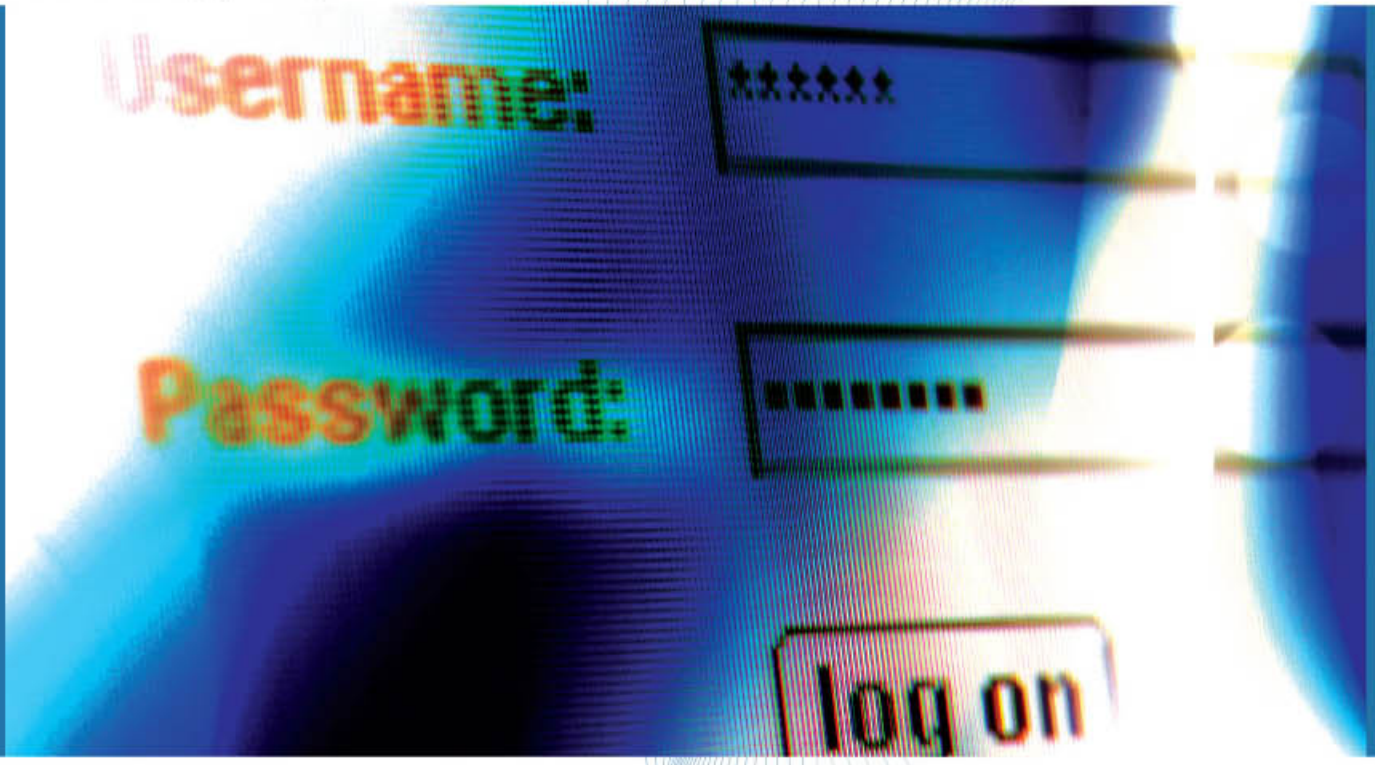
CyberSecurity MALAYSIA

e-Security

MOSTI

Volume 15 - (Q2/2008)



" Treat your password like your toothbrush.
Don't let anybody else use it, and get a new one every six months."

Clifford Stoll

Contributors

ISSN 1985-1995

9 771985 199003

KDN License number: PP 15526/10/2008(007180)

From the Editor's Desk

vphilip@cybersecurity.my

It's Quarter 2 of 2008. An extremely hectic quarter for us here at CyberSecurity Malaysia as all hands were on deck for the recently concluded INFOSEC.my events in conjunction with the World Congress on Information Technology (WCIT) 2008.

Well, if you missed that, you missed a lot. CyberSecurity Malaysia organised 3 events in conjunction with WCIT 2008. We had INFOSEC.my Awareness session for schools, INFOSEC.my Conference for information security professionals and practitioners, and INFOSEC.my CEO Breakfast Session.

It was an extremely successful event as the awareness session saw a total of 450 students and teachers attending with talks on internet safety and positive use of the internet. The conference was attended by about 330 participants. The highlight was a special session by Prof. Howard Schmidt and the cryptology guru, Bruce Schneier. It was a truly interactive session with participants making full use of the session with lots of questions to these two experts.

Finally it was the CEO Breakfast session with a panel of experts from local and international lead by Prof. Howard Schmidt. This session was officiated by the Deputy Minister of MOSTI and was attended by 60 participants.

So, having said that, what's in our newsletter this time around? More great articles of course! Once again, we start with the MyCERT quarterly summary report. In a nutshell there has been an increase in incidents reported to us in quarter 2, mainly contributed by spam incidents. Other interesting articles include areas on forensics, cryptology, business continuity management, spam on facebook, 2-factor authentication and an overview of our National Cyber Security Policy.

Also, CyberSecurity Malaysia will be introducing a new Professional Certification soon with our collaboration with Business Continuity Institute (BCI) UK. With this collaboration, we will be the official authorised provider here in Malaysia. We will also be the official authorised exam centre for BCI and SANS Institute by August 2008.

We will also be announcing soon the Information Security Leadership Awards (ISLA) from (ISC)2 which is open for nominations.

So, check out our website **http://www.cybersecurity.my** regularly for updates. Feedback is welcomed and all you security professionals and practitioners out there, if you have a good article that you would like to contribute, please do email us. Till then, be safe and be smart. Also, check out our awareness portal **www.esecurity.org.my** for new stuff.

Philip

Philip Victor
Editor

A Message From the Head of CyberSecurity Malaysia

Greetings to all our readers. It is my pleasure to once again address the community of security professionals and practitioners both local and internationally.

As we have just completed the second quarter of 2008, many events and achievements have been accomplished. For a start, a very successful and knowledge filled INFSOEC.my event held recently in conjunction with WCIT 2008.

My appreciation to the Minister and Deputy Minister of MOSTI for their support for the INFOSEC.my event in making it a truly successful international event that brought the best from the world of information security.

In this quarter, we also see an increase in incidents being reported to us. I would like to highlight especially on the high increase in fraud & intrusion incidents especially. The major contributor to fraud is phishing cases. We would like to advice users out there to be extra careful and not to respond to emails asking you to update your banking details or revealing your passwords. Always check with the bank if you are not sure.

Another high increase is incidents related to intrusions. Our reports show that majority of these cases are related to web site defacements in particular .my websites. As most of these incidents are caused by web application vulnerability, we would like to advice organisations to keep their web sites updated and patched and refer to MyCERT's advisory on our website on prevention and corrective methods.

Our cyber space are facing more complex and challenging attacks and this will need us to take extra measures to prevent and mitigate these attacks. More security professionals need to be developed to increase our nation's pool of experts to better protect our cyber space.

Once again, a big thanks to all our contributors. Let us all help to make the internet a safer place and continue to educate and build a culture of security especially among the younger generation to inculcate this culture. Thank you.

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

Table of Contents

READER ENQUIRY
Training & Outreach
CyberSecurity Malaysia
Ministry of Science, Technology and Innovation (MOSTI)
Email: training@cybersecurity.org.my

PUBLISHED BY
CyberSecurity Malaysia (726630-U)
Level 7, Sapura@Mines
7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

PRODUCED BY
Epac Advertising Sdn Bhd (719875-A)
No 8 Ground Floor
Jalan Vivekananda, Brickfields
50470 Kuala Lumpur, 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

MS-134.072008: MyCERT Quarterly Summary (Q2) 2008
Original Issue Date: 16th July 2008

Introduction

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

MyCERT believes these statistics are only a tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order for us to assist those who are affected.

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

Incident Reports

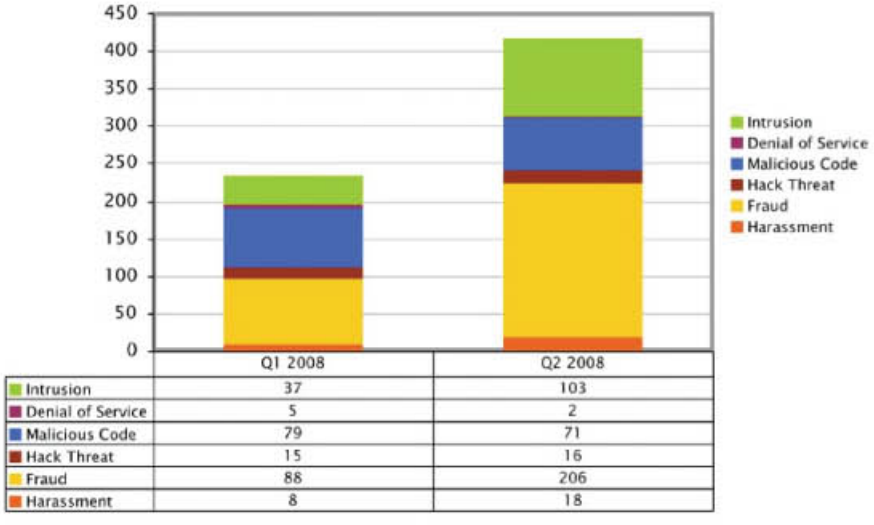
In the second quarter of 2008 (Q2), a total of 16958 incidents, inclusive of spam incidents, were reported to MyCERT representing a 63.88% increase of incidents compared to Q1 in 2008. The majority of the incidents reported this quarter is contributed by spam reports. There were no critical outbreaks in terms of malware or exploitation nor any significant increase in any particular incidents that had raised alerts in our constituency. All categories of incidents classified by MyCERT such as intrusion, hack threat, malicious code, denial of service and spam had an increasing number of incidents. On the other hand, malicious code and denial of service incident had decreased.

Attached is the Table of Figure showing the comparisons between number of reports received in Q1 2008 and Q2 2008.

	Q1 2008	Q2 2008	%
Harassment	8	18	125
Fraud	88	206	134.09
Hack Threat	15	16	6.67
Malicious Code	79	71	-10.13
Denial of Service	5	2	-60
Intrusion	37	103	178.38
Spam	10122	16542	63.43
Total	**10354**	**16958**	**63.88**

Table of Figure for Q1 2008 and Q2 2008

Comparison of Incident Statistics between Q1 2008 and Q2 2008



	Q1 2008	Q2 2008
Intrusion	37	103
Denial of Service	5	2
Malicious Code	79	71
Hack Threat	15	16
Fraud	88	206
Harassment	8	18

Attached is the graph showing number of reports received for types of incidents in Q1 2008 and Q2 2008:

Malicious Codes

Malicious code incidents had decreased slightly in this quarter compared to previous quarter. A total of 71incidents were reported compared to 79 in previous quarter. In this quarter, we received several reports from foreign CERTs and security organizations regarding bot infected machines (drones), control & command (C&C) server of botnets and malicious files hosted on machines in Malaysia. Some of these reports contained IP addresses, most of which are on home users network that had been reported to us previously. In all of the instances, MyCERT had notified and assisted the respective ISPs on bot removal and mitigation strategies. These bots are normally used to carry out malicious activities such as spamming, executing denial of service attacks, hosting phishing sites and spreading malware.

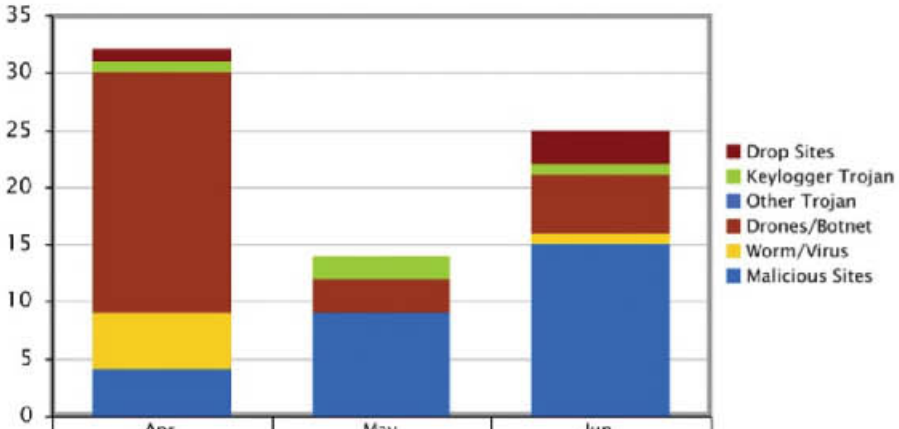
MyCERT had also responded to 29 incidents involving drones and botnet command & control infrastructure operating in Malaysia. Machines infected with bots were successfully notified and rectified accordingly.

Other incidents that we received include the discovery of 3 drop sites or servers storing credentials such as usernames and passwords, hosted in our constituency. These credentials were stolen mostly from machines/PCs infected with malicious codes. MyCERT had notified respective parties and the drop sites were managed to shutdown.

MyCERT received 4 reports received from a foreign CERT regarding some details found on a server which was used by a trojan to log keystrokes. The keylogger Trojan, named the Nethell Trojan, had successfully captured keystrokes of usernames/passwords belonging to various internet accounts in our constituency, which includes banks, ISPs and government agencies. MyCERT had notified the respective parties for immediate rectifications on the compromised passwords.

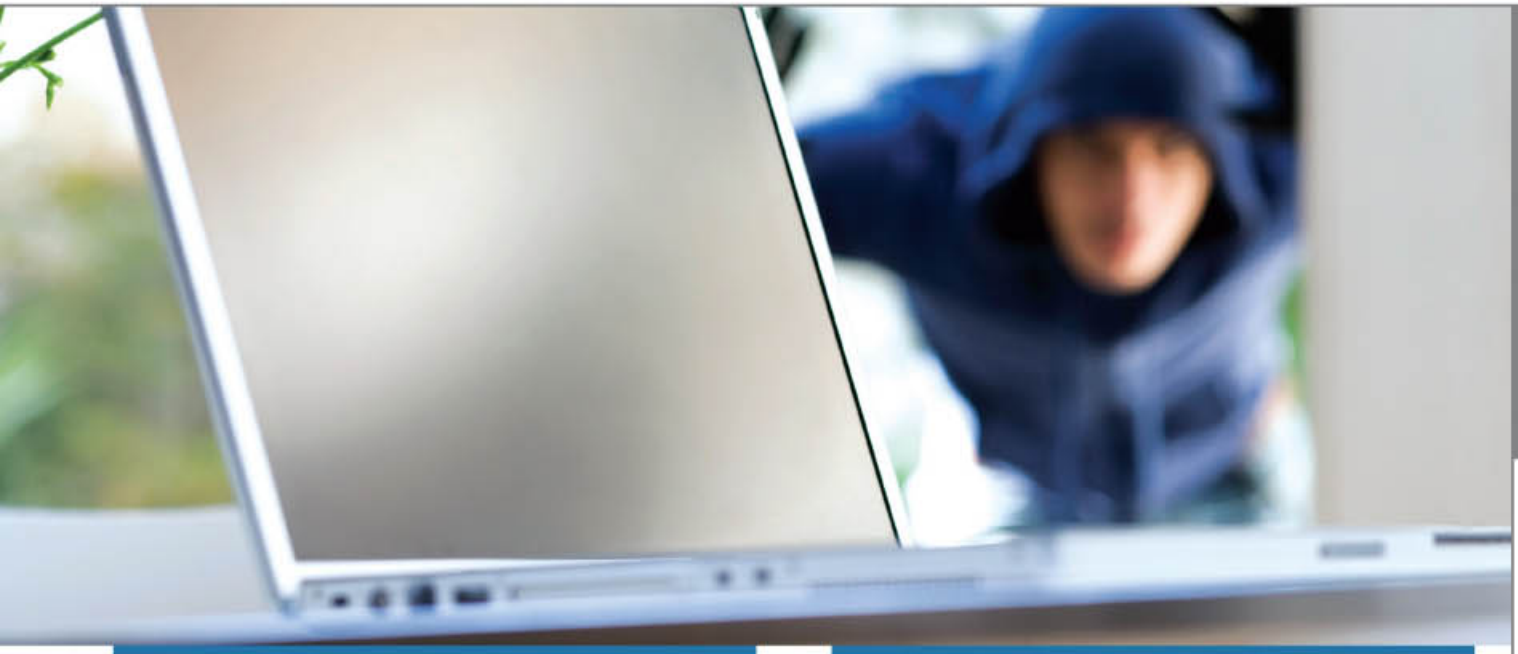
The following graph shows breakdowns of malware incidents received in this quarter:

Breakdown of Types of Malware Incident in Q2 2008



	Apr	May	Jun
Drop Sites	1	0	3
Keylogger Trojan	1	2	1
Other Trojan	0	0	0
Drones/Botnet	21	3	5
Worm/Virus	5	0	1
Malicious Sites	4	9	15

We advise users to safe-guard their computers against malware infection. Please visit the following URL: **http://www.esecurity.org.my/adult-malware.htm** to view some tips on this topic.



Hack Threat

MyCERT received 16 reports for the category of hack threats, 1 report more than in previous quarter. Most of the hack threat reports were received from foreign security organizations where the sources of the attack are from Malaysian IP addresses. Some of the common attacks observed are ssh brute-force attacks, port scanning and other malicious or suspicious activities that had triggered alerts.

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

Denial of Service

In this quarter, reports on denial of service had decreased to about 3% compared to previous quarter. The number had decreased from 5 incidents in previous quarter to 2 incidents in this quarter. The denial of service attack consists of sending huge traffics, continuously to a system, causing the system to slowdown or choked. In distributed denial of service attacks, the source of the attacks mostly come from various spoofed multiple IPs and majority of denial of service attacks originate from 1 single IP address. Majority of denial of service attacks were successfully handled or stopped by blocking the source of the attacks at customers' upstream router.

Intrusion

MyCERT received 103 reports related to intrusion in this quarter. The majority of the incidents in this category were web defacements (or re-defacements in some incidents) of .my websites hosted in Malaysia.

In this quarter a total of 97 .my sites belonging to various sectors and running on various platforms were defaced. Most of these defacements were caused by web application vulnerabilities such as remote file inclusion, sql injection and unpatched third party add-ons.

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

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

In this quarter, we also received report on a large number of websites around the globe being targeted by a mass SQL injection attack.

This attack causes the contents of the websites to be modified with codes that will redirect users to another server which contain malicious codes and exploits. The malicious codes or exploit will then allow the attacker to gain control of the victim's computer.

Based on our assessment, we have only detected very few Malaysian sites that have been affected by this mass SQL injection attack. However, MyCERT encourages administrators to be vigilant and alert of this attack or attempts of exploitation.

Most of the servers hosting the malicious scripts and exploits are using the .CN domain and located in various countries.

MyCERT had released an advisory on the attack available at:

Mass SQL Injection Attack

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/577/index.html

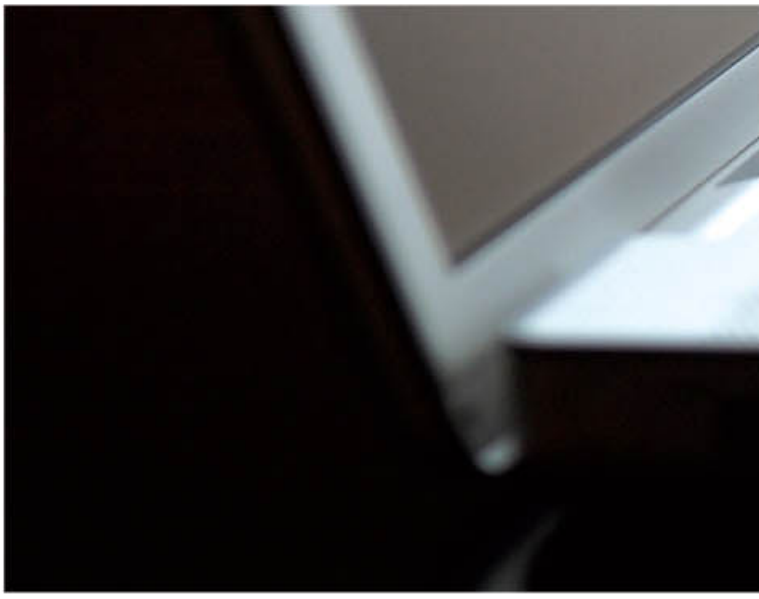
Harassment

MyCERT had responded to 18 incidents under the category of harassment compared to 8 incidents in the previous quarter. The harassment cases include email threats to defamatory messages/pictures/photos on internet forums and social networking websites. Majority of harassment cases were handled successfully in which the defamatory messages/pictures/photos were able to be removed from the respective forums/sites. And source of email threats were able to be traced and handed to the respective Law Enforcement Agency.

Users who are harassed via Internet or who observed any kind of harassments on web forums, which has religious, social, political or economic implications are advised to report to MyCERT for further analysis, besides reporting to the police. Users are also advised not to reveal or upload their personal information such as their contact numbers, home address, photos on the net or transmit to untrusted parties as this information could be abused by irresponsible parties.

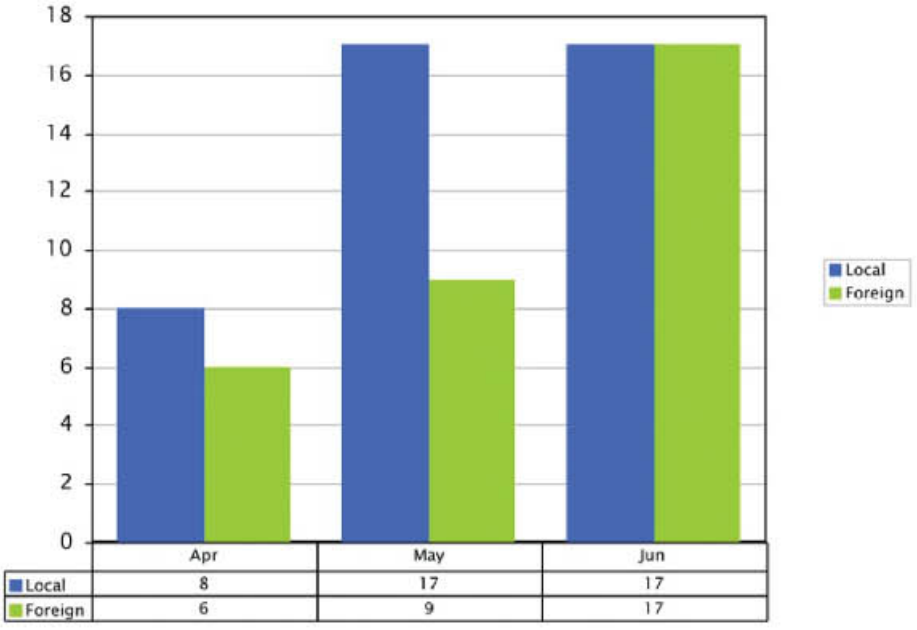
Fraud

This quarter saw a tremendous increase in fraud incidents to about more than 100%, which comprised of 206 reports compared to 88 reports in previous quarter. Majority of fraud incidents reported were phishing incidents -involving local and foreign financial institutions or brands. We observed a surge on phishing reports with 52 reports received on phishings in this quarter. This includes reports on phishing emails and phishing sites impersonating local/foreign financial institutions or brands. MyCERT had handled the phishing reports by communicating with respective parties and the phishing sites were abled to shutdown within 24 hours and less.

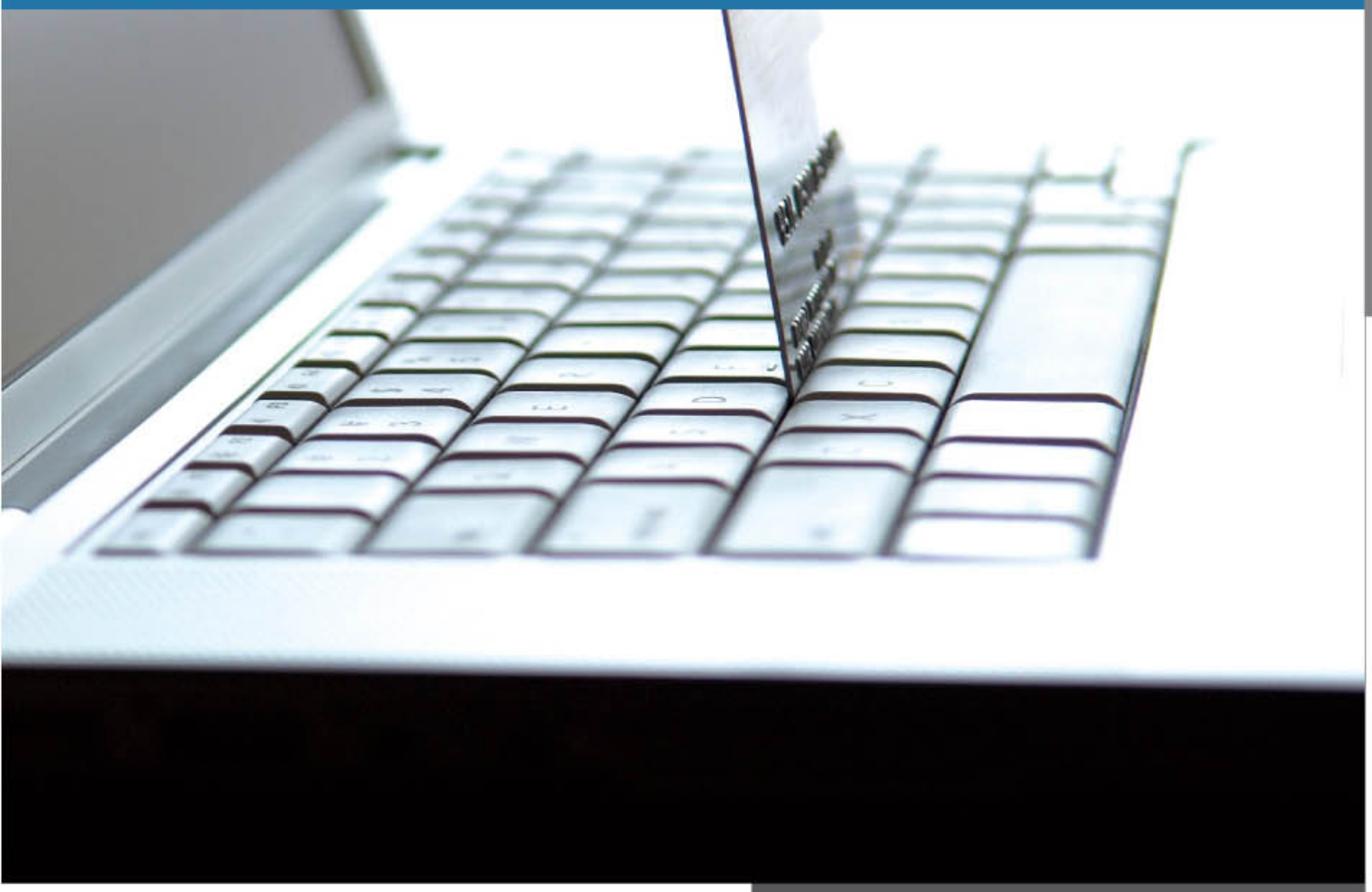


The breakdown of phishing sites between local and foreign brands is shown below:

Breakdown of Phishing Sites Between Local and Foreign Brands



	Apr	May	Jun
Local	8	17	17
Foreign	6	9	17



In this quarter we also observed a surge on SMS scam cases due to the recent wide coverage by the local media that had raised awareness among the public on reporting SMS scams as well as reporting other types of scams. In the month of June, we received 19 reports of SMS scams from the public. MyCERT had responded to the reports by escalating to the Law Enforcement Agency and providing advises on scam preventions for the public.

Other types of fraud incidents reported to us besides the SMS scam reports are suspicious online investments, ponzi or pyramid schemes, Nigerian scams, Lottery scams, cheatings and misuse of organization's Intellectual Property such as logo, url, domain name for promoting illegal activities on the net.

With the increase of scam activities on the net, MyCERT had released a guideline on scam preventions which is available at:

Tips and Guidelines on Scam Preventions

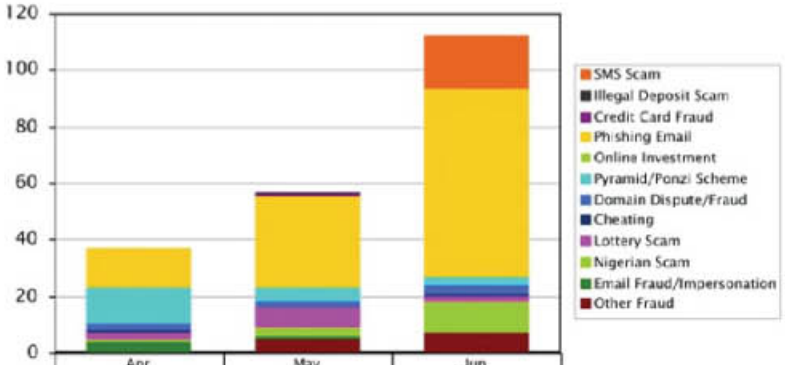
http://www.mycert.org.my/en/resources/fraud/main/main/detail/588/index.html

In this quarter we also observed a surge on SMS scam cases due to the recent wide coverage by the local media that had raised awareness among the public on reporting SMS scams as well as reporting other types of scams.

In this quarter, MyCERT had handled 7 incidents involving domain names disputes which were mostly set up for suspicious activities. MyCERT had advised the affected organizations to obtain Legal advises from their Legal Department by referring to the relevant domain dispute resolution policies before taking any action.

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

Breakdown on Types of Fraud Incidents in Q2 2008



	Apr	May	Jun
SMS Scam	0	0	19
Illegal Deposit Scam	0	1	0
Credit Card Fraud	0	1	0
Phishing Email	14	32	66
Online Investment	0	0	0
Pyramid/Ponzi Scheme	13	5	3
Domain Dispute/Fraud	2	2	3
Cheating	1	0	1
Lottery Scam	2	7	2
Nigerian Scam	1	3	11
Email Fraud/Impersonation	4	1	0
Other Fraud	0	5	7

Vulnerabilities Reported

In this quarter MyCERT also received 58 reports from various sources regarding web application vulnerabilities found on Malaysian websites. The vulnerabilities include sql injection, directory listing and weak administrator's passwords. MyCERT had verified the reported vulnerabilities at the said websites and inform the respective system administrator to fix the vulnerabilities before any unwanted incidents occur.

Some of the steps that Administrators can implement are:
To prevent against sql injection attacks.

http://www.mycert.org.my/en/resources/web_security/main/main/detail/572/index.html

For choosing strong passwords, Administrators may refer to the below guidelines:

http://www.us-cert.gov/cas/tips/ST04-002.html

http://www.microsoft.com/protect/yourself/password/create.mspx

To fix directory browsing, Administrators may refer to the below guides:

For sites running on Apache web servers

By removing Indexes directive in Apache configuration (httpd.conf) can disable directory browsing. If needed, it can be secured by using htaccess file. Search the line where Indexes is located and then remove the Indexes.

For sites running on IIS web servers

By deselect Directory Browsing if it is selected at the Web directory.

Sample of the properties can be found here:

http://microsoft.apress.com/images/articles/articles_20011130_1.gif

Spam Incidents

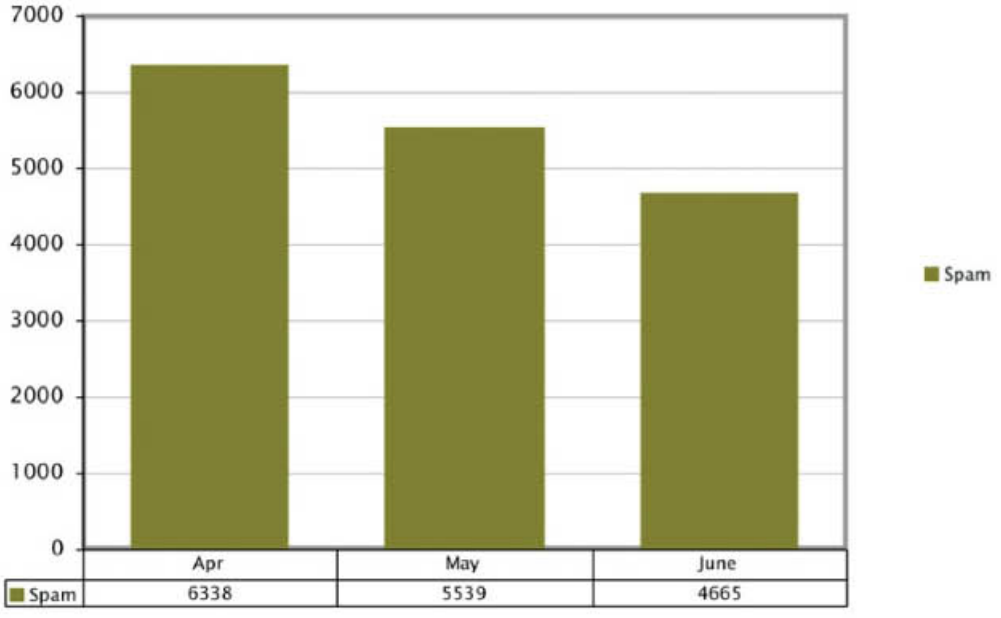
MyCERT had observed that spam related incidents had increased to 63.43% in this quarter compared to the previous quarter. A total of 16542 reports were received compared to 10760 reports in previous quarter. Spam incidents remains as the incident with highest number of reports received compared to other incidents. Based on our observation of the monthly spam statistics, we noticed spam emails were recorded higher with the outbreak of a certain security threat. Based on our observation, majority of spam emails are related to scam emails such as the Nigerian scam, Lotterry scam, get rich schemes, Trojan Dropper, Virus and Phishing.

Promoting and selling of products/services still remain as one of the main contributor to spam.

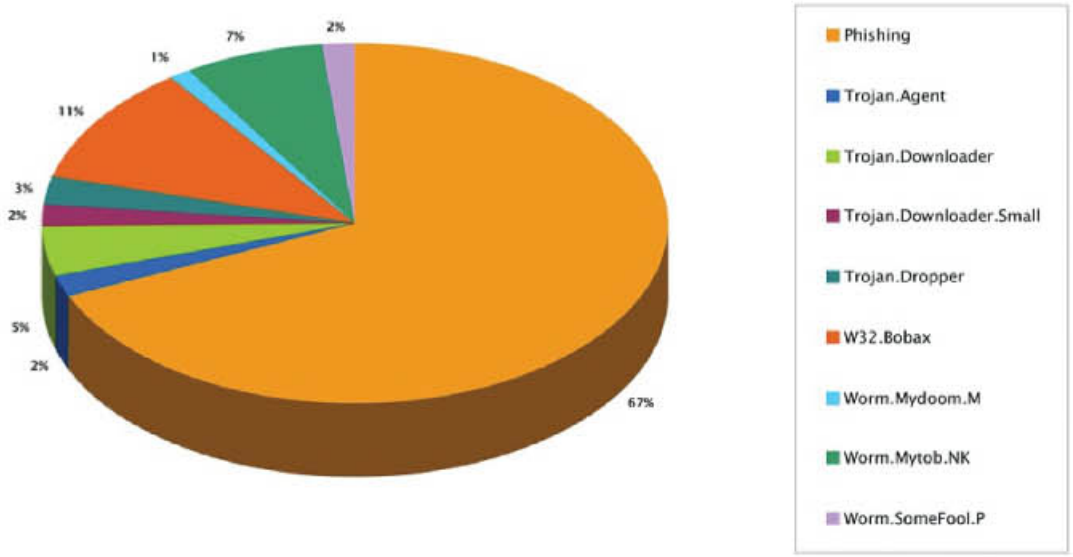
There are no perfect techniques or tools to completely eradicate spams, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users email clients. Users are also advised not to respond nor purchase products promoted via spams.

Attached graph on number of spams recorded by months in this quarter and spam payload detected by ClamAV.

Statistics on Spam Incident in Q2 2008



Spam Payload Detected by ClamAV in Q2 2008



Alerts & Advisories

In this quarter, MyCERT had released 6 alerts related to critical vulnerabilities and mass SQL injection attacks. The advisory and alerts are available at:

MyCERT Special Alert -
Vulnerabilities in Microsoft Products (16 June 2008)

http://www.mycert.org.my/en/resources/web_security/main/main/detail/572/index.html

MyCERT Special Alert -
Vulnerabilities in Adobe Flash Player (30 May 2008)

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/581/index.html

MyCERT Special Alert -
Fraudulent Domain (28 May 2008)

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/580/index.html

MyCERT Special Alert -
Mass SQL Injections Attack (16 May 2008)

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/577/index.html

MyCERT Special Alert -
Vulnerabilities in Microsoft Products

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/578/index.html

MyCERT Special Alert -
Malicious April Fool Emails (3rd April 208)

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/569/index.html

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

Microsoft Security Advisory (954960)
(30 June 2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/589/index.html

Microsoft Security Bulletin Summary for June 2008
(10 June 2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/589/index.html

Apple Quicktime Updates for Multiple Vulnerabilities (10 June 2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/584/index.html

SNMPv3 Authentication Bypass Vulnerability (10 June 2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/585/index.html

Microsoft Updates for Multiple Vulnerabilities (10 June 2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/583/index.html

US-CERT: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability (16/05/2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/582/index.html

US-CERT: Microsoft Updates for Multiple Vulnerabilities (13/05/2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/576/index.html

US-CERT: Apple QuickTime Updates for Multiple Vulnerabilities (03/04/2008)

http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/575/index.html

Activities from Research Network

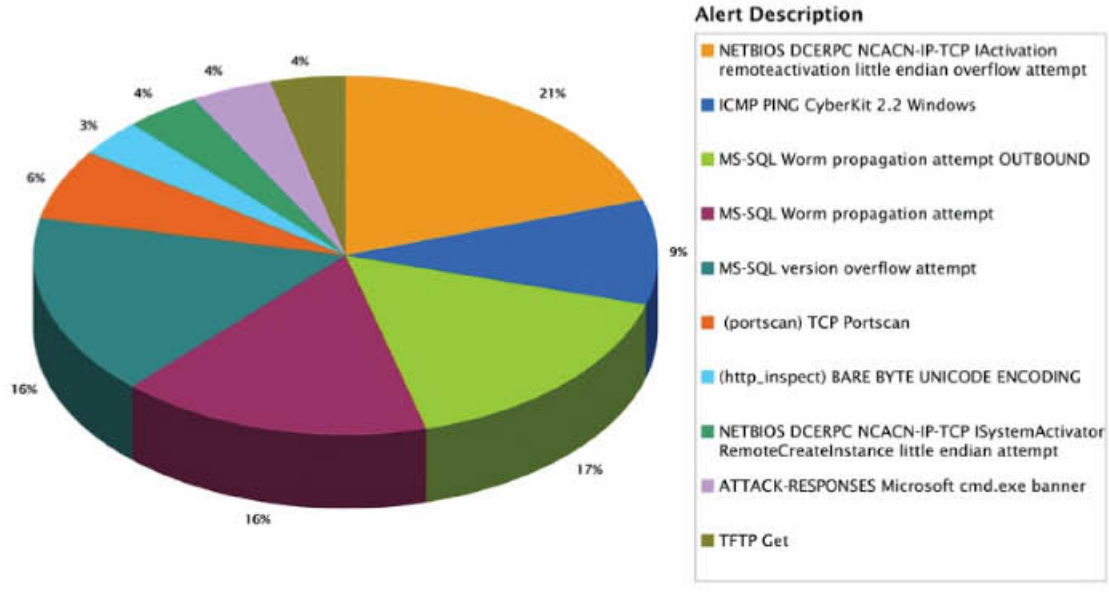
The CyberSecurity Research Network monitoring objectives are:

- To monitor the network for suspicious traffic as well as to monitor for the occurrence of known malicious attacks.
- To observe attacker behaviour in order to learn new techniques being deployed, to determine the popular techniques that are currently being used as well as to confirm the continued use of old and well known attack techniques.
- To compile and analyse 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.

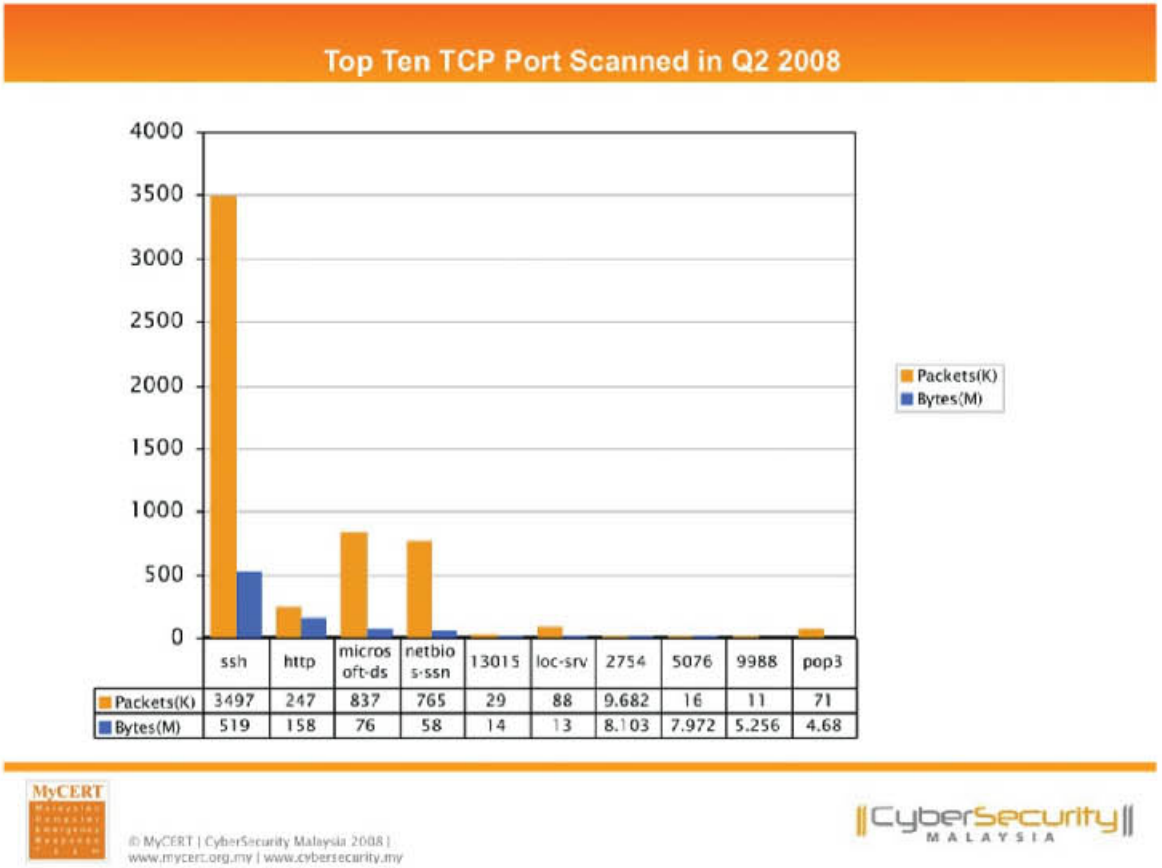
The following is a summary derived from MyCERT's research network for Quarter 2 2008.

Top Ten Alerts Generated by Our Sensor

Top Ten Alert Generate by our Sensor in Q2 2008



Top Ten TCP Ports



Conclusion

Overall, the number of incidents reported to MyCERT had increased to 63.88% compared to previous quarter with incidents mainly contributed from spam incidents. Other reports that contributed highly to the number of incidents received are fraud incidents, malicious codes which consist of reports of botnets, command and control & command server, drone activities hosted on local machines and intrusions. MyCERT would like to advise system and security administrators to take precautions on these activities and prevent their machines to become targets. Neither crisis nor outbreak was observed in this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. MyCERT strongly advise users/organizations to report and seek assistance from us in the event of any security incidents.

MyCERT can be reached for assistance at:

Tel : 03-89926969
Fax : 03-89960827
Email : mycert@mycert.org.my
Web : http://www.mycert.org.my/report_incidents/online_form.html
HP : 019-2665850
SMS : 019-2813801

Feedbacks can be directed to MyCERT.

Produced in 16 July 2008 by MyCERT, CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI).

Revision History :
Initial Release : 16 July 2008

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

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

THE NEW FRONTIER FOR

(This article was published in the STAR In-Tech on 1 Jul 2008)

Introduction

CYBERSPACE is a virtual place that has become as important as physical space for social, economic and political activities. Many nations in the world are increasing their dependency on cyberspace when they use information and communications technology (ICT).

This dependency places countries in a precarious position because cyberspace is borderless and vulnerable to cyber attacks. Individuals have the ability and capability to cause damage to a nation from afar, through cyberspace.

Merely accessing a single personal computer through an Internet connection could cause as much damage as using a traditional weapon, such as a bomb. Cyber attacks are also attractive because it is a cheap weapon in relation to the costs of developing, maintaining and using advanced military hardware.

What is Cyber Terrorism

The term is becoming increasingly common nowadays, and yet a solid definition of it and what constitutes cyber terrorism are subjective and broad.

At first glance, there is nothing new about this term, except for the "cyber" prefix. War, crime and terrorism are traditional concepts that occur in the physical domain; "cyber" refers to the new domain for warfare.

The most widely cited definition of cyber terrorism is by Professor Dorothy E. Denning, director of the Georgetown Institute for Information Assurance, at the Georgetown University in the United States.

According to her: "Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

"Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples."

"Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not."

The use of a computer and its applications as a weapon to attack "computers, networks and the information stored therein" constitutes cyber terrorism. There are a number of ways that the terrorist can use a computer as a cyber weapon — computer viruses, hacking, malware, and botnets are a few.

The challenge nowadays is that an attacker's tools and techniques are becoming more powerful, while requiring less technical knowledge. Furthermore, most of these tools are available on the Internet and at minimal cost, and in some instances, free of charge.

Impacts of Cyber Terrorism

Cyber terrorism is the use of cyberspace to commit terrorist acts. This includes warfare attacks against a nation's state and forcing critical communications channels and information systems infrastructure and assets to fail or to destroy them. These would be:

1. Crippling the electrical distribution grid by shutting down control systems;

2. Disrupting national telecommunications network services;

3. Sabotaging airport traffic control systems;

4. Attacking oil refineries and gas transmission systems by crippling control systems;

5. Destroying or altering banking information on a massive scale, thereby crippling the financial sector;

6. Remotely altering medical information; and,

7. Gaining access to dam control systems in order to cause massive floods.

Why would a cyber terrorist decide to use ICT rather than resort to the usual methods of assassination, hostage-taking and guerrilla warfare?

By using ICT, a handful of cyber terrorists can cause greater damage to a country than an army of a few thousand.

Countries which are increasingly dependent on ICT, especially those that have many systems connected to the Internet, are vulnerable to these kinds of attacks. The paradox is that the more wired a nation is, the more vulnerable it is to cyber attacks.

In an era where the use of ICT is a necessity, it is regrettably also highly vulnerable to attacks and opens a new dimension of threats.

Examples of Cyber Terrorism

It can be argued that cyber terrorism requires political motives and the use of violence. The objective is to create fear within the target population, and monetary gain is not the focus.

One example is the major power failure in the northeast of the United States and Canada on Nov 14, 2003. A power grid is considered one of the major components in a nation's critical infrastructure. It was reported that hackers were trying to hit the power system — as many as 100 times a day to compromise the security of the grid.

The incident raised the question of whether it was a cyber attack. Many have worried about the security of control systems in the United States, such as Supervisory Control and Data Acquisition (SCADA) systems that are increasingly being placed online and being opened up to remote access — a move that could contribute to more frequent cyber attacks.

The FBI and the US Homeland Security Department said that the outages appeared to be a natural occurrence and not the result of terrorism. However, Al-Qaeda's group claimed responsibility for the power outage, according to a statement carried by an Arabic newspaper. The truth to this is still not known.

On Aug 4, 2004, it was reported that Japanese Government computers were under attack. Eight government agencies' computer networks were disrupted almost simultaneously. Those networks experienced denial-of-service attacks, and the affected networks were not accessible for a few hours. Most recently, in May last year, Estonia came under cyber attack for several weeks in the wake of the removal of a Russian World War II memorial. This was a distributed denial-of-service attack that paralysed the Internet communications systems of the government, banks and news media.

Conclusion

Cyber threats are real and no longer limited to the movies. While development in the areas of ICT allows for enormous gains, it has also created opportunities for those who have devious ambitions to cause harm.

We, as a nation, must be prepared for the worst when protecting our critical national information infrastructure. Co-ordination and collaboration from all parties are essential in order to enhance the security of our country in cyberspace.

Adware Uses Trickery to Catap Most-Reported Threats for May 2008

Bagful of Adware Tricks Snares Users with Virus Protection Offer

MALAYSIA, 3 June 2008 – Fortinet today announced the top 10 most reported high-risk threats for May 2008. The strongest development of the month showed adware Vapsup flooding users with advertisements for rogue virus protection software. Vapsup jumped 42 positions to land on the second spot, just .01 percent behind persistent malware leader, Netsky. From using plug-ins that hi-jack control of users' Web browser navigation to rogue antivirus scanner pop-ups, Vapsup had a bagful of tricks and scare tactics to lure the unsuspecting user into clicking affiliate links. The incentive for all this trickery was the per-click payouts through affiliate marketing programs linking back to servers located mostly in Russia and the U.S.

"Judging by the high level of activity by Vapsup in the past month, the cyber criminals behind this adware should be getting a huge payday," said Derek Manky, security researcher for Fortinet.

Fortinet's FortiGuard Global Security Research Team compiled this report based on intelligence gathered from FortiGate multi-threat security systems in production worldwide.

Additional malware trends observed during this period include the following:

- Online gaming Trojan activity continues in Asia, still concentrated in Taiwan and China;
- An Iframe injection campaign runs strong through Iframe.DN, pointing to Korean servers;
- Parasitic file infector, Virut.A, which made itself known in March remains in the top five for three consecutive months, showing longevity.

Following are the Top Ten individual threats and Top Five threat families in May. Top 100 shifts indicate positional changes compared to April's Top 100 ranking, with "new" representing the malware's debut in the Top 100.

Top Ten Individual Threats

Rank	Threat Name	Threat Type	% of Detections	Top 100 Shift
1	W32/Netsky!similar	Mass mailer	8.18	-
2	Adware/Vapsup	Adware	8.17	+42
3	HTML/Iframe_CID!exploit	Exploit	6.25	-
4	W32/Virut.A	Virus	5.05	+1
5	W32/Pushdo.EV@mm	Trojan	3.49	new
6	W32/OnLineGamesEncPK.fam!tr.pws	Trojan	2.35	-
7	HTML/Iframe.DN!tr.dldr	Trojan	1.99	+7
8	W32/MyTob.BH.fam@mm	Mass mailer	1.99	-
9	W32/OnLineGames.ADRE!tr.pws	Trojan	1.72	new
10	W32/Zafi.E@mm	Mass mailer	1.65	+8

ult onto Fortinet's

Top Five Families

Malware Family	Percentage	Top 10 Shift
Netsky	14.0	-
MyTob	8.0	-
Virut	5.5	+1
Pushdo	3.7	+1
MyDoom	2.5	+1

To read the full May report, please visit:

http://www.fortiguardcenter.com/reports/roundup_may_2008.html

For ongoing threat research, bookmark the FortiGuard Cente

http://www.fortiguardcenter.com

or add it to your RSS feed by going to

http://www.fortinet.com/FortiGuardCenter/rss/index.html.

Live Evidence Acquisition in M

Introduction

How can we acquire live digital evidence? Often employees involved in insider crime or raiding officers may ask of you this question, in relating themselves as the first responder. To preserve live system evidence, a first responder should follow a step-by-step forensically sound guideline so that the integrity of the evidence will be preserved. On top of that, the responder should also acquire the most volatile evidence first as described below:

1. Image volatile data
   - Memory
   - Network configurations
2. Log and "print screen" all windows
3. Log the system info
   - System uptime
   - OS type, version and build
   - Date and time
   - Partition table map
   - User account information
   - Other related information
4. Image the evidence

However, this article will focus primarily on hard disk acquisition. The acquisition will be performed using common crossed CAT5 network cable between Acquisition laptop and Suspect laptop.

Procedure for Windows Live System Acquisition

The following steps will guide the first responder on how to perform live acquisition using Helix 1.7 Knoppix Live CD.

1. Prepare the acquisition setup and format the external hard disk to FAT32 file system, that hard disk will be use for store image of the evidence.
2. Connect the external USB hard disk to the Acquisition laptop.
3. Connect the Acquisition laptop with the Suspect laptop using network crossed cable.

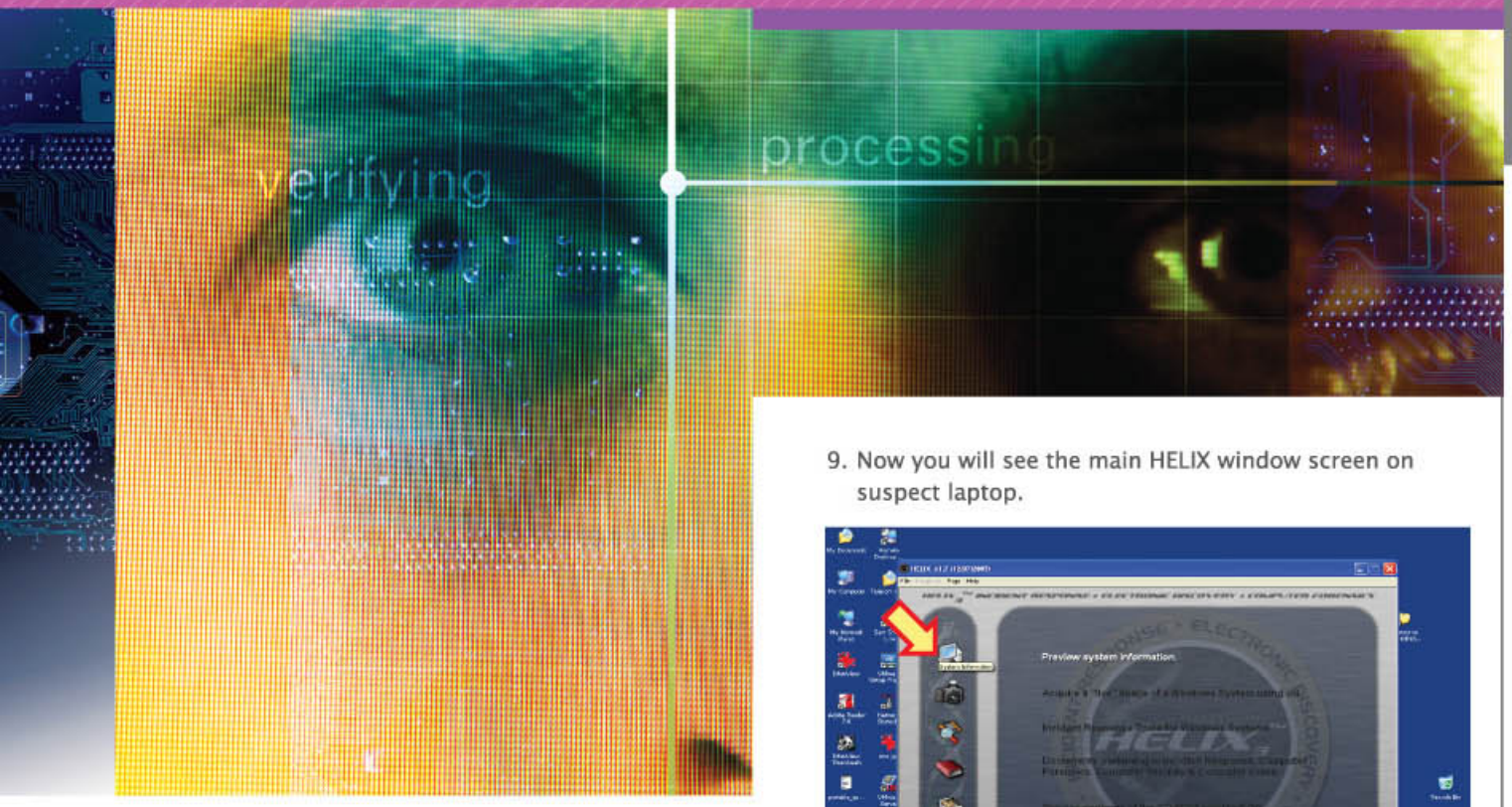
4. Configure the Acquisition laptop IP address to gateway IP address of the Suspect laptop.
5. Establish the network for both machines. This means both machines are able to ping each other.
6. Run "nc" and "dd" command from the Acquisition laptop. These combinations of command use for accept image of the evidence from Suspect laptop. Example of command:

nc -l -p 9000 | dd of=/share/casename.dd

Picture 1: Acquisition setup between Acquisition laptop and Suspect laptop.

7. Insert the HELIX 1.7 Knoppix Live CD into the Suspect laptop.

icrosoft Windows Environment



Picture 2: Acquisition using HELIX 1.7 Knoppix Live CD.

8. Wait until the HELIX main screen window shows up on the suspect laptop and press "I Agree" to continue the process.

Picture 3: Helix End User License Agreement information.

9. Now you will see the main HELIX window screen on suspect laptop.

Picture 4: Preview system information by clicking on the computer icon.

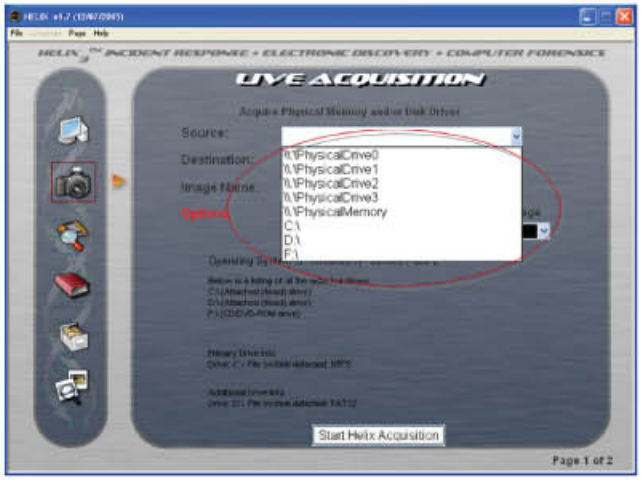
10. Click on the Computer icon to view the system information.

Picture 5: System information window.

11. Click on the Camera icon to start the live acquisition

Picture 6: Live acquisition window appears after clicking the camera icon.

12. Choose to image the whole hard disk on the Suspect laptop.



Picture 7: Hard disks and partitions list.

13. Select option "NetCat" and type in IP address and and Port number of the Acquisition laptop. Press "Start Helix Acquisition"..

Picture 8: IP Address and Port number of Acquisition laptop.

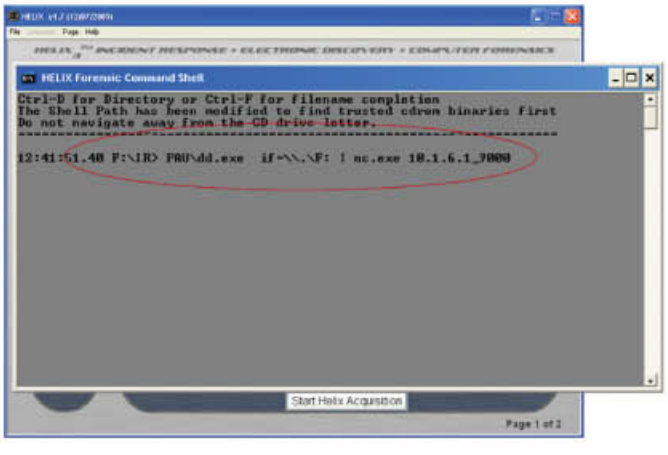
14. Press "Yes" to proceed.

Picture 9: The dialog box shows the command line that will be executed.

15. Press "OK". The argument to run the acquisition will be automatically copied for you by Helix.

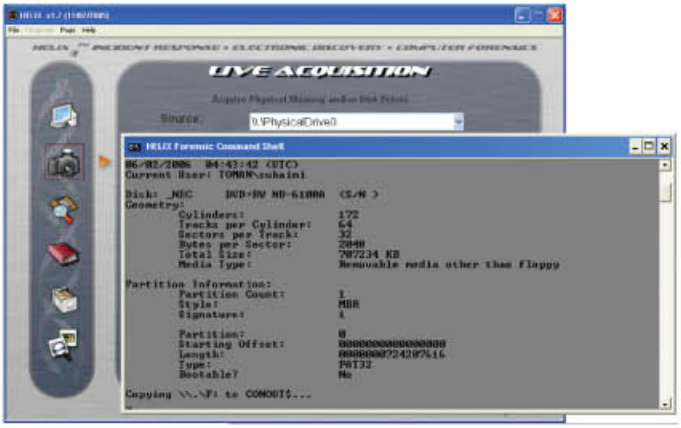
Picture 9: Confirm the process.

16. Paste the argument at the command prompt and press "Enter".



Picture 11: Paste the command line at the command prompt and execute it.

17. Let the process run until it is completed.



Picture 11: The acquisition process in progress.

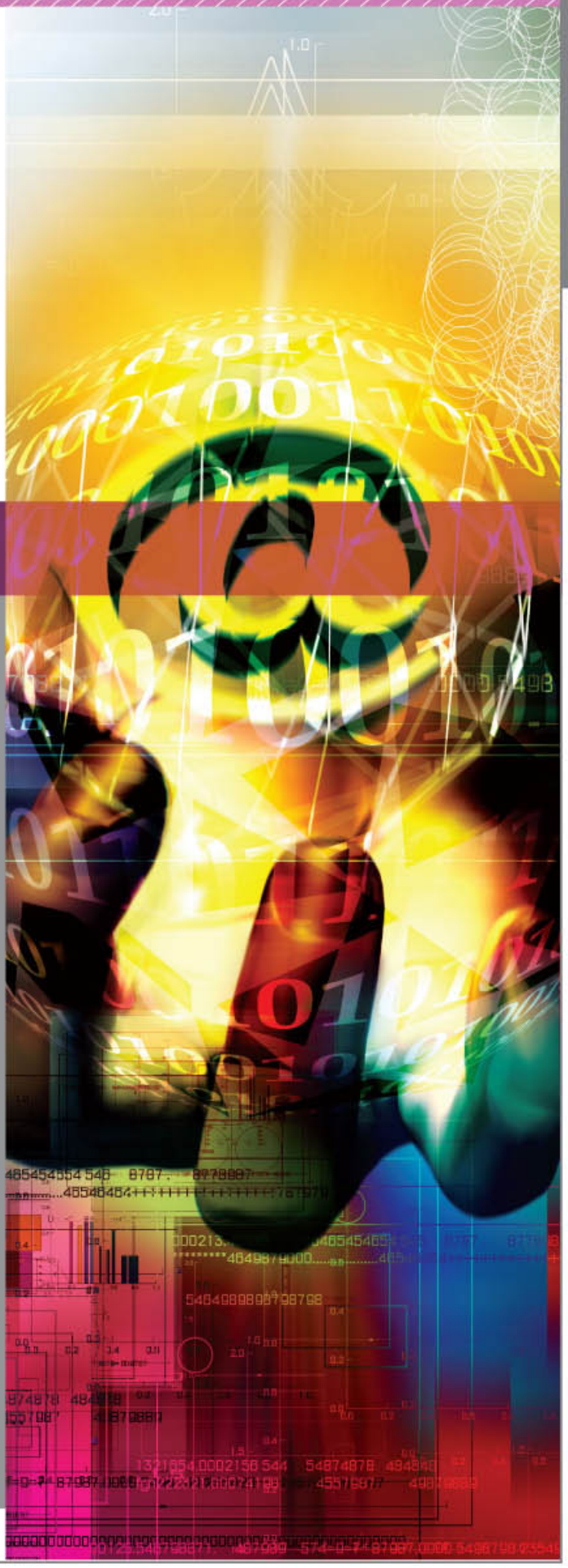
Summary

The acquisition process will produce a *.dd file. It is a raw image file of the suspect hard disk. The image file is the snapshot of the live system on that particular time. This image file can be used for analysis using most of the forensic software in the market (both proprietary and open source).

By performing the live acquisition by the first responder team would help preserving the digital evidence especially on the volatile evidence before the law enforcement team arrives at the crime scene. This will minimize the probability of the digital evidence being deleted or overwritten. In this critical moment, first responder actions will be of a big help to preserve the digital evidence.

The live acquisition using Helix is a good option for first responder to preserve the digital evidence at the crime scene because it is fast, simple and portable. First responders need not have massive knowledge to perform this task, a minimum knowledge in Linux or Windows environment will do.

This process will not only help the investigators to preserve the digital evidence immediately but also will accelerate the overall case investigation process.



Introduction Of Cryptography-Part 2

This article is continuity to the Introduction of Cryptography that was presented in Q1 article. In the previous article, we discussed on two most famous classical methods used in Cryptography - the Caesar Cipher and the Porta Cipher. Conversely, this quarterly article introduces another two classical methods employed in this field; the Playfair Cipher and the Transposition Cipher.

Playfair Cipher

Playfair Cipher was first invented in 1854 by a scientist, Sir Charles Wheatstone. However, the method was not named after the inventor but was ironically named after Lord Lyon Playfair who successfully promoted the system until it was officially used by the British government.

Playfair Cipher is also known as *Playfair Square*, the system comprises of a 5 by 5 square. There are three pivotal steps that must be followed in order to employ this system:-

Step 1: *Keyword Formation*
Step 2: *Playfair Table Generation*
Step 3: *Pairing of Plaintext*

A short keyword is used to form the 5 by 5 alphabetic table. For example, let's use the word "PLAYFAIR" as the keyword. Any duplicated letters should be dropped out to create a shortened keyword. In this case, the second A in "PLAY-FAIR" will be omitted from the keyword and will give us "PLAYFIR".

Keyword:	P	L	A	Y	F	~~A~~	I	R
Shortened Keyword	P	L	A	Y	F	I	R	

A 5 by 5 table will only gives us 25 characters. As we are aware, there are 26 alphabets from A to Z. There are two ways to overcome the problem; we can either combine I and J in one cell or we can omit Q as it is the least used alphabet in frequency count. To continue on with this example, we will consider the first approach.

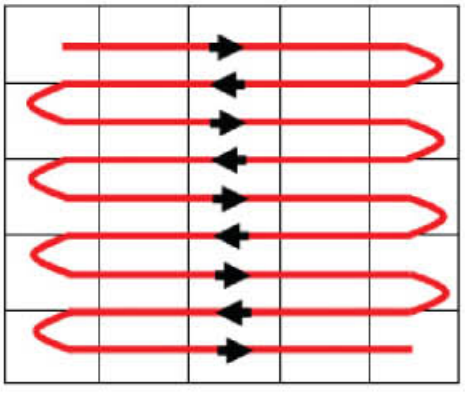
Arranging all these alphabets also depends on certain pattern. Three most used patterns in creating Playfair Table are:-

a) Start from top row, moves from left to right and continues on to the next row.

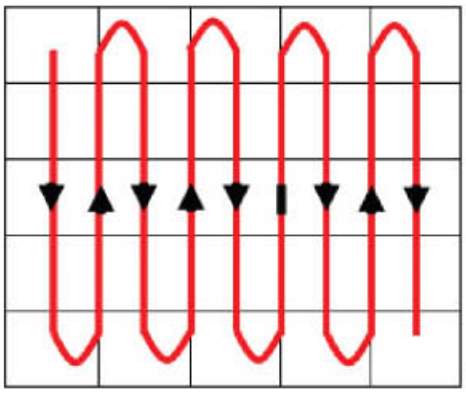
b) Start from left column, moves from top to below and continues on to the next row.

c) Spiral pattern: Begins from top left box, moving to right end and continues down. This pattern will end in the middle of the table.

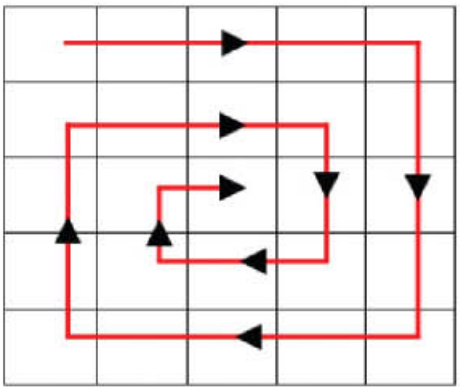
These three patterns are shown below:



(a)



(b)



(c)

Again, we will consider the first pattern in our example. The shortened keyword is first written in this table followed by the remaining letters of the alphabet, filled in order.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Now, let the plaintext that is to be encrypted be "GOOD BROOMS SWEEP CLEAN". First of all, the plaintext must be broken into diagraphs; two-letter groups. Identical pairs are to be excluded. However, when this occurs the identical pair must be padded with the alphabet Z between them. This padded Z must also be applied if the number of letters is odd.

Plaintext : G O O D B R O O M S S W E E P C L E A N
Plaintext in diagraphs: GO OD BR OO MS SW EE PC LE AN
Plaintext with padded Z : GO OD BR OZ OM SZ SW EZ EP CL EA NZ

When the Playfair Table is ready and the plaintext has been paired, only then can the encryption process be applied. The paired letters can only appear in three possible combinations in the Playfair Table. The cipher text of each paired letters must be read according to these three rules:-

a) If the plaintext letters appear in the same row, each cipher text letter will be the next letter on its right (rows are cyclical).
b) If the plaintext letters appear in the same column, each cipher text letter will be the next letter below it (column are cyclical).
c) If the plaintext letters appear in neither the same row nor the same column, the substitution of cipher text letters will be based upon their intersection.
   - The first cipher text letter is in the intersection of row of first plaintext letter and column of second plaintext letter.
   - The second cipher text letter is at the edge of rectangle formed by the three letters.

Examples of these three rules are shown below:-

I/J	R	B	C	D

(a)
BR→CB

P				
I/J				
E				
N				
U				

(b)
PE→IN

	R	B	C	D
	G	H	K	M
	O	Q	S	T

(c)
OD→TR

Thus, the discussed example gives the following answer:-

Plaintext : GO OD BR OZ OM SZ SW EZ EP CL EA NZ
Cipher text : OV TR CB TV TG TX QX MU NI RY HP TU

Transposition Cipher

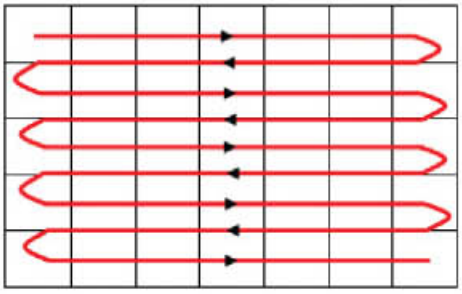
The Transposition system is one of the most frequently used method of encryption or decryption in a classical cryptology. In this system, the plaintext characters of message are rearranged without changing the letters. In other word, the same characters of the plaintext are still present but the order of the letters (plaintext) is changed systematically.

Types of Transposition System

There are many types of Transposition System but based on the current discussion, we will focus on the geometric process based on the fact, that it is the most used Transposition System that be employed in this process. In the geometric processes, plaintext is written into geometric figure such as square or rectangle and is extracted given the selected geometric figure by a different path. In this model, there are two types of Transposition known as the Columnar Transposition and the Route Transposition. When the geometric figure is a rectangle or square and the plaintext is entered by rows and extracted by columns, it is referred to as the Columnar Transposition. Whereas, when another route other then rows and columns are used, it is described and known as the Route Transposition.

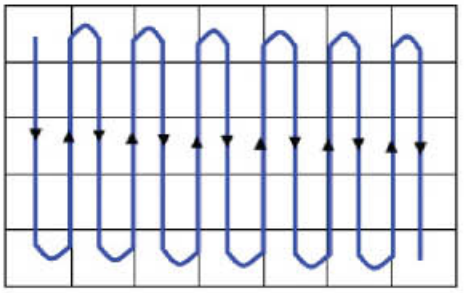
Example of a Columnar Transposition

The Columnar Transposition is the most commonly used method of Transposition. The Transposition denotes that the plaintext is entered into a rectangle or square and extracts the cipher text by columns from left to right. For example, a simple Columnar



In this method, we fill the plaintext from the top row, and then we move it from left to right and continue on to the next row.

Transposition with a width of seven is shown below.



After having arranged the plaintext, we can then encrypt the plaintext by column, beginning from the left column and then moving it from top to bottom and continue on to the next column.

Plaintext: THE BEAUTY LIES ON THE EYES OF THE BEHOLDER

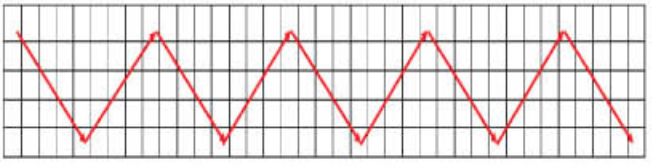
T	H	E	B	E	A	U
T	Y	L	I	E	S	O
N	T	H	E	E	Y	E
S	O	F	T	H	E	B
E	H	O	L	D	E	R

Ciphertext: TTNSE HYTOH ELHFO BIETL EEEHD ASYEE UOEBR

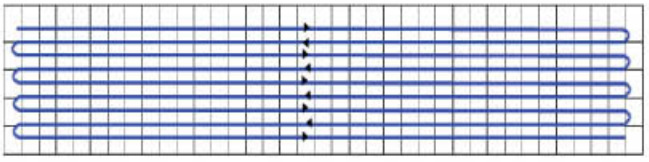
Example of a Route Transposition

There are many other ways to transpose messages or plaintext using Route Transposition rather than Columnar Transposition. Some of these methods are shown below.

1. The rail-fence cipher is inscribed by zigzag pattern and extracted by rows



In this example, we write the plaintext by using a zigzag pattern from top to bottom and continue on until the plaintext has been completed.



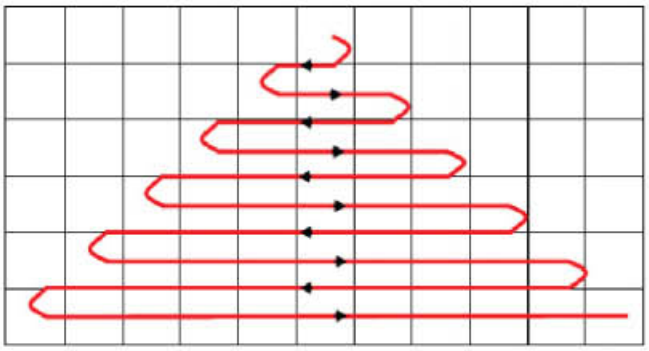
To encrypt this plaintext, we should read from the top row, and then move from left to right and continue on to the next row.

* If the length of the message is not enough to fill the selected box, then we should add the appropriate number of Zs at the end before we begin to encrypt.

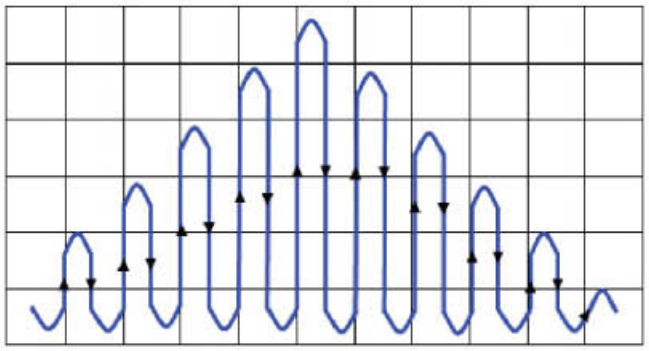
T								Y								H								T							D			
	H						T		L						T		E						F		H						L		E		
			E					U				I				N				E				O				E				O				R	
				B		A							E		O						Y		S						B		H					Z	
					E									S									E							E						Z

Ciphertext: TYHTD HTLTE FHLEE UINEO EORBA EOYSB HZESE EZ

2. The triangular pattern is inscribed by rows and extracted by columns.



In this type of encryption, we write the plaintext by using the triangular pattern, by writing it up from the top row, and then moving it from left to right and continuing on to the next row.



To encrypt it, we extract it by using column, which means we read it from left column, and then we move it from top to below and continue on to the next column.

					T					
				H	E	B				
			E	A	U	T	Y			
		L	I	E	S	O	N	T		
	H	E	E	Y	E	S	O	F	T	
H	E	B	E	H	O	L	D	E	R	Z

Ciphertext: HHELE BEIEE HAEYH TEUSE OBTOS LYNOD TFETR Z

Given the two examples of the classical method, why not try to encrypt the following plaintext given below by means of using the Playfair Cipher and the Transposition Cipher?

Keyword 1 : CODEBREAKING
Plaintext 1 : BE PREPARED TO ATTACK AFTER DAWN

Keyword 2 : PASSWORD
Plaintext 2 : PROCRASTINATION IS A THIEF OF TIME

Keyword 3 : KEYWORD
Plaintext 3 : TO LISTEN IS TO LEARN AND TO UNDERSTAND IS TO INSPIRE

There are of course other classical methods that have not been discussed in this article. Await for our next article, in which we will further explore other classical cryptography methods.

Spam 2.0 Moves to facebook

MALAYSIA, 31 March 2008 – Fortinet Global Security Research Team warns about hijacked Facebook accounts posting deceptive messages on Wall.

Like most social networking sites, Facebook has a "Wall" feature, allowing users to post comments on friends' profiles. This is currently being exploited by spammers to post deceptive messages, linking to typical spam sites such as (but perhaps not limited to) online "pharmacy" shops.

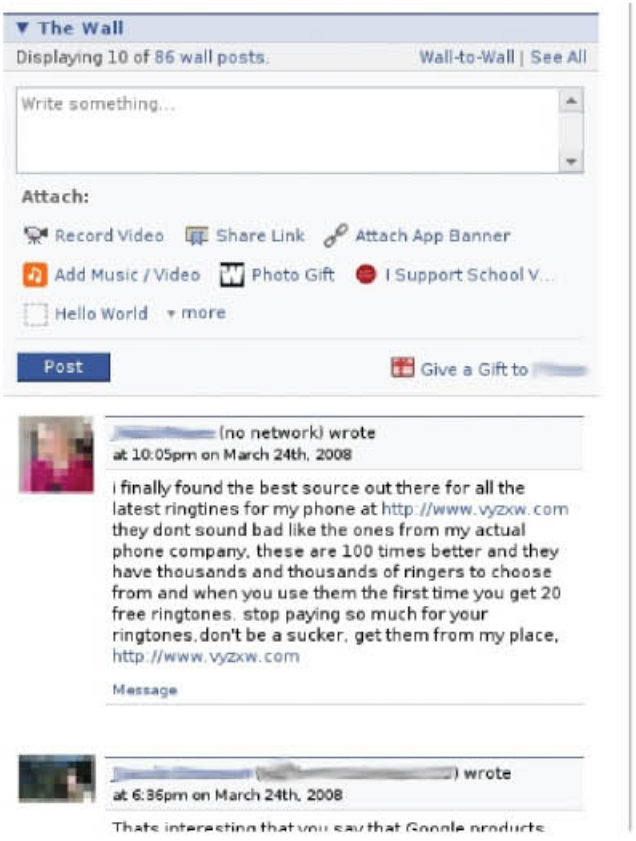


Figure 1: Spam 2.0 Paradigm

Figure 1 above shows a typical Spam 2.0 message posted on a Facebook profile. The user who posted was verified to not be a spammer; rather, her account was hijacked by identity thieves who likely later sold (or rented) it to spammers. The means utilized by the identity thieves to hijack this victim's account are not known, however, in such cases, the phishing hypothesis prevails: A phishing worm was spotted spreading on Facebook earlier in the year¬¬[1] and both incidents may be related.

Please note that although this has been rarely seen on Facebook so far, it is fairly common on MySpace. Further details about the whole process and the economics behind it were given at VB2007 Conference[2], and are summarized here. One of the spamvertised links has been confirmed to resolve to a web host that also serves content for several pill pushing sites, involved in a criminal fraud ring. Included in this ring is Canadian Pharmacy - an analysis of which can be seen here. (More details on this criminal ring will be published shortly in a second analysis.)

The Fortinet Global Security Research Team advises social networking site users to be wary of phishing attempts: when confronted by a login page or upon clicking a link contained in a friend's message, carefully check the login page URL. Legitimate login pages are hosted on the original social site domain (here, Facebook.com), while rogue login pages cannot be. Also, mental tricks may sometimes be utilized to trap users (eg: Facebook.com.dsfsafdf.cn, Facebook-login.com, Facebopk.com, etc.), as it is frequently the case in phishing schemes. For these reasons, leveraging adapted security gear that integrates real-time blackhole lists of known phishing sites is pertinent.

Beyond that, wall posts containing links must be handled with care. While hijacked accounts have not been proved to be utilized for anything beyond posting relatively innocuous spam 2.0, it is not a stretch to think that links to drive-by-install malicious sites could be injected at some point. Following links contained in wall posts is therefore not recommended.

Facebook has been notified, and is looking into this issue.

Acknowledgment

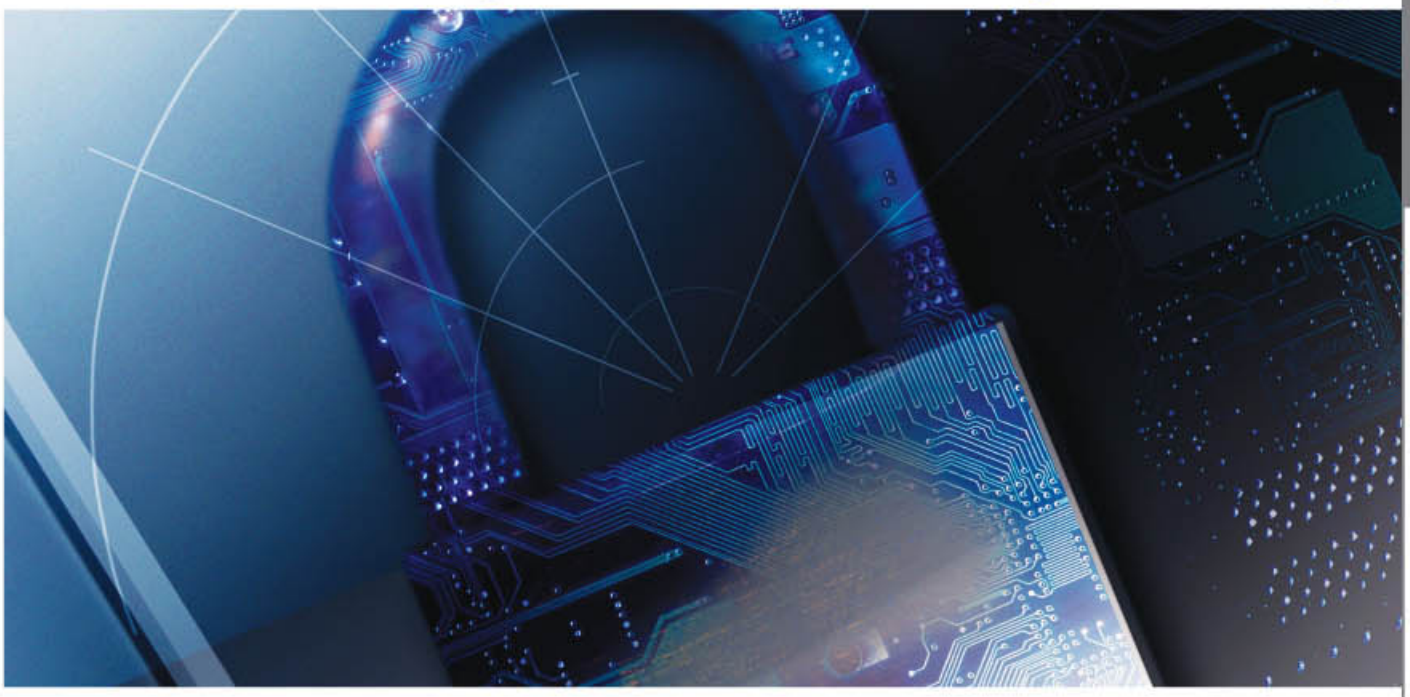
· Initial blog post by Jesse Stay

Notes

http://www.wired.com/politics/security/news/2008/01/facebook_phish

Menace 2 the Wires: Advances in the Business Models of Cybercriminals, Guillaume Lovet, VB2007, Vienna

An Overview Of The National Cyber Security Policy



In 2005, with the aim to accommodate Malaysia's journey towards a knowledge-based economy (K-economy), the Ministry of Science, Technology and Innovation (MOSTI) realized the increased reliance on Critical National Information Infrastructure or also referred to as the CNII. With this in mind, a study was conducted against strategic efforts in order to secure the nationwide information infrastructure. Thus the National Cyber Security Policy (NCSP) was drafted with the objective of addressing and mitigating the risks faced by the CNII.

The policy defined the CNII as "information infrastructures" that are crucial to the nation and if paralysed by cyber attacks, it would significantly disrupt national function, its economic strength, image, defence and security, public safety and health, thus contributing to the government's capabilities to function effectively.

Other developed countries such as the United Sates and Canada have formulated national security strategy in dealing with cyber threats. The United States has in place the National Security Strategic Plan, the National Strategic to Secure Cyber Space and the National Response Framework. Conversely, in Canada there is the Canada National Security Policy and the National Critical Infrastructure Protection Strategy. Similarly in Malaysia, the National Cyber Security Policy, is aligned and formulated along the same line.

The National Cyber Security Policy consists of eight areas which are referred to as the thrusts. These thrusts provide focus and directions on the implementation of the policy. The eight Policy Thrusts are:-

Thrust 1
Effective Governance

Thrust 2
Legislation and Regulatory Framework

Thrust 3
Cyber Security Technology Framework

Thrust 4
Culture of Security and Capacity Building

Thrust 5
Research & Development towards Self Reliance

Thrust 6
Compliance and Enforcement

Thrust 7
Cyber Security Emergency Readiness

Thrust 8
International Cooperation

Each of the thrusts is interrelated with each other and has its own role in mitigating cyber incidents and disruptions to the CNII. For example; Thrust 1 - Effective Governance, is to ensure that the implementation of the National Cyber Security Policy is developed and coordinated properly by bodies or parties hold the appropriate authority. In addition, to achieve this objective, Thrust 1 also identifies the need for effective information sharing between the public and the private sectors. A framework will be formulated so as to channel or delegate any decisions that are made at the higher level and translated into actions on the ground.

Meanwhile Thrust 2 - Legislative and Regulatory is meant to review and enhance Malaysia's cyber laws to accommodate cyber security threats and simultaneously ensure that the local legislations are in accordance with international laws, treaties and conventions. Thrust 3 - Cyber Security Technology Framework, on the other hand is proposed to provide a reference point for formulating information security standards as a baseline requirement for ICT products employed by the CNII organizations.

Further, The Culture of Security and Capacity Building as enumerated under the Policy Thrust 4 gives emphasis on the human elements. It is solely designed to create awareness and to inculcate the culture of security amongst the CNII and the general public. Thrust 5 - Research & Development Towards Self-Reliance is designed to promote research and development on information security technology of which, could result into an enhanced security research community. In order to ensure that all the CNII organizations are at the required minimum level of security, the information security management standards need to be established and complied with. Thus, Thrust 6 - Compliance and Enforcement, takes care of the latter. It focuses on standardising, strengthening and developing the cyber security systems across the CNII organizations.

Despite comprehensive precautions taken through the adoption of the information security management standards, the risk to the CNII should also be managed by ensuring proper emergency response mechanisms, as seen in Thrust 7. Thrust 7, focuses on strengthening the national computer emergency response teams (CERTs) in order to have an effective cyber security incident reporting mechanism. Finally , Thrust 8 - International Cooperation spells out the national involvement in the field of cyber security. The involvement caters for active participation in conferences and hosting similar events, to keep abreast with the latest threats, methodologies and technologies relating to cyber security.

In terms of implementation, the National Cyber Security Policy is divided into three Phases, concentrating on different objectives. The Immediate Phase is to address current concerns with measures taken with the existing available resources. The intermediate phase is to build the necessary infrastructure while, the final phase will focus on developing self-reliance of the CNII.

In conclusion, the National Cyber Security Policy is a policy framework to enhance the security level of the CNII and to enable Malaysia to remain competitive whilst taking a proactive position in handling cyber security issues globally.

MS 1970: Business Continuity Management (BCM) Framework at a glance.

Business continuity management (BCM) is currently being taken more seriously by organizations in Malaysia. More organizations now understand the importance of BCM and have taken appropriate measures to ensure organization's resiliency. Bank Negara Malaysia, for instance has taken a proactive measures in ensuring service continuity of its banks and financial institution, by producing BCM Guidelines. This guideline is to be adhered by all financial institutions.

Department of Standard Malaysia has officially launched MS 1970:2007 Business Continuity Management Framework on 6th May 2008. The standard marks the first standard pertaining Business Continuity Management (BCM) in Malaysia.

The standard is the first part from 3 series of BCM standards that is to be developed. The next part which is already in the development phase is BCM Guidelines. The third instalment of the standard will be BCM Self assessment checklist.

MS 1970 is aimed to provide the user with a structured process of developing BCM Framework. Although it is not meant to be implementation guidance and most probably will not answer the question of how to implement BCM in the organization, however it still sets a foundation for BCM implementation.

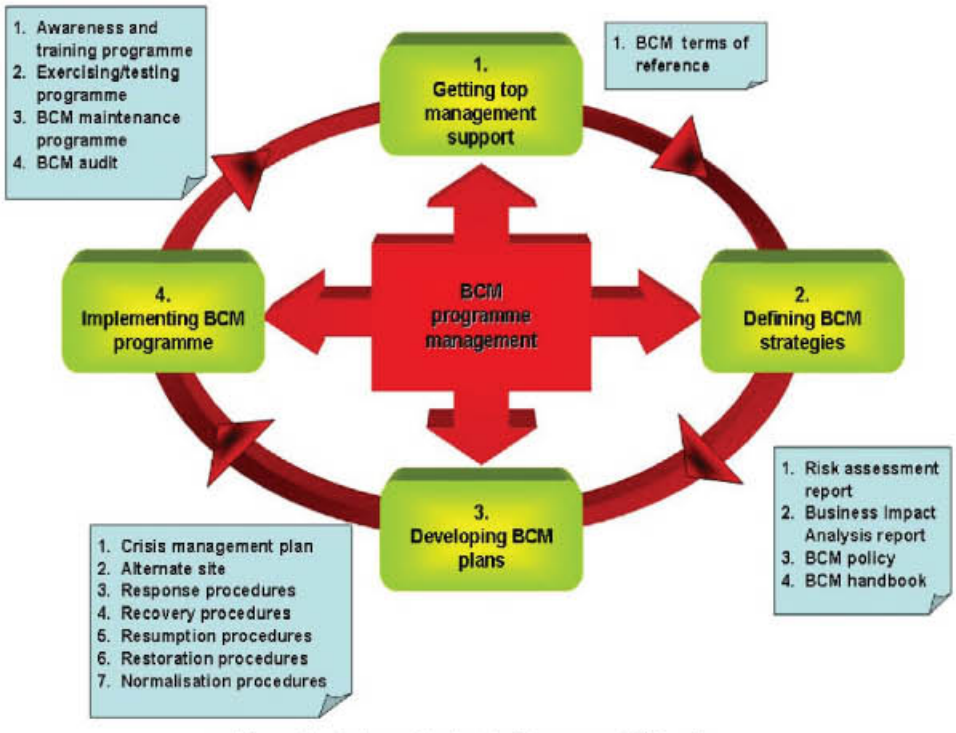
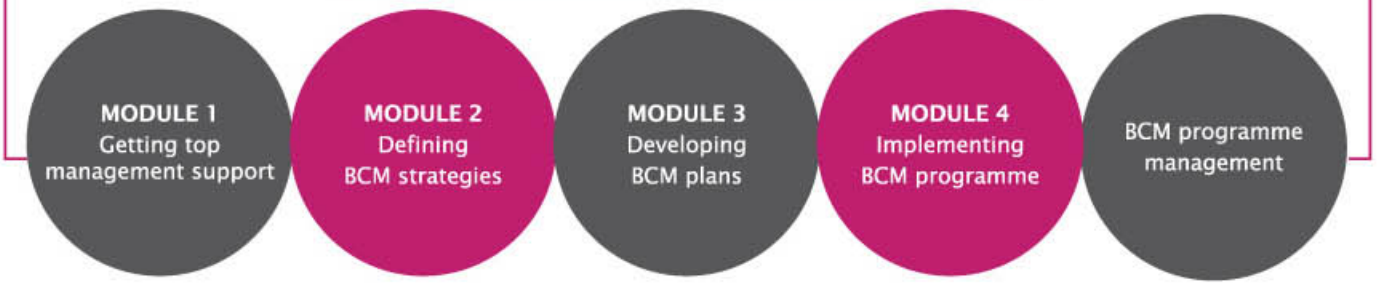


Figure 1. Business Continuity Management life cycle

The life cycle highlighted 5 modules, which are:



Each module have its own set of deliverables. For each module, description, objectives, deliverables, assumptions and recommended steps are explained in high level. These modules are meant to be executed in sequential manner, where one module must be completed one after the other. Each deliverable for each module is essential in initiating the next module. The modules are managed by BCM programme management, which oversees the execution of each module.

Module 1 highlights the importance of top management support. BCM implementers must be able to convince top management on the need to implement or revise the existing BC plan. Top management must support BCM initiatives in terms of providing company's directive and financial support for BCM implementation to be successful. The deliverables for this module is an endorsed Term of Reference.

Module 2 emphasise on data gathering activities. Assessment of current organizational business impact and risks are done during this phase. This module would be one of the most tedious modules to be delivered, because it involves a lot of inputs and data analysis. The deliverables for this module includes Risk Assessment report, Business Impact Analysis report, BCM policy and BCM handbook.

Module 3 is where all strategy defined in Module 2 will be implemented. All plans developed in this phase, must be in line with Business Impact Analysis findings and must be able to mitigate and reduce risks findings in the risk assessment report. Deliverables for this phase encompasses Crisis Management Plan, establishment of one or many alternate sites and continuity/recovery plans.

Module 4 is the maintenance module, which is developed to ensure the state of readiness of the organization is maintained. Following an awareness and training programme, all plans that has been developed on Module 3, will be exercised in this module. BCM audit will be conducted to ensure that the organisation has an effective BCM programme. Deliverables for this module consist of Awareness and Training programme, Exercising and Testing, BCM programme maintenance and BCM audit.

How can the public benefit from the standard?

Business Continuity implementers with certain extent of knowledge in business continuity can adopt the BCM life-cycle in their BCM implementation easily. They can build their BCM implementation plan, based on the framework.

Industries or regulatory bodies can or should use the standard as a base to develop their sector specific BCM guideline. As MS 1970 is a Malaysian standard, it is crucial for it to become the main reference for all local organization across all industries.

But the issue is, how can a BC implementer who has no experience in BCM implementation? Can they benefit from the standard? As mentioned before, MS 1970 is not an implementation guidance where, a non-experienced BC implementers can easily use as step-by step guidance to assist in BCM implementation. It doesn't have BC templates, or toolkits that can be used to ease the implementation process.

However, from the high level BCM lifecycle, BC implementers can use it as a basis of their BCM term of reference. They can use it to know the minimum requirement and deliverables for each phase of BCM implementation. One of the ways to optimize the usage of the standard is by using it as a reference and use other best practices, tools, checklists and templates to fulfil MS 1970's requirements.

MS 1970 is in line with other standards in the world which are BS 25999 Part 1- Code of Practice by British Standards and HB 221 Business Continuity Standards by Australian and New Zealand Standard. Most BCM standards are upholding the same values and of course the same objective which to guide BC implementers in improving organizational preparedness and its resiliency during crisis.

MS 1970 is a new standard. It needs to be used and scrutinized by BC players and implementers in order to attain feedbacks on the framework. The coming BCM Guideline by Malaysian Standard, will offer more assistance in implementing BCM. More guidance, control, and templates will be recommended in the guideline. For now, BCM Framework can be used as the starting point of the implementation.

2 Factor Authentications (2FA); Authentication and Security

Introduction to Authentication

Protection through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications. Online banking user interfaces are secure sites (generally employing the https protocol) making it generally impossible for a third party to obtain or modify information after it is sent. However, encryption alone does not rule out the possibility of hackers gaining access to vulnerable home PCs and intercepting the password as it is typed in (keystroke logging). There is also the danger of password cracking and physical theft of passwords written down by careless users.

Authentication is the process of verifying that the identities of computers, and the identities of people, are authentic. When a system attempts to verify the identify of a person, the process is called user authentication [2]. In other words, the user wishes to log on to a network or service and claims to be a certain person. The authentication process attempts to verify this claim via the provision of a predefined characteristic (PIN / password / token / biometric or other information), or multiple characteristics that are associated with the claimed identity.

Authentication is the process of verifying that the identities of computers, and the identities of people, are authentic. When a system attempts to verify the identify of a person, the process is called user authentication [2]. In other words, the user wishes to log on to a network or service and claims to be a certain person. The authentication process attempts to verify this claim via the provision of a predefined characteristic (PIN / password / token / biometric or other information), or multiple characteristics that are associated with the claimed identity.

Introduction to Strong Authentication

A definition of strong authentication isn't common. Below are some examples of the definition found on the internet:

"Strong authentication[3] is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network."...

"strong authentication[4]
Strong authentication, also called two-factor authentication, is defined as two out of the following three proofs:

- something known, like a password,
- something possessed, like your ATM card, and
- something unique about your appearance or person, like a fingerprint.

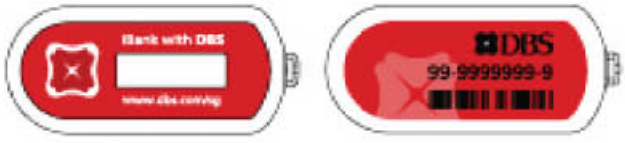
Using strong authentication provides more protection for sensitive information than a simple username and password can provide. Strong authentication, especially when combined with other practices like mutual authentication and non-repudiation offers a strong assurance that a transactions are conducted by two known and trusted parties."...

There are several different ways to authenticate a user and relates this to factors. Using more than one way or factor is also sometimes called strong authentication. Below is the list of multiple ways through which a user can identify herself and combination of 2 ways is called two-factor authentication:

- Knowledge: - Something you know (for example a PIN or password)
- Possession: - Something you have (for example card, key or token)
- Being: - Something you are (for example fingerprint, iris and voice)

Two-factor Authentication – (Knowledge & Possession)

The combination of something the user has (e.g., ID card, security token, software token, phone, or cell phone) and something the user knows (e.g., a password, pass phrase, or personal identification number (PIN)) is considered as 2FA and are widely used nowadays especially in banking.



Hard Token (Front) *Hard Token (Back)*

Currently passwords are still the most common method being used for authenticating users. The technique is easy to administrate and simple for most users and also the least expensive method of user authentication. However, passwords have some drawbacks. User usually selects passwords that are very short and simple, which makes them easy to guess. This problem can be solved by implementing password policies that may require a minimum password length or include mixed case letters or numbers, and may even force users to change passwords on a regular basis. Unfortunately, these rules make passwords even more difficult to remember, which leads some users to write them down and therefore, compromise the original goal of security.

Something that the user has (e.g., ID card or bank card) has evolved from the magnetic stripe into smart card technology. Basically, the term "card technologies" include any technology that can be placed on a card. The card can be made of plastic (polyester, pvc, or some other material) or paper, or even some amalgamation of materials. It used to provide "access" to something and it includes some form of automatic identification and data capture technology.

There are two main card technologies which is widely used by the bank industry as listed below:-

1. Magnetic Stripe Technology
2. Smart Card Technology

Magnetic Stripe Technology

A magnetic stripe card is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called a magnetic stripe, is read by physical contact and swiping past a reading head. Magnetic stripe cards are commonly used in credit cards, identity cards, and transportation tickets. They may also contain an RFID tag, a transponder device and/or a microchip mostly used for business premises access control or electronic payment.

List of advantages in using this technology:-

- Data can be modified or rewritten
- High data capacity in relation to bar codes
- Added security since it is not in human readable form
- Immune to contamination with dirt, water, oil, moisture, etc
- No moving components, physically robust
- Well established standards
- No consumables required for writing or rewriting

List of disadvantages in using this technology:-

- It doesn't work in a distance, thus requiring close contact to the reader.
- Data can be damaged by stray magnetic fields
- Since it's not in human readable form can be a disadvantage in some applications

Smart Card Technology

A smart card, chip card, or integrated circuit card (ICC), is defined as any pocket-sized card with embedded integrated circuits which can process information. This implies that it can receive input which is processed - by way of the ICC applications - and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally PVC, but sometimes ABS. The card may embed a hologram to avoid counterfeiting.

List of advantages in using this technology:-

- The card cannot be cloned easily; hence it offers better security and reduces fraud in comparison to the current magnetic based ATM cards.
- The chip embedded in the Bankcard is a tamper resistant and the data or other information stored on the chip that are significantly harder to extract and copy.
- Allows multi-application convenience in a single card and the applications on the card can be updated without issuing a new card.
- Each card has a unique serial number.
- Provides convenience and safety of not having to handle large amounts of cash.
- Improves service through convenient operations and faster transaction processing

List of disadvantages in using this technology:-

- The cost of the cards, particularly during the early years of its use when fixed costs need to be amortized over small volumes;
- The cost of installing new devices or adapting existing terminals to read the cards. Replacement of existing point-of-sale devices is typically undertaken on a cyclical basis about every 5 years, and the cost of premature replacement is likely to remain prohibitive;
- The need for an external device to provide a power-supply, clock-function and (in most cases) input-output capabilities; and
- The need for sophisticated key management mechanisms, including the establishment and satisfactory performance of a certification agency.

Compared to magnetic stripe, smart card is more secure to be used. By having chip on the card, smart card protects the information stored from damage or theft. Current magnetic stripe cards have limited capacities to copy information.

By using smart cards that have greater capacity, customer profiles can be broader and information can be easily added or deleted from the memory. In addition, smart card can perform decision making due to the powerful processing capabilities, such as data encryption.

Two-factor Authentication – (Knowledge & Being)

More secured authentication using combination of something the user has (e.g., ID card, security token, software token, phone, or cell phone) and something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier) is become popular especially on physical security such as door access.

A biometric cannot be transferred between individuals and represents as unique identifier. The strongest single approach to achieving user authentication involves the analysis of a unique physical attribute of a person, such as a fingerprint or patterns in the eye. This field of technology is known as biometrics.

Biometric authentication factors include:

Fingerprint scanning

Which analyses the unique pattern of ridges on a person's finger[4]. The fingerprint scanners shine a light through a prism that reflects off a finger to a charge-coupled device (CCD), creating an image that gets processed by an onboard computer. It's should be noted the actual fingerprint image is not recorded. Instead, the devices perform reduction of the image to data points, called minutiae, that describe the fingerprint layout, called a template[5].

Iris scanning

This utilizes cd camera element and requires no contact between user and reader [6]. It has the potential for higher than average template matching performance. Ease of use and system integration have not been have not been strong points with the iris scanning devices.

Retinal scanning

This is an established technology where the unique patterns of retinal are scanned by a low intensity light source via an optical coupler [5]. Retinal scanning has proven to be quite accurate but it does require the user to look into a receptacle and focus on a given point which is not convenient for the user if he/she wears spectacle. This is the reason retinal scanning has fewer user acceptance than other technologies [8]

Voice recognition systems

Which recognize a unique audio wave pattern that is generated when a person says a specific word [5]. Voice authenticators use a telephone or microphone to record a user's voice pattern, then use that pattern to validate the person. Since these software systems rely on very low-cost devices, they are generally the least expensive systems to implement for large numbers of users. The standard caveats learned from voice dictation systems apply here. These services must be able to work with background noise and the variability f off-the-shelf microphones [7].

Facial recognition systems

Which store the unique features of a person's face, such as the distances and angles between the eyes, nose and mouth[5]. Face recognition devices use PC-attached cameras to record facial geometry. To date, facial recognition systems have had limited success in practical applications. However, improvements have been made into this area and facial recognition may become a primary biometric technology [7].

Conclusion

User authentication is an important process in any security systems. There are three types of authentication used:

- Knowledge (password or PIN)
- Possession (smart card, magnetic stripe card or a physical key)
- Being (your fingerprint, retinal/iris scan or voice pattern)

The password authentication technique is simple and least expensive. However, it provides a weak form of authentication as password can be stolen or shared by users. The combination of Possession and Knowledge factors such as password/PIN and smart card will provide a stronger form of authentication. This is 2FA and if the card is stolen, the system cannot be accessed without a password/PIN, and vice versa . The disadvantages of this approach are that tokens can be lost or stolen, and users must remember to have them in their possession. Tokens are more expensive than simple passwords to implement and manage.

The problem with recognition of passwords, cards and other tokens for authentication is that it does not necessarily guarantee the recognition of the person who has provided it. A biometric however cannot be transferred between individuals and represents as unique identifiers. This is another type of 2FA, biometric factors demonstrate the strongest form of user authentication because they cannot be lost or stolen, shared or forgotten.

A two-factor authentication such as password and smart card or smart card with biometric will improve the level of security. Multi-factor authentication will provide the highest level of security however the drawback of this approach is that it may cause inconvenience for the user during the authentication process.

References

[1] Authentication from Wikipedia, the free encyclopedia [Web document] Available: http://en.wikipedia.org/wiki/Authentication

[2] Lynch, C., April 1988, A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources. [Web document] Available: http://www.cni.org/projects/authentication/authentication-wp.html#Introduction

[3] Strong Authentication at Fermilab (Sept 2006) [Web document] Available: http://www.fnal.gov/docs/strongauth/

[4] Information Security Glossary: strong authentication [Web document] Available: http://www.rsa.com/glossary/default.asp?id=10800

[5] Ashbourn, J., 1999, The biometric White Paper, [Web document] Available: http://homepage.ntlworld.com/avanti/whitepaper.htm

[6] Ashbourn, J., 1999, Biometrics and PKI, [Web document] Available: http://homepage.ntlworld.com/avanti/pki.htm

[7] ZDNet. Are you ready for Biometric ? [Web document] Available: http://www.zdnet.com/pcmag/features/biometrics/

[8] Clegg, B., April 1999, Searching for the key to your identity. [Web document] Available: http://www.findarticles.com/cf_0/m0COW/1999_April_8/54459494/p1/article.jhtml?term=%2BBiometric+%2Bresearch+%2BUsage

Security in the SMB

According to a Panda Security study, available on the Infected or Not website (http://www.infectedornot.com), 72 percent of companies are infected by malware. Having malware on a corporate network can result in loss of important data, reduced productivity, and even complete paralysis of business activity.

So what can a company do to avoid being part of this 72 percent? Firstly, it must carry out an analysis of its network, determining the critical entry points for threats and how they can be protected. It must then install the corresponding security measures in each of these critical points: security appliances, security solutions for mail servers, security suites in PCs, etc. It is also important to be sure that applications installed across the company are up-to-date, so there are no vulnerabilities that can be exploited by cyber-crooks to infect computers or take remote control of systems.

These measures should be complemented by security training for employees along with frequent security audits. With respect to the former, bear in mind that a company's end-users are the weak point in the security chain. As such, it is important to instill some basic concepts such as not opening emails from unknown sources, not running attachments to these kinds of emails, not clicking links in emails or instant messages and not connecting memory sticks or other devices to the network without ensuring that they are malware-free.

Security audits, for example, are necessary given the rate at which new malware is appearing -some 5,000 new strains every day-, rendering traditional security solutions ineffective. That's why auditing tools such as Malware Radar (http://www.malwareradar.com), which can detect threats that have slipped past other protection, are an essential part of the overall security scenario.

Often, however, no matter how necessary these measures are, an SMB may find them impossible to implement, simply due to a lack of resources (materials, personnel and finance). In these cases the most rapid and effective solution, currently being taken up by SMBs all over the world, is the concept of managed security services.

Put simply, it involves handing over the task of securing a company to a firm specialized in this area. The security company will have sufficient expert resources to implement the necessary security measures.

What are the advantages of this security model for companies? Firstly, it ensures that the SMB's security is in the hands of professionals who have the tools and the experience to provide the highest levels of protection, while allowing company staff to concentrate on their core business. There are also cost savings as, although the service has to be paid for, this is easily offset against the costs of paying a security administrator, buying security devices and solutions, damage incurred through inexpert security management, etc. In short, a company will save on operating costs and loss of productivity, and will benefit from business continuity and security.

For companies that offer this type of service, or those who simply want their own managed security service, Panda Security has launched Panda Managed Office Protection (http://www.pandasecurity.com/enterprise/solutions/managedprotection/?sitepanda=particulares) a Web-based subscription service that eliminates the overheads and costs of managing security hardware, software and personnel for SMBs and remote/branch offices.

Vista's Readyboost Forensic Analysis

Introduction

ReadyBoost is a new disk caching technology included in Windows Vista that uses flash memory to boost the system performance. It can use any form of flash memory such as a USB 2.0 drive (thumb drive), SD card or CompactFlash. ReadyBoost functions as a complement for SuperFetch, giving SuperFetch another place to cache data. SuperFetch is a technology included in Vista which prioritizes the programs that are being run over background tasks and adapts to the way we work. This technology tracks the computer usage behavior and intelligently preloads applications into memory. This helps improving the general performance of the system and the loading times of the core applications [Wikipedia, 2008].

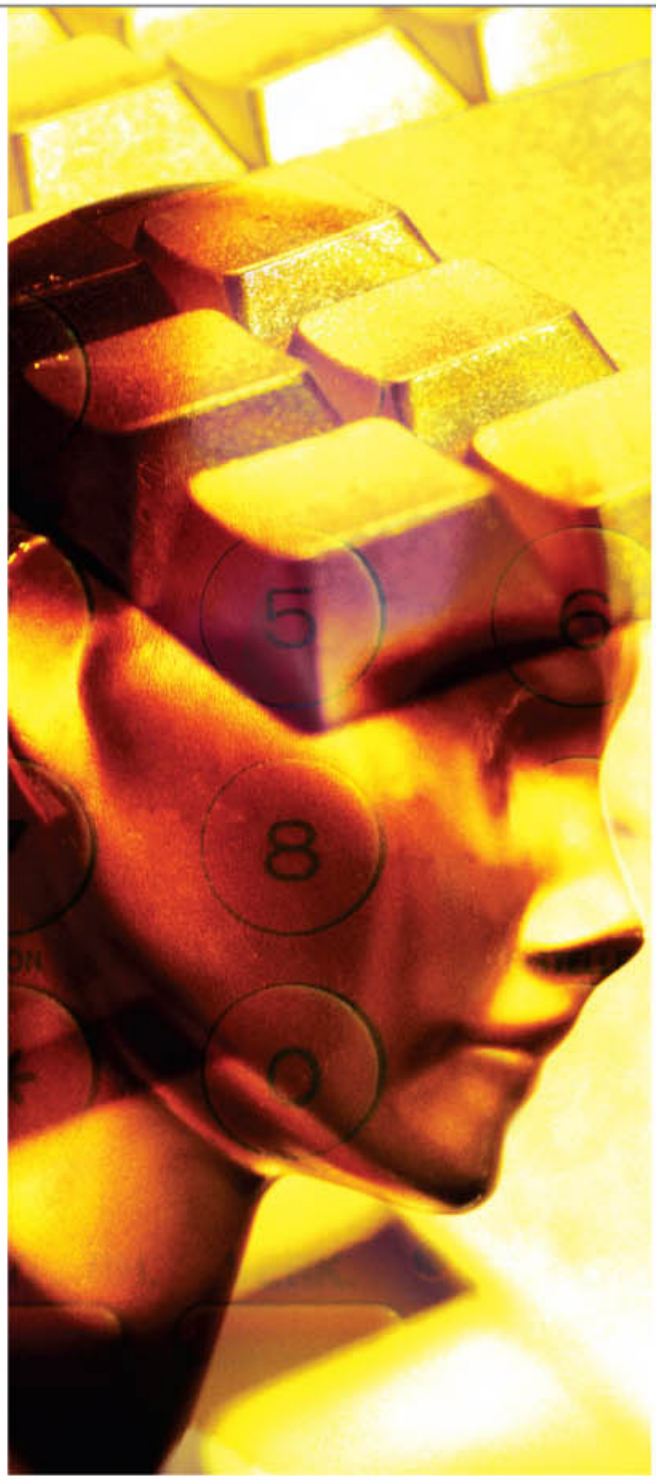
There is a similar feature in Windows XP which is used as RAM expansion. This feature in XP is called pagefile.sys which uses a portion of the hard disk to function as RAM. As far as it is concerned, this pagefile.sys is of a great interest during any forensics investigations because it normally contains abundance of evidences related to a case. Information such as recently opened files, recently run programs and recently accessed websites can also be found inside pagefile.sys. Pagefile.sys is a hidden file and it can be viewed by just "unhiding" the hidden files from the view options of windows explorer.

While SuperFetch loads by default all the necessary files into the main memory, ReadyBoost complements it by loading data into alternate storage devices such as USB 2.0 flash memory sticks. While the USB flash drives are not as fast as the main memory, they can be faster than a hard disk drive and enabling ReadyBoost can free up some of the main memory which could be used for other more important tasks and applications. ReadyBoost mainly functions like an updated version of Windows XP's prefetcher which performs analysis of boot-time disk usage patterns and creates a cache which is used in subsequent system boots. That way, you never lose any previous data that is meant to be written to a hard drive. After all, a flash memory key can get yanked out of a system at any time [windowsvistablog.com, 2008].

The cache which is created by ReadyBoost itself is encrypted using AES-128 encryption [Wikipedia, 2008], so no one can steal the flash memory key and casually browse through the cache file to see what the content is or what the user has been doing. This will surely pose a massive interest and challenge for forensics analysts because ReadyBoost will definitely store loads of important data (evidences) if found at crime scenes. The challenge is now how forensics analysts going to work around the AES-128 encryption and uncover the evidences. When using ReadyBoost-capable flash memory (NAND memory devices) for caching allows Vista to service random disk reads with performance that is typically 80-100 times faster than random reads from traditional hard drives. This caching is applied to all disk content, not just the page file or system DLLs. The speed of CPUs and memory are fast outpacing

that of hard disks, so disks are a common system performance bottleneck. Random disk I/O is especially expensive because disk head seek times are on the order of 10 milliseconds-an eternity for today's 3GHz processors. While RAM is ideal for caching disk data, it is relatively expensive. Flash memory, however, is generally cheaper and can service random reads up to 10 times faster than a typical hard disk [tutorialninjas.net, 2008].

When a compatible device is plugged in, the Windows AutoPlay dialog offers an additional option to use the flash drive to speed up the system; an additional "ReadyBoost" tab is added to the drive's properties dialog where the amount of space to be used can be configured. 250 MB to 4 GB of flash memory can be assigned. Apart from encrypting the content, ReadyBoost also compresses all data that is placed on the flash device; Microsoft has stated that a 2:1 compression ratio is typical, so that a 4 GB cache could contain up to 8 GB of data [Wikipedia, 2008].



Investigating Readyboost

The subsequent experiment was to dig further into Ready-Boost to see if there is any way that the contents of Ready-Boost can be read. Based on many experts' experience, Vista will reject most of the flash drives in the market to be used as ReadyBoost. Later it was found that the reason for this is that there are a few requirements that a flash drive must meet to be compatible with Vista to be used as Ready-Boost. Some of them are such as the flash device must have an access time of less than 1ms, the device must be capable of 2.5MB/s read speeds for 4KB random reads spread uniformly across the entire device and 1.75MB/s write speeds for 512KB random writes spread uniformly across the device. However, we can force Vista to use any flash drives as ReadyBoost by doing some modification to its registry and the how-to can be found on the Internet.

Figure 1 below shows the cache file of ReadyBoost viewed via windows explorer. A file called "ReadyBoost.sfcache" will be created within the USB drive. You will not be able open the file by just double clicking it because Vista protects the file.

Name	Date modified	Type	Size	Tags
System	2/14/2008 4:37 PM	File Folder		
LaunchU3.exe	2/13/2007 9:33 AM	Application	1,084 KB	
ReadyBoost.sfcache	2/19/2008 9:00 AM	ReadyBoost Cach...	1,884,161 KB	

Figure1: ReadyBoost cache file viewed via windows explorer

EnCase Forensics was used to analyze the cache file and Figure 2 below is the result of the analysis. All that can be seen are meaningless, randomly generated characters which indicate that the cache file is encrypted. Based on the articles and write-ups released by Microsoft and various other computer experts, this cache file is encrypted using AES-128 encryption algorithm.

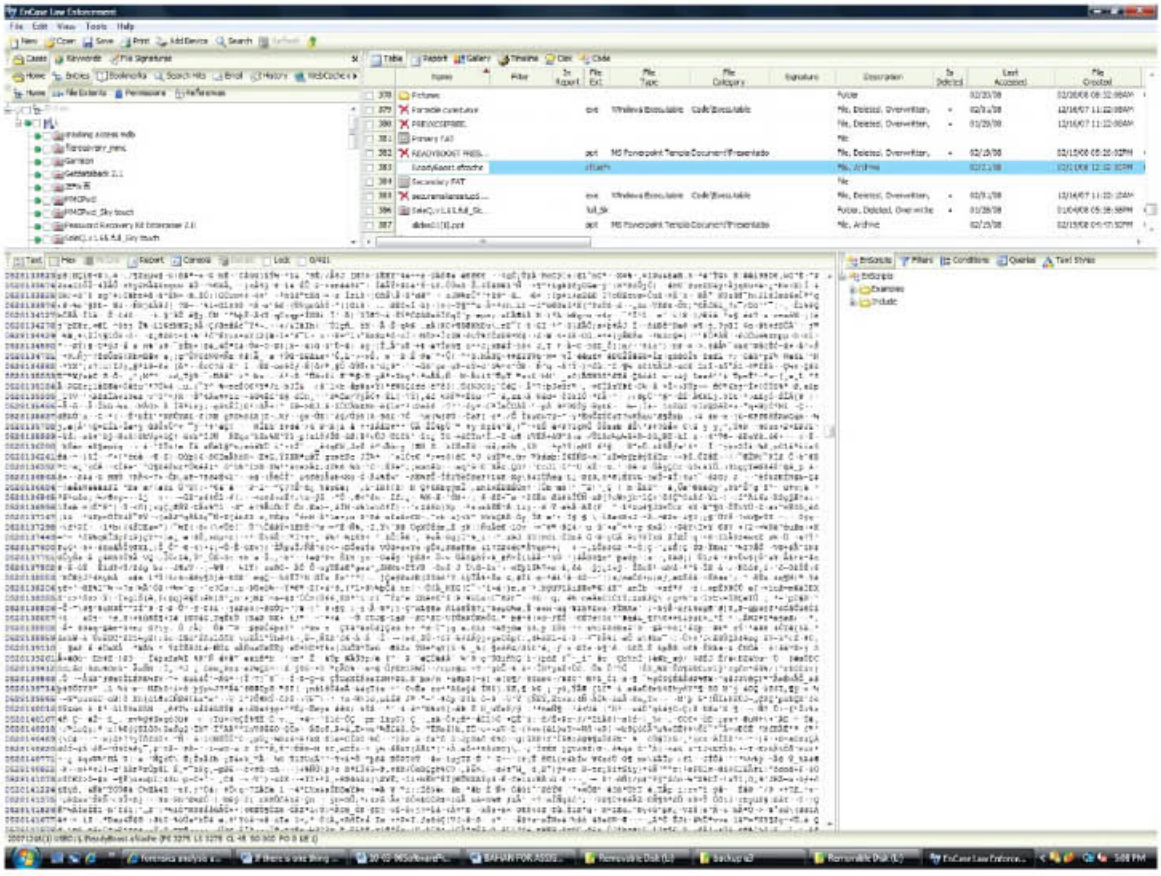


Figure 2: ReadyBoost cache file viewed via EnCase Forensic

Discussion

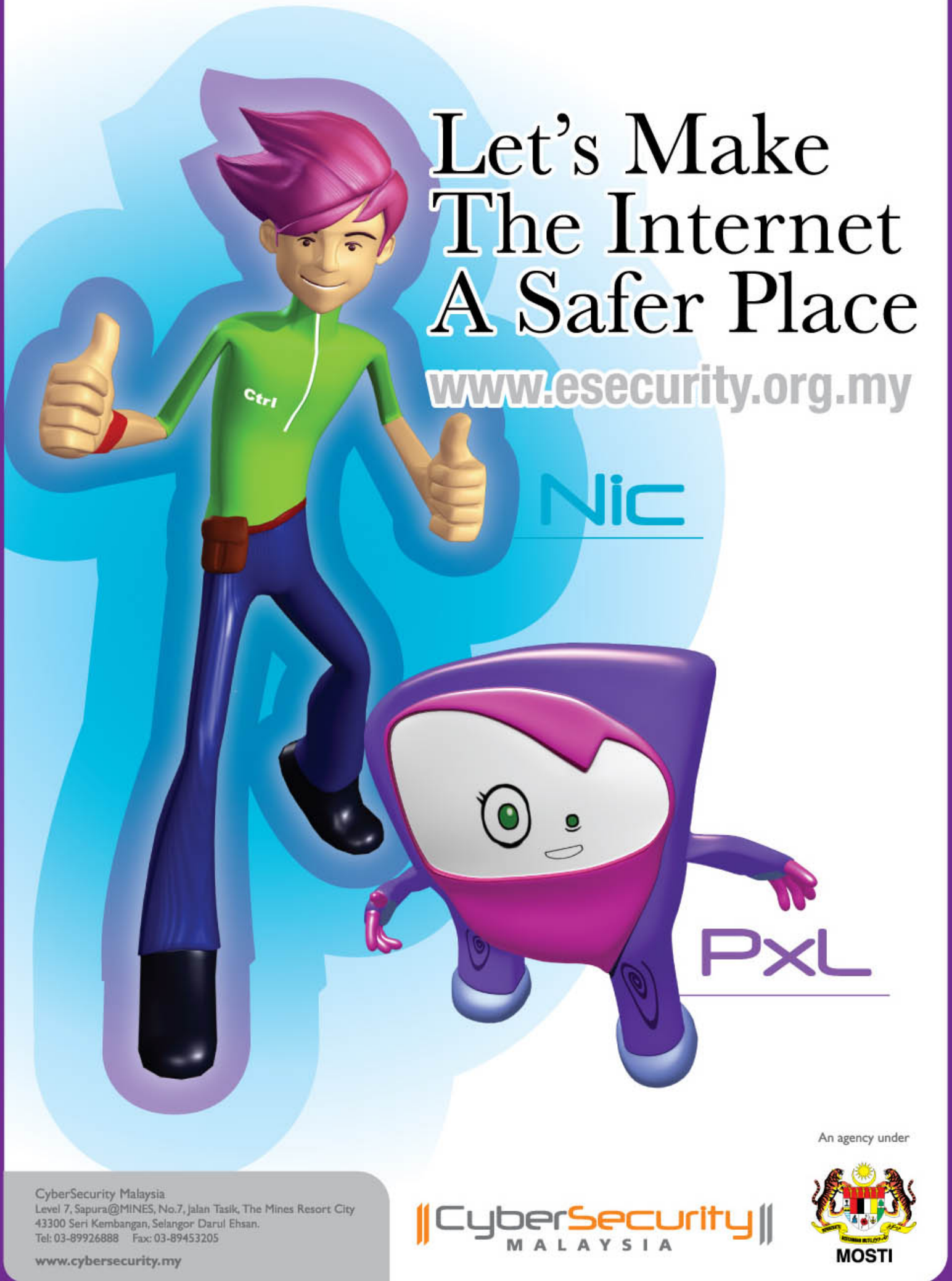
It is proven that ReadyBoost can certainly increase the performance of a Vista machine by caching disk data. This initially seemed like a very interesting prospect from an investigation point of view but it is proven that Microsoft has employed a very strong encryption algorithm; i.e. AES-128 to protect ReadyBoost's content from malicious attacks. AES which stands for Advanced Encryption Standard is being used widely by the US government and theoretically it will take years and some supercomputing power to break it via brute-force attack. According to a discussion on a thread in a forum titled "Bitlocker No Real Threat to Decryption" on Slashdot, no one alive today will be able to break AES-128 at least for the next 50 years and it seems it would take Moore's law approximately 100 years before computer technology is sufficient to break AES.

Since Vista encrypts the whole ReadyBoost cache file with AES-128, it makes a meaningful examination of the device impossible. This will definitely pose as a big danger because perpetrators will definitely find a way to make use of this safe haven to save all the processes ran on the system onto ReadyBoost. Imagine the prospect of perpetrators bypassing the RAM completely and channel all the processes to ReadyBoost leaving no computing trails on the computer. This possibility is very scary because forensics examiners will not be able to analyze the flash drives used as ReadyBoost.

The attempt to analyze or view the contents of a ReadyBoost while it was in use was also not successful. It seems like Vista encrypts the data on ReadyBoost on the fly and leaves no room for anybody to view its contents. As far as we can remember, no one has ever broken the AES-128 encryption and trying to achieve it is definitely a waste of time. However, it is believed that it can be achieved by Microsoft giving a helping hand and work hand-in-hand with law enforcements in investigations involving ReadyBoost.

Conclusion

The much talked about feature in Vista; i.e. ReadyBoost, is something that forensics analysts should be worried about. Since the ReadyBoost cache file is encrypted using AES-128 algorithm, there is no way an analyst could get his / her hands into its contents. It is very worrying that some perpetrators who are computer geeks could easily use this feature to their advantage by directing all the processes to be run from ReadyBoost instead of RAM. If RAM is totally discarded from the computer's operation, forensics analysis for running processes especially in intrusion cases cannot be accomplished.



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

CyberSecurity MALAYSIA

An agency under

MOSTI