at new approaches by countering issues with Anti-Spyware software.

Why is it important to secure data from being accessed by unknown users? From all issues in security and vulnerabilities, the one and only matter that an attacker is concerned with is the data that may only describe name and ID of the owner; he could still manipulate the useful data or commit fraud.

This kind of attack or unethical event should drive the need for a complete data protection or data security solution. Wikipedia, the free online encyclopaedia defines Data security as "the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data" . One of the best solution is to use data encryption, either software encryption or hardware encryption.

What is Encryption?

> Encryption is "the process of transforming information using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext)" . In short, one way to conceal data is by using encryption and authorised users are granted access based on proper authentication method. solution is to use data encryption, either software encryption or hardware encryption.

Software Encryption versus Hardware Encryption

There are many software and hardware that implement encryption within architecture which allow user(s) to encrypt data in a fast and secure manner.

Software based encryption provides privacy of data, depending totally on the computer systems disk by using the Processor (CPU) to perform encryption/decryption and related cryptographic operations. The variables that are selected to be encrypted based on the selection by user(s) in terms of specific files and directory (folder) could also include the non-operating system disk drive or vice versa. Not just on computers, software based encryption could also be applied to Mobile Application and Mobile devices.

Hardware based encryption is relatively the same concept as software based encryption but different via mode of its operation. Hardware based encryption provides the user with capability to encrypt/decrypt data on the fly within its own storage and with its own special chipset 2. Every process of encryption or decryption is done when the data is copied into the encrypted disk storage (external data storage) using small built-in software. Normally, the hardware based encryption uses a USB as the medium of transport for transferring data between computer and encrypted storage. It could be a small pen drive, an external hard disk or maybe a small watch that you could wear. Software encryption uses CPU as the main module to run the cryptography process although now PCs come with TPM chips that are capable of handling encryption and offloads the CPU from performing this function. For hardware encryption, the firmware will do. Both have different approaches but with the same goal i.e. security of data from unknown threats.

Table 1 below shows several advantages and comparisons that could be useful on deciding which method (hardware or software encryption) preferable to be implemented:

	Hardware Encryption	Software Encryption
Purpose of Usage	Single Purpose: - Eliminates PC performance penalty - Secures data inside the encrypted storage hard disk - Contains own processor and cryptographic algorithm - If applicable, acts as security token	Multi-purpose: - Message encryption via email, chat and VoIP - Digital Signature - Sign Email and Encrypt Attachments
Medium	Only within hard disk of: - External hard drive on the hardware device - USB Pen Drive - Secure Token - Smart card	- Create Virtual Container (Encrypted disk) - Use on Internal Hard Disk/Partition or External Hard Disk
User Accessibility	- Fast - GUI interfaces - Has its own software interface for data transferring to devices - Mobile - Small	- Need to create container if creating a virtual drives - Can be slow, depending on software - Complicated for first time user - Required manual
Space Limitation	Limit to the hardware storage space. - 512MB to 80GB. - Cannot be reduced	Limit based on internal hard disk free space. - Could reduce space limit by installing new hard disk
Enhancement	- Biometric Authentication & Authorization - Security Token	- Encrypt installed application - Lock Folder
Authentication	- Biometric Fingerprint - Password	- Password only

Table 1: Advantages/Comparison of Encryption Platform.

Recommendations on How to Secure Your Data

There are several ways to secure data from being breached. Table 2 below would recommend on how to handle data securely with the aid of hardware or software encryption;

Steps	Description
Purpose of Usage	Secure data from any accessible point of intrusion. - Always secure your encrypted data (inside external hard disk) and place it separately. - Safeguard your external storage (Hardware/Software Encryption) by hiding/put away into safe place when you are not using them. - Lock your computer with secure cable when leaving it. Also lock the desktop screen with password. - Before leaving your computer, dismount any Virtual Drive or Container. Save and close any data or application before leaving your computer.
Medium	Caring for your Private Data. - When carrying about your encrypted storage, always make sure it is hidden from sight and be selective with telling anyone. - Do not jumble up all your files inside one folder or container. Categorise files based on Level of Confidentiality (Public, Confidential, Top Secret, etc). - Use Mix Characters, Numbers or Special Characters when updating password. - Share your files using PGP key when exchanging attachments. - Do not lend your encrypted storage to others. - Do not share your password.
User Accessibility	Back-up & Recovery. - Always back-up your data from your computer to your encrypted drive. And also, if applicable, have an off-site external encrypted hard disk for secondary backup (may be placed at home). - Email: Have your PGP key (Private and Public) back-up in a safe place. - Have a different password for your secondary encrypted storage, if it is used for backup and recovery of data.

Table 2: Steps on How to Secure Your Data.

Nonetheless, there are also many ways on handling data securely in the Internet. Many security blogs, security portal and also Microsoft Products on Security explain how to handle the data especially when it is classified as confidential.

Other recommendations on how to secure the data by using applications and hardware are explained in Table 3 below.

Steps	Description
Email	**OpenPGP or GNUPG** Website: http://www.gnupg.org and http://www.openpgp.org * if using Mozilla Thunderbird, require enigmail for add-on extension (http://enigmail.mozdev.org)
Software Encryption	**TrueCrypt (Windows)** Website: http://www.truecrypt.org **Bit-Locker** Website: http://www.bitlocker.com * Integrated software inside Windows Vista. **Ghost (Mac OS)** Website: http://www.pointblanksoftware.com * Shareware; additional features available with registration.
Hardware Encryption	**IronKey Secure USB** Website: https://www.ironkey.com/dataprotection **T3 Pro Security Key USB** Website: http://www.tiss-msc.com * Also could be used as USB Security Lock Token.

Table 3: Hardware & Software Encryption.

Conclusion

Data encryption is important to secure personal information, financial statement, online banking transaction records and other confidential information.

Information Security is important and should be integrated in our lifestyle. Quoting Microsoft Senior Security Strategist, Steve Riley... to understand security is to implement Ten Immutable Laws of Security. Thus, I would also recommend understanding these three laws in securing our valuable information:

# Law 5: Weak Password trump strong security.
# Law 7: Encrypted data is only as secure as the decryption key.
# Law 10: Technology is not a panacea.

Therefore, necessary steps are to be taken to protect your personal details from threats and to be concealed using appropriate cryptographic algorithm or systems.

References

📖 Brute Force, Cracking the Data Encryption Standard, Matt Curtin, Copernicus Books, Springer, 2005.

10 Immutable Laws of Security; http://technet.microsoft.com/en-us/library/cc722487.aspx

NetAction's Guide to Using Encryption Software; http://www.netaction.org/encrypt/reviews.html

Seagate (SANS), Hardware versus Software; http://www.seagate.com/staticfiles/SeagateCryptofaceoff.pdf

NetAction's Guide to Using Encryption Software; http://www.netaction.org/encrypt

Hard Drive Encryption Software; http://www.techsupportalert.com/pdf/r1178.pdf

Taking Information Security

Organisations have differing views on ownership of information security within their organization. Majority park it under the IT Department, while others leave it to the Chief Information Security Officer (CISO) or the Chief Information Officer. Since late 2003, there were already talks and trend that information security governance should be part of corporate governance within developed countries. However, in Malaysian corporations are only beginning to look into it as more policy and regulatory requirements come into being.

In today's business environment, traditional boundaries are no more relevant. Contractors and outsourcing companies co-exist in the same work environment, leading to greater insider threats. Customers are given access to more key resources and information in order to make the best decisions. The so-called boundaries are blurred. Organisations are challenged to classify information, conduct valuation of information, assigning risk level and eventually identifying relevant controls to protect relevant information from breach of confidentiality, integrity and availability. Many organizations feel with a huge IT infrastructure, these tasks appear daunting, especially with legacy systems in place.

Why Corporate Governance?

Corporate governance is the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled. The ISG, Corp Governance Task Force Report, Apr 2004 stated that the road to information security goes through corporate governance. The document provided a framework on roles of Board of Directors, Executive Officers, Senior Officers and employees in information security. It also required implementation of security program, reporting requirements and independent evaluation.

In short, corporate governance is a platform and information security can be addressed effectively by leveraging that platform. How can information security be taken up to the level of board of directors? Will they spend time to listen on plans on implementing information security across the organization? They will, if the risk-based approach is used. Risks relate to impact to the organization image, safety, security, economy and business ability to function. As such, insufficient measures in addressing information security can lead to financial loss, such as loss of business opportunities, reputation and recovery cost. Financial impact can be used as the justification for inclusion of information security within the corporate governance.

In order to address information security issues across the organization, active engagement is required with key executives. The programs must reach everyone within the organization as well as extended to those that are in contact with the organization. It has to have systemic effect.

Characteristics of effective Information Security Governance

According to a report by CMU, SEI, CERT in 2007, there are eleven characteristics of effective security governance as well as ineffective security governance. Unfortunately, by observing most of the corporations today, the practice in place is the latter. Effective information security governance is when the agenda on security is understood at the Board of Director level. The board needs to address information security governance in line with corporate governance and profit projection. Controls and countermeasures are implemented on risk-based approach. Documentations are made for reference/guide, review and improvement and not for mere filing. Digital assets have clear ownership, and employees held accountable thus require reporting of any breach of policy. There is a security committee of senior executives from

Governance to the Next Level

across the organization that meet regularly to discuss effectiveness of security programs, new issues and to coordinate problem solving.

Quoted from Governing for Enterprise Security (GES) Implementation Guide, governance and management of security are most effective when they are systemic. The word systemic is often used in medicine and in this context it means the affect is on the entire system. What this entails is that the governance creates consistency and seamlessly interwoven into the culture of the organization that integrates people, technology and process. Contrary to common belief the information security is technical, effective information security governance requires integration between legal, operational, managerial and technical requirements. Information Security today need to be addressed in the business context, aligned with the organisation's strategic goals, operational framework, compliance requirements and technical system architecture. To sustain, the organization must move towards information security governance that is strategic and systemic.

Information Security within organization structure

I have heard the complaints and efforts, to no avail, by personnel given a portfolio on information security, among other functions, who were unsuccessful in bringing the security agenda to the attention of their top management. When information security dialogue sessions are held for CEOs, the CEO sends the CIO or head of IT.

In an organization, the information security ownership must lie within the number one position. It must be embraced by the rest of the employees and the board of director must provide the oversight. The appointed Chief Information Security Officer or Chief Security Officer must report to the highest level, even to the board deem necessary, the way an internal audit operates. That function cannot be assigned to the head of IT for example, that reports to several layers of management before it reaches the number one post.

Within an organization, often there are several departments that are responsible for security, such as physical security, ICT security, personnel security, risk management, internal audit, business continuity management etc. Often, these departments report to different key executives. The challenges faced by these various departments often have some commonality. The skills and knowledge required by personnel responsible within these departments are fast converging. The factor that drives the convergence is information. Information exists in many forms as such information security requires control measures that provide the same if not better protection regardless of format and medium when the information is at rest and in transit.

I debated recently with another practitioner as to whether units or departments with various security related function within an organization should be consolidated, or left as it is, decentralized, due to historical reasons and difficulty in mindset change among top management. Perhaps it is true that having common objectives does not warrant these departments to be consolidated and centralized. The disparate condition can be compensated by having coordination at a high level committee that consists of senior managers and key executives. This high level committee led by the top management, shall govern a security program, to address issues and to set strategic measures in information security assurance. Although it is a challenge to have the security related functions report to different key executives, however, it may survive by having a common organizational information security policy with aligned business objectives.

Measuring Benefit

Key measurement in making any business decisions is the ultimate financial gain. How much will I make or how much will I save? Security is often viewed of as how much will I save if I were to put these control measures in place and something does go wrong. As such, security awareness is often not part of marketing initiatives.

However, it is important that leaders see that security is also about how much you will make. An approach to this would be to put security awareness initiatives as part of marketing initiatives. Information Security awareness raising initiatives can also be part Corporate Social Responsibility in which it projects an organization that cares.

There are several ways to make information security as a mechanism to build customer confidence. However, corporations must realize there is no ultimate security and as such customers must not be eluded with thoughts of a panacea. Educating the customers of their roles in information security such as guarding their access to critical information, detecting and defending against scam and fraud, would be effective approach aligned with the information security governance.

Taking on the systemic effect, the benefits of information security governance shall not be limited to within the organization alone. Ultimately, it will benefit the customers through enrichment of trust and confidence in their services.

References

- [Information Security Governance, Corp Governance Task Force Report, Apr 2004]
- [Governing for Enterprise Security (GES) Implementation Guide, Carnegie Mellon Univ, Feb 2007]

9 Security Predictions For 2009

The economy will be driving many things in 2009, and IT security will be no exception. Securing corporate networks will continue as a high priority, but companies will be looking for ways to economize and will base technology purchasing decisions on a need-to-have vs. nice-to-have basis. But this doesn't mean they will want to sacrifice performance or feature richness, especially in security.

In addition, the digital ne'er-do-wells will be undeterred by the failing economy and may prove to be more active and organized than ever, which means the definition for security needs-to-have will change as perimeter security will no longer be enough. With growing numbers of applications to exploit, a plethora of online avenues and revenues to pilfer, and many more corporate networks to hack, cybercriminals will have no shortage of targets to pursue. The heightened interest and response from law enforcement worldwide in bringing cybercriminals to justice will force them to be even more aggressive and creative in their efforts to sidestep the law.

An active criminal element means companies can't afford to let their guard down, so IT departments will have to be even more proactive and expeditious in their defense. Fortinet has provided these "Top 9 in '09" security trend predictions to help companies safeguard their networks by mounting a multi-layered, multi-vectored and comprehensive defense strategy.

More bang for the buck -- security consolidation and then some

Integrated security appliances will happen in greater numbers than ever before as IT departments are pressured in a down economy to trim cost yet maintain network integrity - essentially, doing more with less. In addition to integrating two or more security functionalities into a single device for capital and operational savings, companies can look for "superset" security solutions that may encompass other network functionalities such as WAN optimization and SSL inspection. In a nutshell, efficiency will be the new technology must-have for 2009.

Web 2.0 vulnerabilities multiply

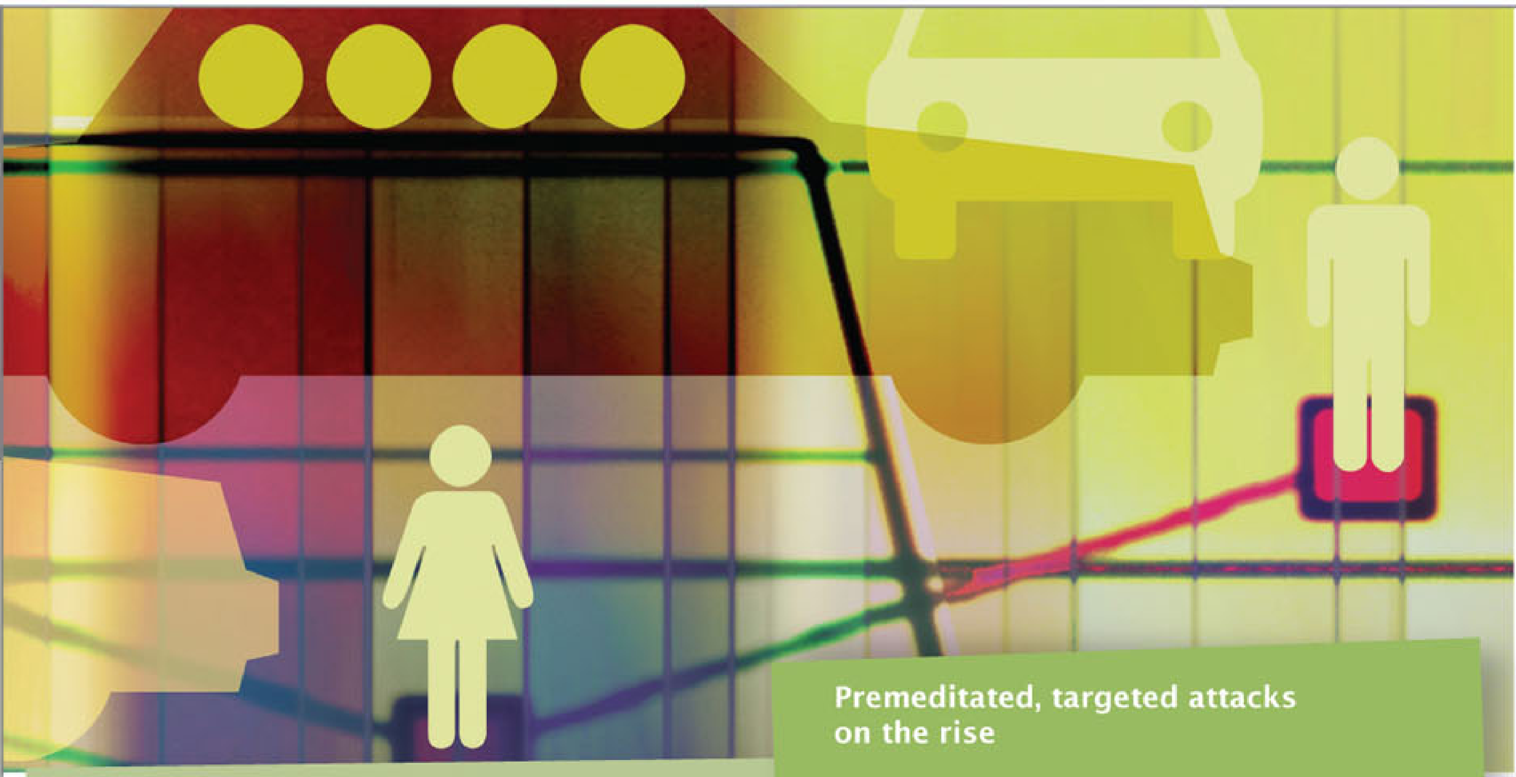
The popularity of social networking sites and in-the-cloud computing (such as SaaS) means the definition of the "network" is now greatly expanded and cyber criminals have many more chinks in the network armor to target as employees traverse in and out of the network proper. As a result, companies will find a greater need to employ web application firewalls and data leakage prevention mechanisms to avoid having employees bring back tainted data into the corporate network and from the inadvertent release of proprietary information.

Information security lockdown

With recent high-profile information theft (AKA database attacks) on TJMax and others, more companies are realizing that it's not enough to padlock the front door to their networks but they also have to put a watchdog on their databases - to detect and prevent both internal and external breaches. In addition, recent PCI-DSS regulations have been updated to require application firewall as a toughened measure for protecting consumers' credit information. As a result, greater emphasis will be placed on database security and regulation compliance, forcing companies to incorporate information security measures as part of their overall network security strategy.

Bigger pipes, faster speed - letting in the good, bad & ugly

10 GbE throughput is not a pipe dream but a welcomed reality, with adoption expected to surge in 2009. But opening up the network spigot means there's also a lot more bad stuff getting in with the good. Enabling 10GbE security protocols that work at the speed of the network is crucial and should be the next area of focus for maintaining the integrity of high-speed networks.



3G -- the next biggest threat to mobile security

Malicious activity on smart mobile devices like smart phones has been low to date, but the anticipated consumer adoption of 3G and the new and business models it enables opens up a new and enormous market for cybercriminal activity. For example, we are just seeing the tip of the iceberg with Google's recent Android OS vulnerability. 3G enables network operators to offer a wider range of more advanced mobile services, such as real-time access to high-quality audio/video transmission, and greater network capacity. This all adds up to greater opportunity for virus infections and attacks and requires a focused approach to securing the millions of handheld mobile devices in operation today.

More cash to flow in the digital underground

Over the last couple of years, organized cybercriminal operations have been building their base and will now look to extend trade with others. More services will be offered, such as botnets or harvested account networks (e.g., social networking). Affiliate programs will increase as organizations will seek to fuel their existing framework; if it works, they will offer more programs/incentives to "script kiddies." A new generation of users are plugging into cyber space. This generation will be more exposed to underground channels, and framework such as phishing/exploit kits. This will in turn tempt more of this generation into joining the dark side.

Premeditated, targeted attacks on the rise

Throughout 2008, we saw a steady drop in monthly distributed malware -- with the exception of the scareware attack, which drove much of the malware volume in the latter half of the year. As we enter an age of information warfare, targeted attacks using custom malware become much more of a presence. We will see more on this front in 2009: premeditated attacks after specific goals, with most of these attacks targeted toward enterprise and governments.

Let the games begin

Online gaming has gained much momentum, particularly in Asia, over the past year. This will continue to grow with the next generation of users. As a result, more interactivity will occur in these virtual worlds. We have seen a sharp increase in Trojans targeting account information, and this will be something to look out for in 2009 as this market grows.

Law enforcement unite online

Law enforcement mounted an aggressive effort in 2008 in bringing malware authors and criminal organizations to justice. We will no doubt see more of this welcomed activity in 2009. However, it will take more than just one year in 2009 to fully get up to the required pace and infrastructure to adequately deal with cyber crime. This will be a slow process, which will require an unprecedented effort between various bodies from law enforcement to effectively address issues in cyber security.

Internet Safety

Introduction

Keeping safe from malware and malicious activity on the Internet is an ever-present challenge even for knowledgeable information security professionals. How then, can the millions of non tech savvy Internet users out there protect themselves? The answers are not simple and the challenge of helping the masses stay safe is enormous.

The Internet Threat Landscape

The information security threat landscape of the Internet is one of the fastest changing environments on the planet, filled with some of the most esoteric technical jargon such as the following:

Intrusion, phishing, virus, Trojan, denial-of-service, botnet, identity theft, scams, spyware, adware, key-logger, rainbow crack, spam, cracking, whaling, DNS cache poisoning, worm, ARP cache poisoning, man-in-the-middle, code injection, crimeware, child predators, spear phishing, social engineering, rootkit, cross site scripting, drive-by-downloads, blended threats, etc.

These terms and the meanings of the threats behind them are obviously well known to information security professionals and technical wizards but just how many are really understood by the average computer user, particularly those with no IT background and just use the computer as a tool? It is clear that many are not even aware of the majority of such threats unless they become headline news and by then it is probably already too late. Even with awareness, it does not mean these people know what to do to mitigate the threats. To compound the problem, new ever more sophisticated threats with new jargon appear ever more frequently. Mitigating such threats is a full time job for information security professionals charged with securing their networks, servers and services, so where does that leave Joe User at home and small enterprises, whose computer is now a valuable asset to cybercrime syndicates?

Countermeasures

The information security industry has been responding to these threats ever since the first Internet worm but it has been a patchy and mostly reactive response, which has spawned its own set of technical jargon for the user to digest:

Anti Virus, firewall, anti-spam, anti-spyware, adware scanner, intrusion detection, rootkit detector, intrusion prevention, event correlation, defense-in-depth, vulnerability scanner, penetration testing, code audit, software patching, configuration management, backup, DNSSEC, mac address management, VPN, encryption, identity management, network admission control, etc.

The average computer user is probably aware of the first five items. Unfortunately, the vast number of products, bundles, services and marketing tactics from information security vendors make it difficult and confusing for non-technical users to evaluate and select the right set of complete tools. The complexity of managing a set of five tools presents a significant challenge to the users without technical skills. To add to that, these tools are constantly evolving to counter new threats and non-technical may not install and keep these tools up to date or replace tools that are ineffective. The result is a vast number of inadequately protected systems.

Evolution of Malware

Malware has evolved from being experiments and pranks in the beginning to being a tool of cybercrime syndicates. As corporations effectively adapt to mitigate information security threats, these syndicates have switched to far more vulnerable targets, home users. While a single home user's computer may not be a major asset, vast numbers of such machines managed by a sophisticated command and control system turns these individual zombies into a fearsome weapon, botnets, vast armies of zombies numbering as high as a million or more computers. In order to maintain these botnets, it is vital that the botnet software is not detected and removed by users and to remain undetected, malware behaviour has changed from being brash and "noisy" to being stealthy and seemingly benign and even useful with a hidden purpose. The previous races by malware creators to be the first to publicly claim to have developed an exploit for any new vulnerability have largely subsided, now new vulnerabilities are closely guarded secrets to be used for criminal and financial exploitation.

Malware sophistication is only increasing, largely given that the limitations of size no longer apply and come with combinations of the following, *inter alia*, capabilities:

- Remain undetected (morphing, encryption, modular, silent, proactive)
- Payload enhancement / modification (phone home downloadable plug-ins)
- Simple, scalable, mass command and control capability (IRC channels, web)
- Information harvesting (keyloggers, sniffers)
- Traffic redirection (DNS/ARP cache poisoning)
- URL injection
- Multiple infection mechanisms (web, email, IM, flash drives, network)
- Offensive Stance (disable scanners, compromise AV web sites)
- Exploit undisclosed vulnerabilities (silent exploitation)

The Reality of Countermeasures

While malware grows in sophistication and frequency, what has really been happening to the information security industry? The following might be an indicator of the state of affairs in the industry.

In an interview with ZDnet UK on the 30th June 2008[1], Eva Chen, Chief Executive of Trend Micro admitted the following:

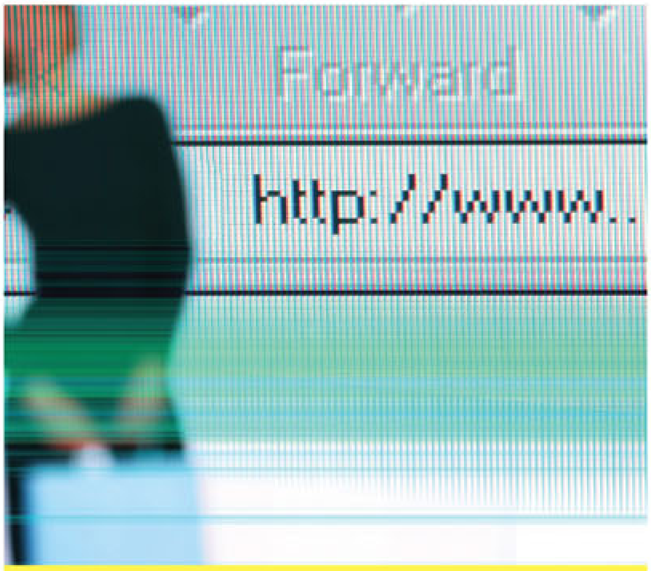
> **“In the antivirus business, we have been lying to customers for 20 years. People thought that virus protection protected them, but we can never block all viruses.**
>
> **No-one is able to detect five and a half million viruses.”**

Who else has been “flexible” with the truth? Do Intrusion Detection / Prevention systems really work? Do deep packet inspection firewalls really work? Do network anti-virus appliances really work? What are the gaps in their performance?

To compound the problems, malware today has the capability of identifying and disabling countermeasures, for example, viruses which disable virus scanners in such a way as to continue to appear to be working. Malware active in memory can also hide from scans which then require the user to reboot in “safe mode” in order to run a virus scanner and some viruses can even prevent a reboot into “safe mode”. Worse still, some windows virus scanners cannot operate normally in “safe mode” and requires the use of an MSDOS command line version. All of these contribute greatly to the difficulty faced by non technical users.

Another issue is that information security vendors do not regularly share information with each other, seeking to maintain perceived technology leads over each other in order to claim to be the “better” than the rest. On the other hand, the hackers community is constantly sharing information with each other in chat rooms and websites, making partnerships, renting botnets, etc.

Despite these issues, the limitations of vendors’ products are well-known to information security professionals, and who have the knowledge and experience to mitigate these weaknesses with processes, procedures and technical design. Unfortunately, the reality for the average home and small business user is blissful ignorance.



Enterprise Information Security

Most large organisations today are well aware of information security threats and should have the resources to manage in-house or out-source information security services. Information security standards, best practices and processes are evolving to counter the threats as they arise.

Through the implementation of information security standards, policies and practices these organisations will, eventually, be able to cope with and mitigate the threats to a manageable level.

The “Big Boys” therefore will, largely, be able to take care of themselves.

Home and Small Business Internet Safety

The majority of small organisations and individual Internet users are not tech savvy, do not have resources, cannot afford to out-source and are generally overwhelmed by the "Threat Tsunami" and the complexity and ineffectiveness of countermeasures deployed without expertise.

Unfortunately, information security standards being developed will not help these two groups much - how do you get the standards to these groups and get them to implement processes and best practices? Even if such standards were available for free, the awareness outside the sphere of information security professionals is minimal.

Clearly, there is a huge gap in the protection of such users, and it is probably not incorrect to assume that these inadequately protected computers are the primary contributors to the botnets out there.

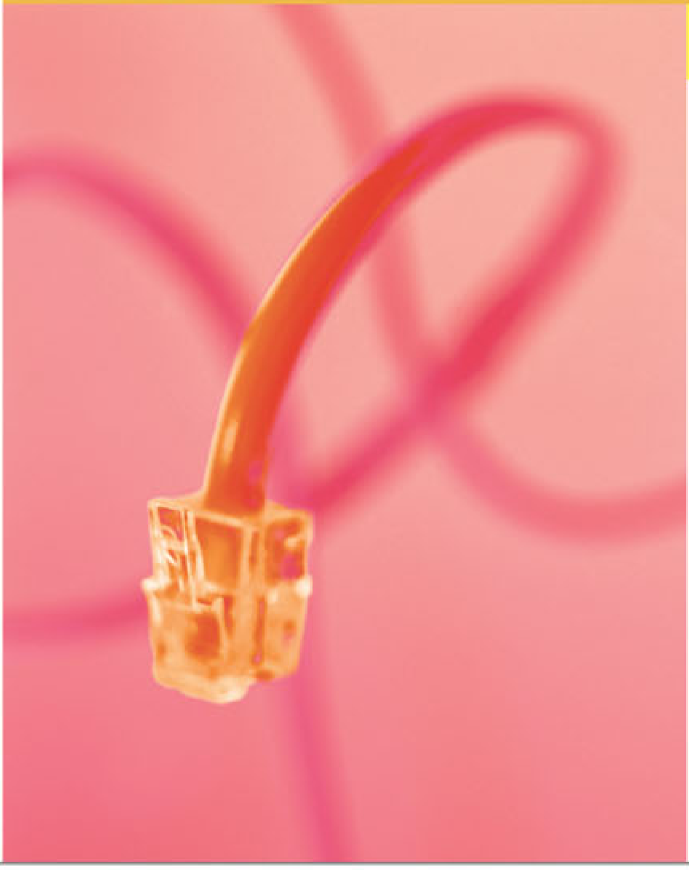
There is an estimated 1.4 Billion people online[2] and their numbers are growing at an average 290% from 2000-2008 (Source: 31st March 2008 - www.internetworldstats.com). The question is how many of these people know enough about Internet safety issues to effectively mitigate the risk?

Even if just 10% of these people were vulnerable, that would mean there are 140 Million potential Zombie machines out there. Unfortunately, with an estimated 15 Million IT professionals worldwide[3] (Source: Capers Jones, chief scientist emeritus of the Software Productivity Research, SPRI), the 10% figure is probably wrong by being far too small.

The information security industry cannot afford to do nothing as the scale of the problem is only increasing and we have already seen direct attacks on vendors of information security products as the malware industry strategy changes to target and disable the defenders.

Conclusion

It would appear that the information security industry is losing the battle to keep non technical Internet users safe. Information security product vendors and operating software vendors need to keep up with the crimeware industry by developing more secured products and continuously improve them to be more resilient and user-friendly, especially for non-technical users. They should also provide clear information for their non-technical users on maintaining and updating software.



References

[1] Trend Micro: Antivirus industry lied for 20 years. http://resources.zdnet.co.uk/articles/features/0,1000002000,39440184,00.htm

[2] World Internet Users and Population Stats. http://www.internetworldstats.com/stats.htm

[3] IT Management. http://www.iss.nus.edu.sg/iss/article_display.jsp?artid=1020

BOTNET 101

for the rest of us mortals

The Internet has been experiencing an exponential growth over the past decade and the phenomenon has, unfortunately, brought along an increasing number of intrusion incidences on computer systems worldwide. Nowadays, any computer that is connected to the Internet is never truly devoid of facing the risk of being attacked by computer hackers. And over the years, contrary to the popular culture portrayed by Hollywood movies, it appears that the motivation that drives these hackers has very much shifted from exposing the corrupt practice of a corporate giant or getting the much sought after recognition among their peers in the hacker community to one that is driven by good old financial gain. Simply put - they hack for money. And one of the most recent, sophisticated and widely used techniques are done through the deployment and manipulation of botnets.

> **“Gone are the days of hackers launching homemade viruses, worms with disease-like name variants and backdoor programmes to prowl into the hard disks of some army dude's PC to find some secret plan. Well, they probably still do that.”**

If your computer has been suspiciously sluggish albeit being the most high end (of the month) and you admittedly could not remember the last time you update the virus definition of your antivirus software (or if you even have one), let alone to even care what you allowed to pass through the firewall checks, then there is a good chance that your PC might have already been a bot of a network of bots, all this while. In other words, your PC has been compromised and you may not be the only one having a control over it anymore. A BBC news report quoted Internet expert and co-developer of the TCP/IP, Vint Cerf, as saying that “Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets.” He also said that, “Of the 600 million computers currently on the Internet, between 100 and 150 million were already part of these botnets.” And that was in 2007.

If you thought that the name botnet somehow reminded you of robot and the Internet, well, in a way, you are right. A botnet refers to compromised computers or computers that, other than their rightful users, are also under the control of a remote user - someone who can be anywhere in the world and conveniently nicknamed – the bot herder. Imagine a scenario where the bot herder, in God knows which spiteful ways, has somehow managed to install a malicious Trojan virus program into your PC. The Trojan will install or propagate itself into your operating system and checks if the host (i.e. your PC) is online. If it is, the said programme will then send out a connection request to the controlling programme on the bot herder's end and he would instantly know that he had just made a catch. This will later open up a secured connection channel between the herder and his herd(s) and he will then be able to communicate seamlessly with all of his bots – signifying a one-sided everlasting relationship and more ghastly things to come.

The bot (previously known as "your PC") has become but one of many nodes in this botnet. The bot herder will use a system to act as the Command and Control centre in which instructions will be issued through this system. It is the one PC to rule them all. And sometimes, a bot is also used to control other collection of bots; which further deepens the hierarchy. But one thing in common though, all will come under his ruling and waiting to be commanded to his liking - which more often than not spells "exploits"! These exploits could range from launching DoS (Denial of Service) attacks to websites, sending out spam emails to unsuspecting recipients all over the world and to commit identity and financial information theft such as harvesting for your banking login IDs and passwords and even your credit card numbers. And all those abuse will take place without you even realizing them, until it is too late. This is even worse than signing up for something and later realising that they are sending you to war!

In a way, a botnet can also be considered as a distributed computing effort more or less similar to the one that is genuinely being carried out by the SETI@home project **(http://setiathome.berkeley.edu/)** but unlike those hopeful extraterrestrial enthusiasts, these bot herders did not ask for your permission to use up your computing resources and they sure are up to no good.

You wouldn't know what else your PC has been doing other than running your usual word processing software or browsing the Internet; but nevertheless, you may have been noticing that the PC has been alarmingly getting slower as if it was running and processing lots of other programs in parallel and apparently also consuming a good chunk of your Internet bandwidth, even though seemingly you have not been downloading or uploading anything - and this is why bot PCs are also known as zombie PCs. For all you know, there maybe something wrong somewhere in your PC, but unbeknownst to your unwary self, on the other side of the world, a bot herder in his basement is amassing all of his thousands of online army of bots (that would include your PC) to help launch a coordinated DoS attacks on a well-known and popular website in a bid to render it inaccessible to the rest of other Internet users - for reasons known only to him.

In 2004, a network of more than 10,000 bot PCs has been dismantled after security staff at a Norwegian telecommunications company, Telenor, located and shutdown its controlling server. In June of the same year, the huge Internet content and application delivery company, Akamai, whose client includes Microsoft and Yahoo! was attacked with a Distributed Denial of Service (DDoS) attack launched by a bot herder in Florida. The DDoS attack sent in bogus traffic to Akamai's DNS servers which rendered its hosted sites inaccessible to the Internet users for a good few hours. The bot herder was apprehended, and consequently charged in the US federal court. In 2005, three men were arrested in Holland for creating a super large botnet of about 1.5 million compromised computers! A Dutch spammer, who was also arrested in the same year, had used around 600 to 700 bots PCs in his botnet to send about nine billion spam messages to all over the world promoting penis pills, pornographic websites and other sorts of advertisement. Some bot herders are even known to sell or rent the access to the botnets they owned, to interested cyber criminals and underground parties. However, all is not lost quite yet. Any Internet user actually has a sporting chance in preventing their PCs from becoming one of the bots. But they should, first and foremost, take all the necessary precautions to ensure that no Trojan virus program can ever get into their PC in the first place. And here are some of the preventive measures that you should adhere to in order for your PC to stay yours:

1

Never open any email attachment you received from unknown and unsolicited sources. If the sender's email address says that it is from your relatives or friends, it would be a smart move to clarify with them first to ensure they did send you those attachments.

2

Always update your antivirus software to the latest definition and fixes. New Trojans are produced now and then; and your antivirus must be recent enough to be able to identify them whenever they come knocking on your door.

3

Do not use pirated software as they often came with Trojans pre-installed on them. And you thought that those pirates are being kind enough to spend nights cracking and reverse engineering expensive software just to share them with you?

4

Do not install any JavaScript, ActiveX and such from any website unless you are really sure of what you're doing. Checking it up first with your IT-savvy acquaintances is even better.

5

Do not arbitrarily plug in any portable disk or thumb drives that aren't yours and drag or copy files out of them into your PC, without properly scanning them first.

Major security firms have been researching and work on devising complex and clever methods to identify these compromised PCs and ways to locate and stop them. Nevertheless, since bots, first and foremost, had to be initiated through virus infections from within a user's PC, early prevention approaches as per listed above are perhaps your best defense for now.

References

Daswani, N., Kern, C. & Kesavan, A. 2007. **Foundations of Security: What Every Programmer Needs to Know.** Berkeley: Apress.

Evers, J. "Bot herders may have controlled 1.5 million PCs", ZDNet News, **http://news.zdnet.com/2100-1009_22-5906896.html**, October 2005.

Johns, M. 2008. **On JavaScript Malware and related threats: Web page based attacks revisited.** Journal in Computer Virology 4:161-178. Springer.

Leyden, J. "Rise of the botnets", The Register, **http://www.theregister.co.uk/2005/03/15/honeypot_botnet_study/**, March 2005.

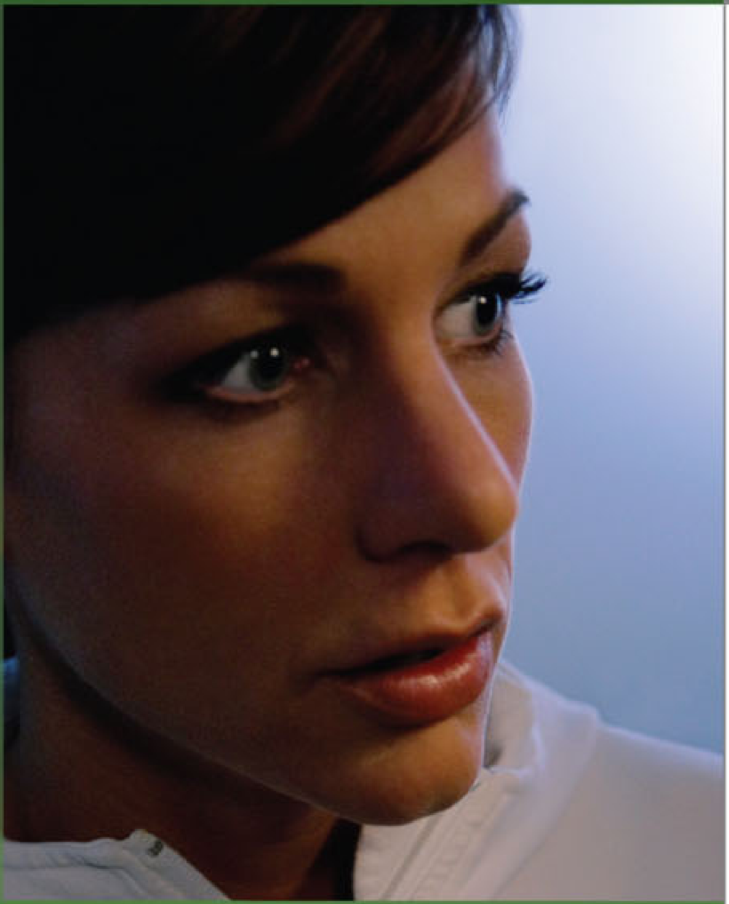
Thing, V.,Sloman, M. & Dulay, N. 2007. **A Survey of Bots Used for Distributed Denial of Service Attack.** 22nd IFIP International Information Security Conference: 229-240.

Thomas, V. & Jyoti, N. 2007. **Bot countermeasures.** Journal in Computer Virology 3:103-111. Springer.

Weber, T. "Criminals may "overwhelm the web"", BBC News, **http://news.bbc.co.uk/2/hi/business/6298641.stm**, January 2007.

Information Security Best Practices Series: How to avoid becoming a victim of Cyberstalking?

Cyberstalking is the use of the Internet or other electronic communication medium/device such as mobile phone, PDA used as a means to stalk or harass someone. The internet today is very much people-centric, where people from various age groups, background and interest come together to share and exchange information for personal or business reasons. While the internet enables people to connect globally with anyone without prior knowledge of their background, it opens up opportunity for criminals to commit crime against people as in the real world. These include fraud and embezzlement, harassment, identity theft and stalking. There can also be much of your personal information posted by yourself or your friends online. The criminal can find and use this information to his/her advantage. They can become your friends online via chat rooms and social networking sites by pretending to be someone they're not. The anonymity on the Internet provides new opportunities for stalkers, since a person's online identity can be easily concealed through the use of different screen names or personal profile information. The fact that cyberstalking does not involve physical contact may lead to the misconception that it is less dangerous than 'real life' stalking. Information gained online by stalkers can easily lead to physical contact, once the victim's location is known.



What can you do to avoid being a victim of Cyberstalking?

- Do not respond to threatening messages or messages that makes you feel uncomfortable.
- Choose a genderless (e.g.Topbird) screen name or a name that is different from your real name.
- Do not complete the online profiles with your personal information. Limit the information posted on your profile.
- Be careful when you post picture of yourself, your family or your friends online. You can put yourself or your associates in trouble with stalker.
- Do not flirt online, unless you're prepared to face the consequences, just like real life.
- Save offending messages and inform the police or MyCERT (A service by CyberSecurity Malaysia - www.mycert.org.my).
- If someone makes threatening remarks in a chat room or on a message board, notify the Police, MyCERT or website moderator/owner immediately.
- Do not confront the stalker, this only create more anger or emotional attacks.
- Get out of a situation online that has become hostile, log off or surf elsewhere.
- Do a web search on yourself to make sure no personal information is posted by others about you.
- Do not respond to any message that seems suspicious.

If you are a victim of Cyberstalking

- If you are under 18 years old, you should inform your parents or guardian whom you trust.

- If the cyberstalker is known, send them a written warning letter to inform them that you will stop communicating if threatening messages are continued. You must keep copies of all communications (hard copy and electronic copy) and do not meet the stalker. It would be advisable that you inform the authorities such as the police or Malaysian Communications and Multimedia Commission (MCMC) when you do this.

- If the harassment continues, you can inform your Internet Service Provider (ISP) to block or filter communication from specific individual.

- Do a web search on yourself to make sure no personal information is posted by others about you.

- Do not respond to any message that seems suspicious.

- If you suspect that you are victim of cyberstalking, collect and keep any form of evidence and document any communication with the stalker.

- Victims should consider changing their e-mail address, Internet service provider, phone numbers, use encryption software, use privacy protection programs and email filtering/blocking software.

- Victims must not meet the stalker face to face to solve the problem as this can be very dangerous.

Possible effects of Cyberstalking

Cyberstalking can be threatening and frightening as any other type of crime even though you may not have any physical contact with the stalker. Victims of cyberstalking can experience psychological trauma as well as physical and emotional reactions. Some of these effects may include:

- **changes in sleeping and eating patterns**
- **depression**
- **anger**
- **nightmares**
- **anxiety**
- **helplessness**
- **fear**
- **shock and disbelief**

Victims should seek help from friends, family or professional counselors in order to cope with the trauma resulting from cyberstalking.

What can I report and who can I report to?

If you feel that you are in danger, consult or report to the local authorities (e.g.: the Police, Malaysian Communications and Multimedia Commission (MCMC)). Ensure that you keep a copy or logs of all communications as proof. This evidence gathered not only provides clues to law enforcement for determining your stalker's identity but also critical to proving criminal intent if legal action is warranted in the future. Reporting or informing a third-party organisation such as CyberSecurity Malaysia can support the investigation that is to be carried out. Reporting the incident to the police will put you in the best position to find the cyberstalker and they will be able to provide advice on your safety.

You can report the following cyberstalking activities:

- **Threatening messages**
- **Death threats**
- **Sexual harassment**
- **Slander**
- **Harassment**

As an added precaution keep any electronic copies or logs on removable media such as external disks, flash drives, or CD ROM. Do not retain this information on your hard drive as stalkers may attempt to gain access to your computer, when you are online, or by using a virus sent to you through e-mail to erase the evidence.

Risk Management within ISMS

ISO/IEC 27000 Family Of Standards

Information security management is a common concept in today's world of zeros and ones. Well, at least it should be. Many times we have read about information security principles like the CIA (confidentiality, integrity, availability), defence in depth, the triad of people-process-technology, and many other frameworks used to describe information security requirements and its related domains. This is due to the fact that information security needs to be looked from a holistic point of view. It needs to be managed and this is why an Information Security Management System (ISMS) is very important in any organisation. ISMS is a systemic approach, based on risk assessment to establish, implement, operate, monitor, review, maintain and improve information security.

Many standards have been developed and accepted at international level to be used as the ISMS reference and guidelines. ISO/IEC 27000 family of standards are a series of standards that specify the requirements and provide guidance for ISMS implementation. FIGURE 1 illustrates the current initiatives in the ISO/IEC 27000 family of standards that include both standards that have been published as well as those which are still under development.

ISO/IEC 27001:2005, published in 2005 is the main standard in the 27000 family and it specifies the requirements for an information security management system. It is being supported by the other standards in this family that provide guidance and detail explanations for relevant processes as required by the main standard.

ISO/IEC 27000 provides an overview and vocabulary to ensure consistent terms and definitions used across all the standards in this family. It is expected to be published in 2009.

ISO/IEC 27002:2005 was previously known as ISO/IEC 17799:2005, published in 2005. It was renumbered to 27002 to make its reference consistent with the rest of the standards in this family. It provides guidance on information security objectives and selection of controls within eleven security domains, thirty nine control objectives and one hundred and thirty three controls.

ISO/IEC 27003 aims to provide practical guidance for the implementation of the Plan-Do-Check-Act model in the ISMS processes. It is expected to be published in 2010.

ISO/IEC 27004 aims to provide guidance on a specific requirement in ISMS measurement. It is expected to be published in 2009.

ISO/IEC 27005:2008 was published recently and is about information security risk management to address the mandatory requirement in managing information security risks in an ISMS implementation.

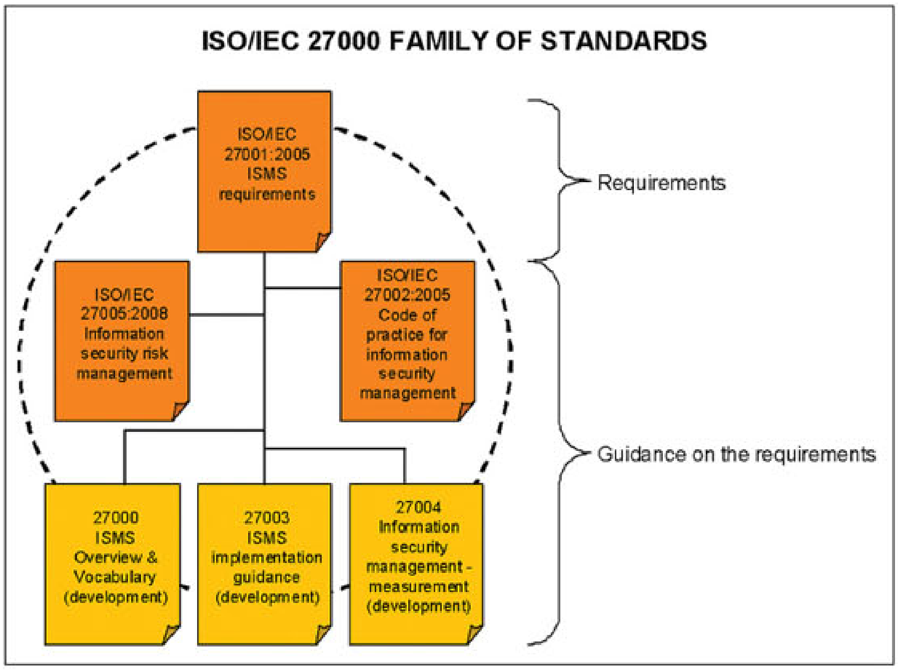

ISO/IEC 27000 FAMILY OF STANDARDS
ISO/IEC 27001:2005 ISMS requirements
ISO/IEC 27005:2008 Information security risk management
ISO/IEC 27002:2005 Code of practice for information security management
27000 ISMS Overview & Vocabulary (development)
27003 ISMS implementation guidance (development)
27004 Information security management - measurement (development)
Requirements
Guidance on the requirements

Figure 1

The New Standard

ISO/IEC 27005:2008 Information Security Risk Management made its debut in June 2008. This newly published standard was prepared by the Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques. It is meant to provide better guidance for information security risk management, in meeting the requirements as set in the ISO/IEC 27001:2005. It is certainly needed as the risk assessment requirement was not discussed thoroughly in the main standard. The requirement may be subject to interpretation by the implementers as well as the auditors which actually pose a challenge within the ISMS communities.

This standard describes the information security risk management process and mapped it well against the PLAN-DO-CHECK-ACT model to ensure a continual information security risk management. FIGURE 2 illustrates the activities involved in each of the phase and this is further described in TABLE 1 and TABLE 2 with details of the relevant clauses from the requirement (ISO/IEC 27001:2005) and the guidance (ISO/IEC 27005:2008) standards.

Planning information security risk for an organisation requires vast effort. This is evident by the number of requirement clauses in ISO/IEC 27001:2005 and the guidance clauses in ISO/IEC 27005:2008. The planning stage includes establishing risk concept, performing the risk assessment activities, identifying risk treatment options and getting approval from the management on risk acceptance. Risk objectives must be determined and shall be aligned to the organisational ISMS policy on risk management. From here appropriate risk assessment approach could be selected to address the risk objectives identified earlier. During the risk assessment exercise, it is important to have the right individuals involved because some decisions may be required throughout the exercises such as the confidentiality, availability and integrity value of an asset and the business impact in the event that the asset's security properties are comprised. The risk assessment results, risk treatment options and risk acceptance shall be communicated to the management to obtain approvals and decisions on the next course of action.

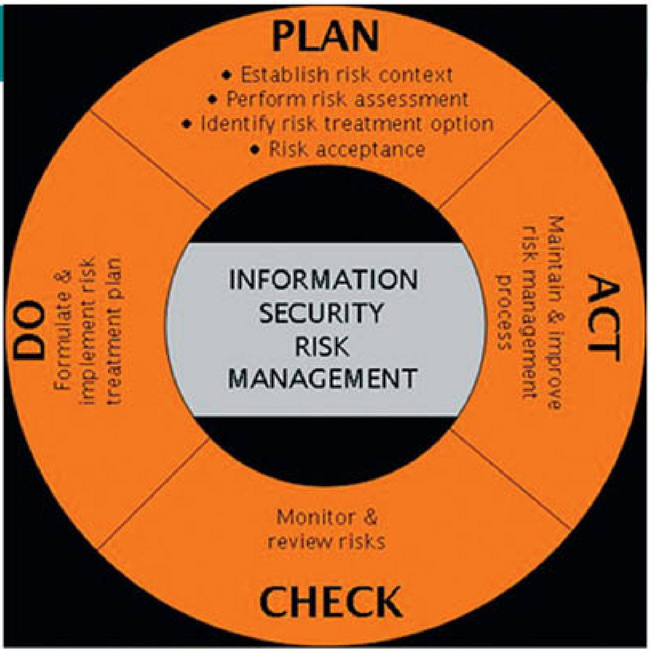

PLAN
• Establish risk context
• Perform risk assessment
• Identify risk treatment option
• Risk acceptance
DO
Formulate & implement risk treatment plan
INFORMATION SECURITY RISK MANAGEMENT
ACT
Maintain & improve risk management process
Monitor & review risks
CHECK

Figure 2: Information Security Risk Management Process

In the DO phase, the risk treatment plan shall be finalised and implemented. It is crucial to list the activities and identify ownerships to ensure successful implementation of the controls. In the last two phases of CHECK and ACT, continual monitoring and reviewing of the risks earlier identified is important to ensure that the risk profile remains adequate and relevant. This would include improving the risk management process, and the activities involved would be similar to those carried out in the PLAN and DO phases.

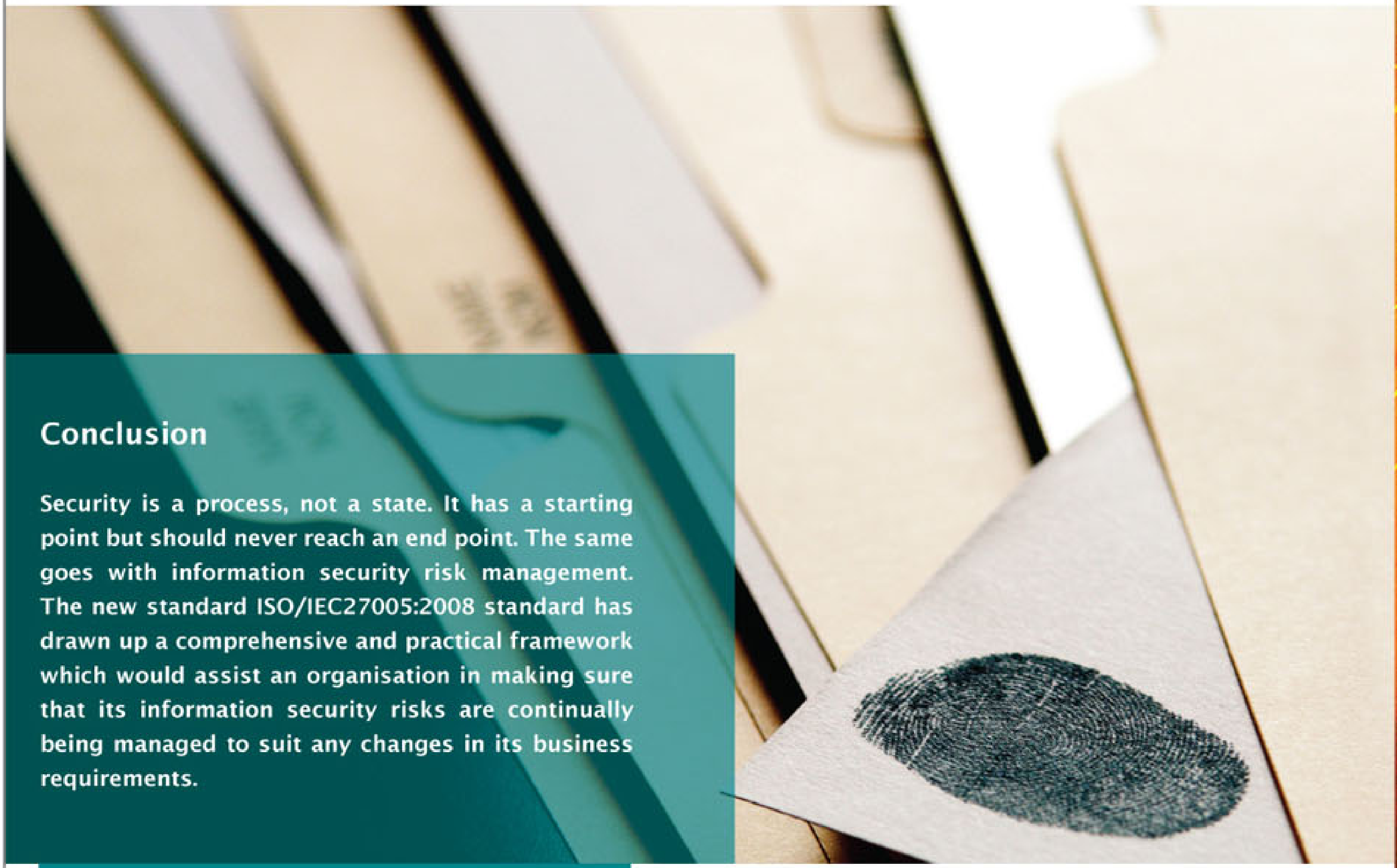
Table 1 and Table 2 are mappings of the relevant clauses between the two standards. This is an attempt to align the requirements and their respective guidance as a quick reference for users to understand both documents.

ISO/IEC 27001:2005 Requirements	ISO/IEC 27005:2008 Process Guidance	
Clause 4.2.1 b) Define an ISMS policy... **Clause 4.2.1** c) Define the risk assessment approach of the organisation	Clause 7.1 General considerations Clause 7.2 Basic criteria Clause 7.3 The scope and boundaries Clause 7.4 Organisation for information security risk management	Clause 11 Information security risk communication
Clause 4.2.1 d) Identify the risks Clause 4.2.1 e) Analyse and evaluate the risks	Clause 8.1 General description of information security risk assessment Clause 8.2 Risk analysis Clause 8.3 Risk evaluation	
Clause 4.2.1 f) Identify and evaluate options for the treatment of risks	Clause 9.1 General description of risk treatment Clause 9.2 Risk reduction Clause 9.3 Risk retention Clause 9.4 Risk avoidance Clause 9.5 Risk transfer	
Clause 4.2.1 g) Select control objectives and controls for the treatment of risks	Clause 9.2 Risk reduction	
Clause 4.2.1 h) Obtain management approval of the proposed residual risks	Clause 10 Information security risk acceptance	

Table 1: ISMS Plan Phase

ISO/IEC 27001:2005 Requirements	ISO/IEC 27005:2008 Process Guidance	
Clause 4.2.2 Implement and operate the ISMS a) Formulate risk treatment plan b) Implement risk treatment plan	Clause 9.1 General description of risk treatment	Clause 11 Information security risk communication
Clause 4.2.3 Monitor and review the ISMS d) Review risk assessments at planned intervals and review the residual risks and identify acceptable level of risks... **Clause 4.2.4 Maintain and improve the ISMS**	Clause 12.1 Monitoring and review of risk factors Clause 12.2 Risk management monitoring, reviewing and improving	

Table 2: ISMS DO, CHECK & ACT Phases



Conclusion

Security is a process, not a state. It has a starting point but should never reach an end point. The same goes with information security risk management. The new standard ISO/IEC27005:2008 standard has drawn up a comprehensive and practical framework which would assist an organisation in making sure that its information security risks are continually being managed to suit any changes in its business requirements.

References

ISO/IEC 27001:2005
ISO/IEC 27005:2008
Implementing the ISO/IEC 27001 Information Security Management Standard (by Edward Humphreys)

The Reality of Cyber-Threats Today

War, crime and terrorism are traditional concepts that occur in the physical domain. The only difference between those concepts and cyberwar, cybercrime and cyber-terrorism is the "cyber" prefix. Cyberwar refers to warfare in cyberspace and includes cyberattacks against a nation state and critical communication network. Cyber-terrorism refers to the use of cyberspace to commit terrorism. It is generally understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives. Cybercrime or crime in cyber-space has been much experienced by many parties where the motive is more of computer-related crimes and monetary gain is the focus.

What is a threat?

From the information security perspective, a threat is defined as the potential to cause an unwanted incident in which an asset, system or organisation may be harmed. There are three sources of threats: Intentional, accidental and environmental. Some examples of intentional threats are those that use malicious software or illegal software. Accidental threats can be seen as service failure, human design error or hardware failure. Meanwhile, examples of environmental threats are earthquakes, thunderstorms or lightning. All these threats cannot be totally eliminated, but can be reduced through the establishment of effective measures to curb such threats within each organisation. Threats however, if not properly controlled, can create an unwanted impact on security, socio-economy and human lives.

Cheap Method

The dimension of warfare can be categorised as conventional, space and cyber- warfare. Conventional warfare and space warfare are expensive whereas cyber warfare is cheap. It is also accessible to many groups and individuals. Cyber warfare enables asymmetric warfare, where individuals have the abilities and capabilities to cause damage to a nation state. Access to a personal computer with an Internet connection can create as much damage as traditional weapons. It is attractive to many because it is cheap in relation to the cost of developing, maintaining and using advanced military capabilities.

The sophistication of an attacker's tools and techniques is becoming more powerful and requires less technical knowledge nowadays. Furthermore, all of these tools are available on the Internet, which is more user-friendly, at a very minimal cost and in many instances, are free of charge.

There are known threats which have limited capabilities and marginal opportunities with high risks of being detected. There are also emerging threats which have many capabilities and broad opportunities and provide low risks of detection. These are the dilemmas that we face today.

Case Studies

Below are several case studies of cyber-threats reported outside Malaysia:

→ Cyberattacks experienced by the Japanese government

It was reported that the Japanese government's computers were under attack on 4 Aug 2004. Eight Japanese government agencies' computer networks were disrupted almost simultaneously, similar to what is known as barrage jamming in telecommunication terms.

Those networks experienced denial-of-service attacks whereby the affected networks were not accessible for a few hours.

→ Hackers clogging up the US customs' computers for hours

The case was reported in August 2005 where viruses attacked the US Customs and Border Protection system for several hours. Several thousands of people were affected.

The viruses left a grave impact on the computers at airports in Miami, New York, San Francisco, Los Angeles, Houston and Dallas.

→ Cyberattacks on Estonia

In May 2007, Estonia was under cyberattack for three weeks. The attacks paralysed Internet communications targeting the government, banking, media and police websites.

Huge economic losses were incurred as online transactions were disrupted.

→ Cyber-warfare between Russia and Georgia

Russia's invasion of Georgia in August had moved into cyberspace as the Russians managed to siege and gain direct routing intended for Georgia.

It was reported that the Russians intercepted the network traffic to Georgia and redirected the route to their servers. Many of Georgia's Internet servers were under their command and control.

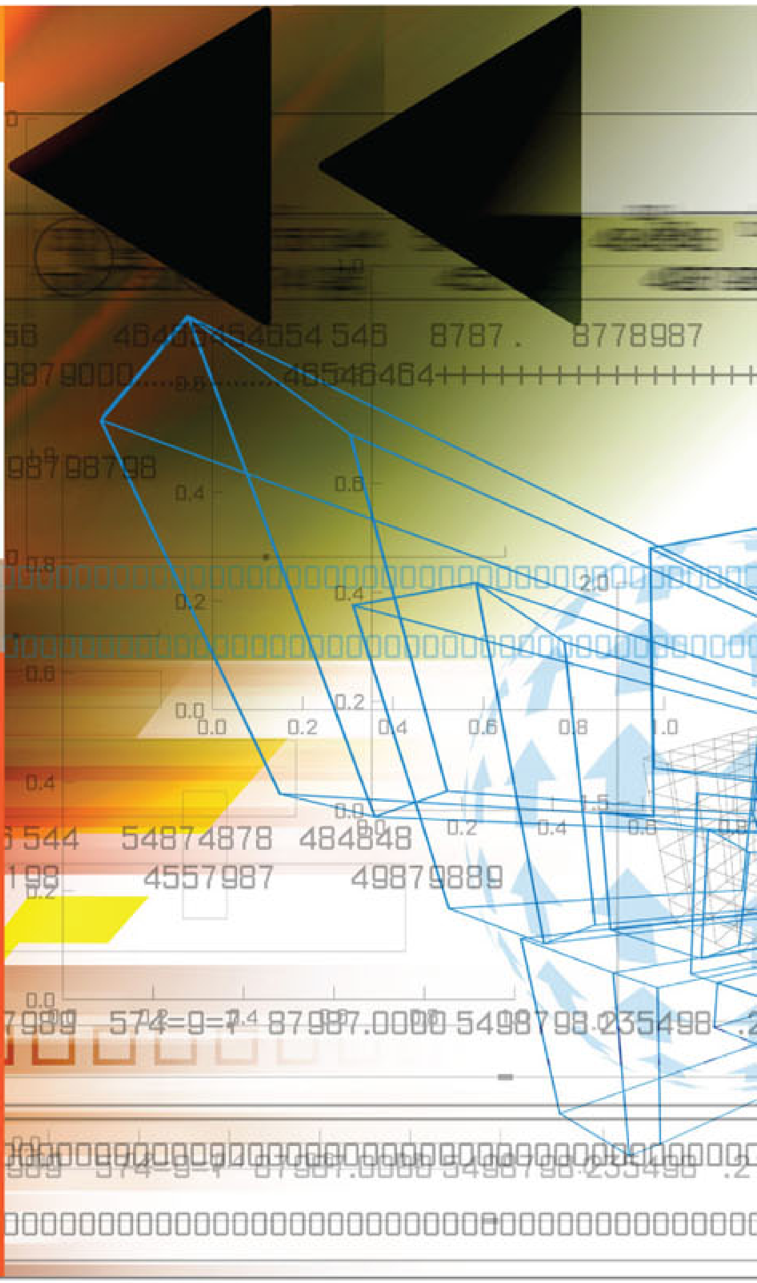
Local attack

In 2001, Malaysia's Internet infrastructure was attacked by the Code Red worm. This was a classic example of infrastructure attack in which the worm spread very fast and brought our national communication network to a standstill. It was reported that the relevant agencies took three months to eradicate this worm and the estimated minimum losses was RM22mil, not inclusive of the losses to the business fraternity and other sectors as well.

Other incidents of cyberattacks were caused by the Blaster and Naachi worms in 2003. The incident started with the propagation of the Blaster worm through the scanning of vulnerable machines via the network, followed by Naachi worms. These worms exploited the vulnerability found in the Windows NT, 2000 and XP software. The estimated cost to eradicate this worm was about RM31mil, not including lost productivity and the cost of lost opportunity.

Modern warfare

Today, cyberspace is the new war frontier whenever there are conflicts between countries. The popular method of a cyberattack is the defacement of websites. Web defacement is a malicious activity whereby a website is "vandalised". Often the hacker replaces the site's content with a specific political or social message. The hacker may even erase all the contents from the site by relying on known security vulnerabilities to access the site's content. The US-China conflict in May 2001, which resulted from an incident where a Chinese fighter was lost at sea after colliding with a US naval reconnaissance plane, is a good example to illustrate this scenario.



End word

In conclusion, cyber-threats are the problems of today and the future. They need to be addressed in a comprehensive manner. In dealing with cyber threats, a country cannot stand alone. There is a need to have strategic alliances to deal with threats and vulnerabilities in the cyberworld. Coordination and collaboration from all parties is important in order to enhance the security of Malaysia's cyberspace.

Training Calendar 2009

CyberSecurity MALAYSIA

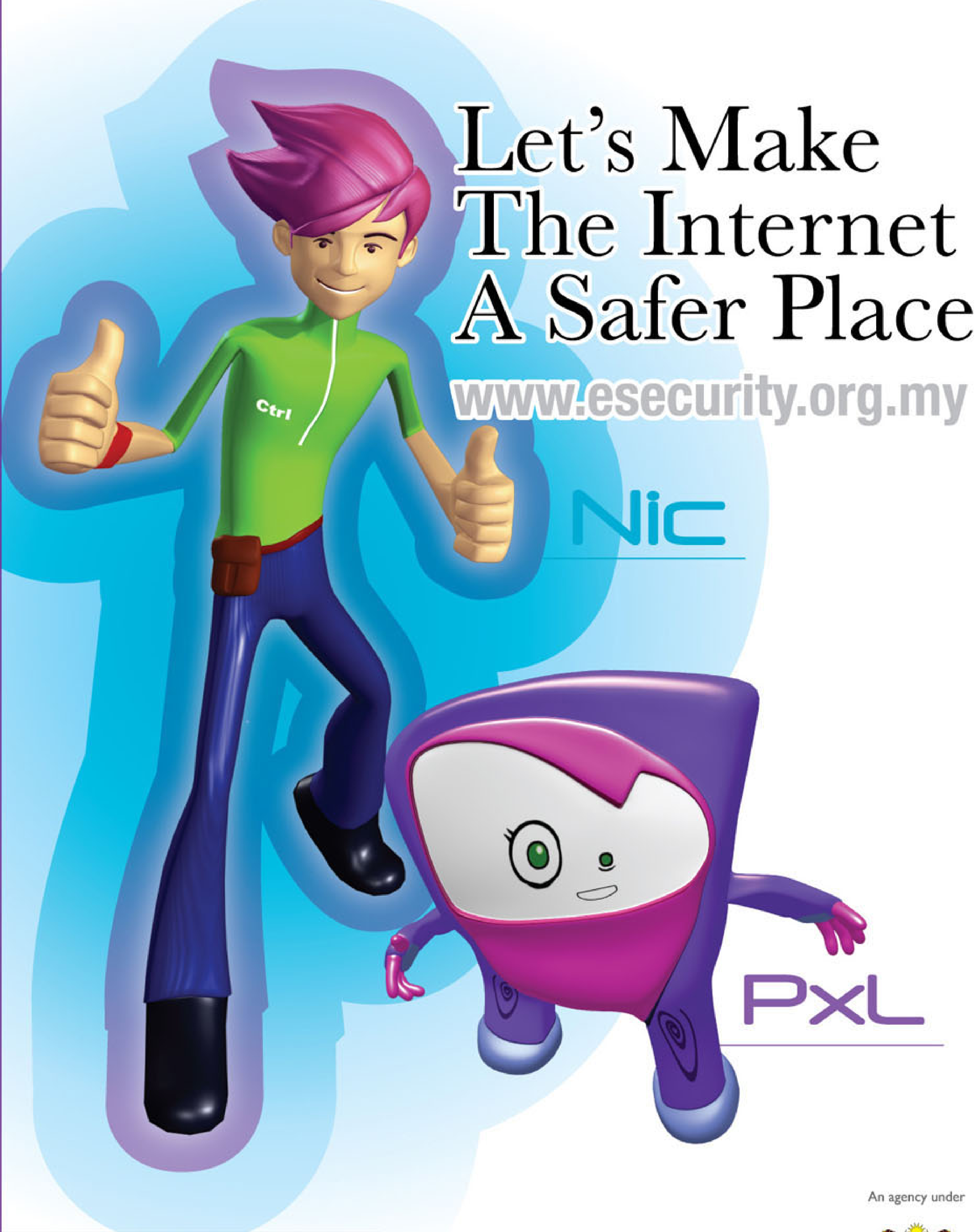
Item	Course Title	Duration (days)	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec
1	CISSP CBK Review Seminar	5				6-10				3-7				
2	SSCP CBK Review Seminar	3				13-15				10-12				
3	CISSP Exam	1		21			16							
4	SSCP Exam	1		21			16				12			5
5	Security Policy Development raining	2			23- 24				13-14		12			5
6	Security Essentials	2			11-12				6-7				23-24	
7	Incident Response & Handling Training	3			16-18								23-25	
8	ISO 27001/Lead Auditor Training	5				20-24				17-21				
9	Wireless Communication Training	3			24-26		5-7					13-15		
10	Wireless Security Training	2							27-28					2-3
11	Mobile Banking Training	2		24-25			13-14					19-20		

Training and Outreach Department
Level 4, Block C, Mines Waterfront Business Park,
No.3, Jalan Tasik,Mines Resort City,
43300 Seri Kembangan
Selangor Darul Ehsan
Email: *training@cybersecurity.my*
Website: *www.cybersecurity.my*

Phone Enquiries: Daisy - 603-8946 0813
Madihah - 603-8946 0849
Azriq - 603-8946 0846
General line: 03-8946 0999
Fax: 03-8946 0844

Let's Make The Internet A Safer Place

www.esecurity.org.my



An agency under

MOSTI

CyberSecurity Malaysia
Level 7, Sapura@MINES, No.7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor Darul Ehsan.
Tel: 03-89926888 Fax: 03-89453205

www.cybersecurity.my

CyberSecurity MALAYSIA