

e-Security

Volume 16 - (Q3/2008)



MOSTI



"We need secure products, not security products."

Phil Venables, CISO, Goldman Sachs

Contributors

**MyCERT 3rd Quarter 2008
Summary Report**
MyCERT
CyberSecurity Malaysia

**A Peek at The Digital Forensics
Analysis of Windows Vista's Recycle Bin**
By Sivanathan Subramaniam
Digital Forensics
CyberSecurity Malaysia
siva@cybersecurity.my

**Rogue Security Applications Dominate
Fortinet's Most-Reported Threats for
August 2008**
By Fortinet

**MySQL Forensics – Case Study: Online
Financial Investment**
By Sarah Khadijah Taylor
Digital Forensics
CyberSecurity Malaysia
sarah@cybersecurity.my

Secure Coding
By Hafizah Che Hasan
Security Assurance
CyberSecurity Malaysia
hafizah@cybersecurity.my

**Mobile Phone Forensics: The Tooth
that Leaves Trails – Part 1**
By Razana Md Salleh
Digital Forensics
CyberSecurity Malaysia
zana@cybersecurity.my

**Pengaruh Laman Web YouTube
di Serata Dunia**
By Redy Jeffry Mohamad Ramli
Cyber Media Research
CyberSecurity Malaysia
rjeffry@cybersecurity.my

Towards ISO/IEC 27001:2005 Certification
By Maslina Daud & Raja Azrina
Security Management & Best Practices
CyberSecurity Malaysia
maslina@cybersecurity.my
azrina@cybersecurity.my

OPC Security – Part 1
By Nor' Azuwa Muhamad Pahri &
Mohammad Noorhisyam Muda
Security Assurance
CyberSecurity Malaysia
azuwa@cybersecurity.my
noorhisyam@cybersecurity.my

ISSN 1985-1995



9 771985 199003

From the Editor's Desk

vphilip@cybersecurity.my

First of all, a belated Selamat Hari Raya from all of us here at CyberSecurity Malaysia. Over here the atmosphere was truly in the Raya mood with decorations and lights. Just waiting for our "makan-makan" kuih raya soon.

Well, Quarter 3 has passed by and I guess it was a quieter month as we saw the Holy Ramadhan month. For us here at CyberSecurity Malaysia was a time for us to sit and do some planning for the year to come.

So, what did we see happening during Q3? Well, we participated at MOSTI's Minggu Sains & Teknologi (MISTI) in Sabah. I must say that it was a good event with the opening by MOSTI's minister, Y.B. Datuk Dr. Maximus Johnity Ongkili. CyberSecurity Malaysia had participated at the exhibition that was held at Sabah's 1-Borneo Mall. During the 4-day event, we had also conducted 2 awareness talks for the general public.

In August we had also conducted our CISSP & SSCP classes. The class was conducted by (ISC)2 certified instructor, Mr. Graham Dobson. All in all we had a great class and many practical sessions were conducted by the instructor for the class. Do check our training calendar for exam and class dates on our website at <http://www.cybersecurity.my>.

Check out our training calendar later for 2009 where we will be introducing many new programs. Some new programs include Network Security, Wireless Security, Web Application Security and Business Continuity. We will be conducting our first Web Application Security class in December that is conducted by an international expert, Mr. Kenneth Van Wyk. Seats are limited, so make sure you get yours. Also we will be having our last CISSP & SSCP exam on the 20th December 2008, so register early to get the early bird pricing.

Another update is that CyberSecurity Malaysia is now an authorised SANS Exam Centre here in Malaysia. So, if any of you would want to sit for any of SANS Institute exams, you can now do it at CyberSecurity Malaysia.

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

Table of Contents

- 03 MyCERT Q3 2008 Quarterly Summary Report
- 10 A Peek at the Digital Forensic Analysis of Windows Vista's Recycle Bin
- 16 Rogue Security Applications Dominate Fortinet's Most-Reported Threats for August 2008
- 18 MySQL Forensics - Case Study: Online Financial Investment

A Message from the Head of CyberSecurity Malaysia

Selamat Hari Raya to all our Muslim readers. Once again, it is my pleasure to address you all in this quarterly issue of the e-Security Newsletter.

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 intrusion incidents especially. Majority contributed to web site defacements. Please refer to our website for advisory on recovery and mitigation methods.

We also see that fraud and hack threats have also risen. I would like to say that cyber attacks are becoming more complex and we need to take extra measures to mitigate them. CyberSecurity Malaysia provides advisory and technical assistance to organisations and individuals on cyber security.

We are also making great efforts in developing more security professionals in the country in our efforts to make the cyber space a safer place. In our latest effort, we have been appointed by BCI, UK to be the official affiliate here in Malaysia in producing more professionals in the field of Business Continuity. Security professionals can also sit for SANS exams here at CyberSecurity Malaysia as we are now the official authorised exam centre.

Moving forward, subscribe to our mailing list to be informed of the latest threats, cyber security related events, happenings so that we will be current in this area so as to be alert on addressing new threats. This is vital in facing today's cyber security challenges.

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

- 24 Secure Coding
- 28 Mobile Phone Forensics: The Tooth that Leaves Trails - Part 1
- 32 Pengaruh Laman Web YouTube di Serata Dunia
- 34 Towards ISO/IEC 27001:2005 Certification
- 37 OPC Security - Part 1

READER ENQUIRY

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

PUBLISHED BY

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

PRODUCED BY

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-137.072008: MyCERT Quarterly Summary (Q3) 2008

Original Issue Date: 14th October 2008

03.

Introduction

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

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

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

Incident Reports

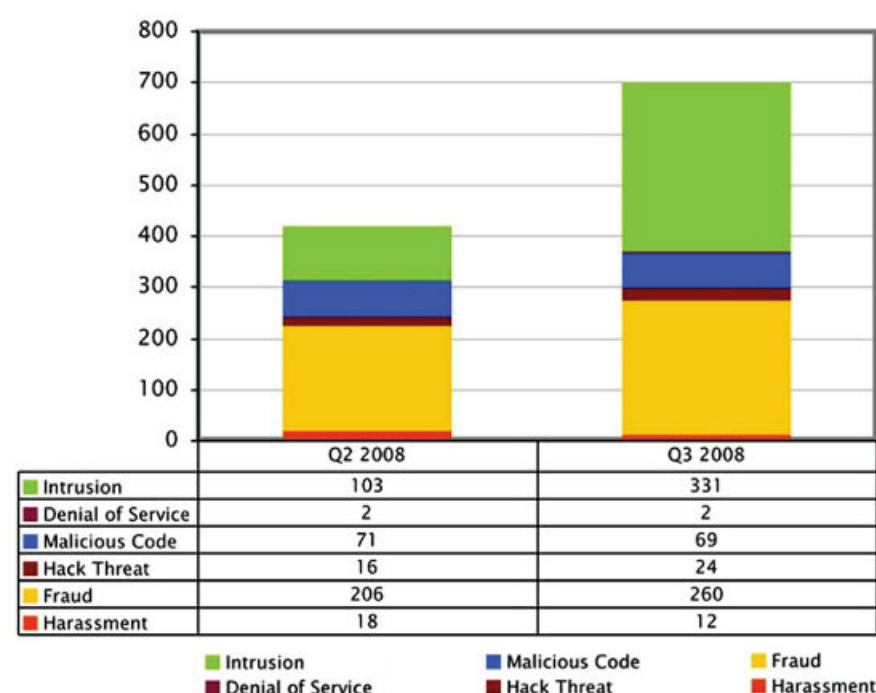
In the second quarter of 2008 (Q3), a total of 21661 incidents, inclusive of spam incidents, were reported to MyCERT representing a 26.73% increase of incidents compared to Q2 in 2008. The majority of the incidents reported this quarter is contributed by spam reports. There was a tremendous increase in intrusion incidents involving web defacements, which exploited various flaws in web applications. However, there were no critical outbreaks in terms of malware or exploitation that had raised red alert or crisis in our constituency. Most categories of incidents reported had increased and on the other hand, malicious code and harassment incidents had decreased. Denial of Service incidents remained same as in the previous quarter.

Attached is the Table of Figure showing the comparisons between number of reports received in Q2 2008 and Q3 2008.

	Q2 2008	Q3 2008	%
Harassment	18	12	-33.33
Fraud	206	260	26.21
Hack Threat	16	24	50
Malicious Code	71	69	-2.82
Denial of Service	2	2	0
Intrusion	103	331	221.36
Spam	16542	20963	26.73
Total	16958	21661	27.73

Table of Figure for Q2 2008 and Q3 2008

The following graph shows the number of incidents handled according to the different categories in Q2 2008 and Q3 2008:



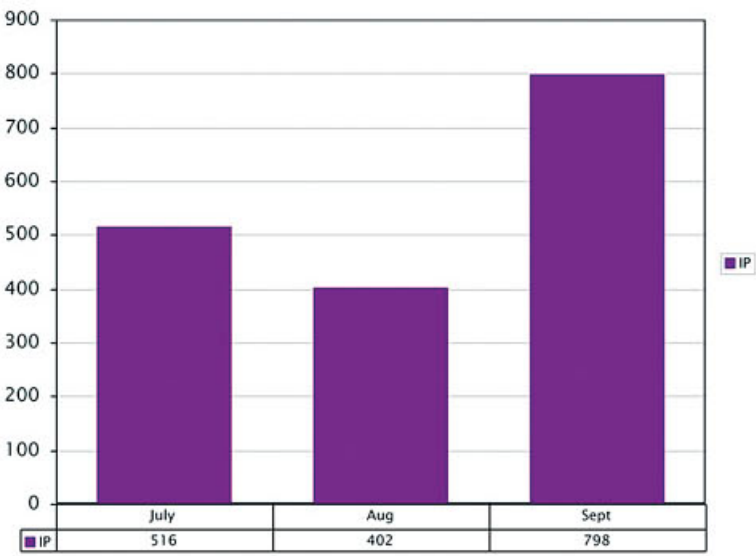
Comparison of incident statistics between Q2 2008 and Q3 2008

Malicious Codes

A total of more than 1000 Malaysian IP addresses were handled in the 69 incidents reported to MyCERT. In this quarter, we received several reports from foreign Computer Emergency Response Teams (CERTs) and security organizations regarding bots infected machines (drones), command & control server of botnets and malicious files hosted on computers in Malaysia. Some of these reports contained IP addresses, most of which are home users network that had been reported to us previously. In all these instances, MyCERT had notified and assisted the respective ISPs on bot removal and mitigation strategies.

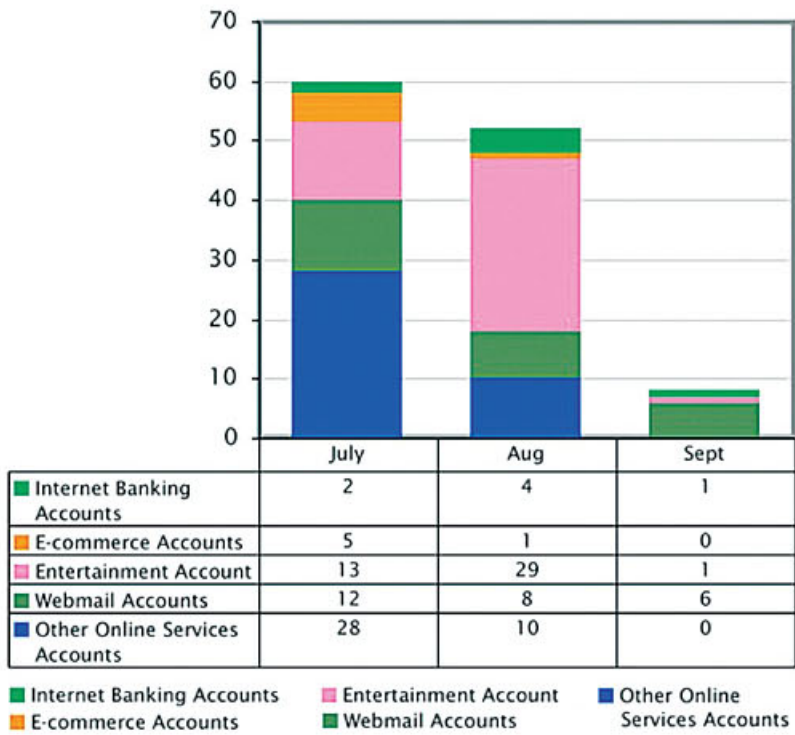
These bots or zombies are normally used to carry out malicious activities such as spamming, executing denial of service attacks, hosting phishing sites and spreading malware.

In this quarter, MyCERT received reports of 1716 IP addresses that were believed to be infected with bots and being used as drones of one or more botnets. The following graph shows the number of IP addresses belonging to Malaysian constituency that had been infected with bots in Q3, 2008.



Statistics on total Malaysian IPs infected with Drones for Q3 2008

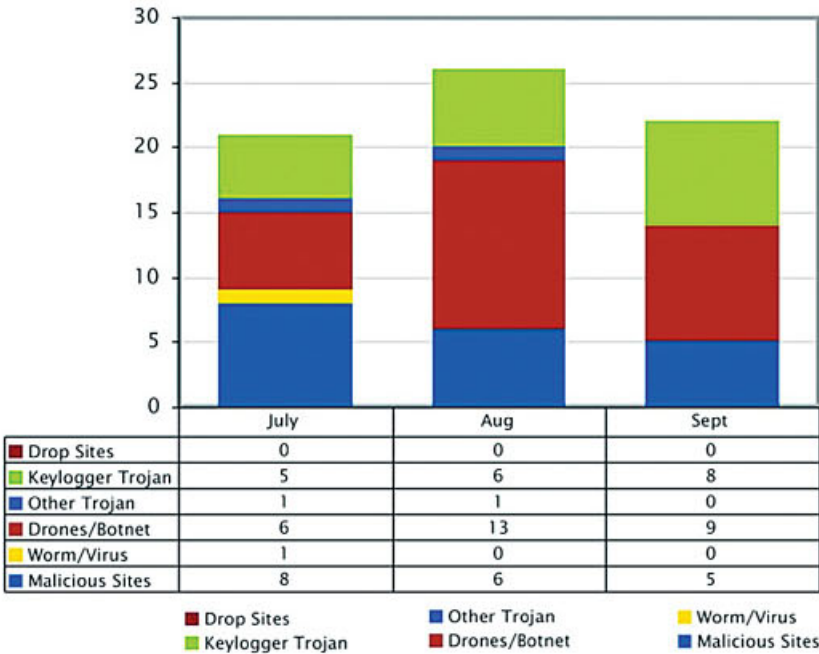
MyCERT received 19 reports from foreign a CERT regarding details found on a server which was used by a trojan to log keystrokes. The keylogger Trojan, named the Nethell Trojan, had successfully captured keystrokes of usernames/passwords belonging to various internet accounts in our constituency, which includes accounts belonging to internet banking, webmail, entertainment, e-commerce and other online services. In this quarter we observed 120 accounts related to the above categories were compromised by keylogger activities as shown in the graph below.



Statistics on types of accounts compromised due to keylogger activities for Q3 2008

MyCERT had notified the respective parties for immediate rectifications on the compromised passwords.

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



Breakdown of types of malware incident in Q3 2008

We advise users to safe-guard their computers against being infected by malicious software. Please visit the following URL to view some tips on this topic:

<http://www.esecurity.org.my/adult-malware.htm>



Hack Threat

MyCERT received 24 reports for the category of hack threats in this quarter which represents a 50% increase compared to the 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 scanings and other malicious or suspicious activities that had triggered alerts.

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

Denial of Service

In this quarter, MyCERT received 2 reports on denial of service which is same as in the previous quarter. Denial of service attack consists of sending huge traffic, continuously to a system, causing the system to slowdown or being choked. In distributed denial of service attacks, the source of the attacks mostly originated from various spoofed multiple IPs and majority of denial of service attacks originate from 1 single IP address. The majority of denial of service attacks were successfully handled or stopped by blocking the source of the attacks at the customers' upstream router.

Intrusion

MyCERT had received 331 reports related to intrusion in this quarter, which represents more than 100% increase compared to the previous quarter. The majority of the incidents in this category were web defacements (or re-defacements in some incidents) of .my websites hosted in Malaysia. Besides that, there were also reports of mass defacements of .MY websites hosted on virtual hosting servers.

In this quarter a total of 322 .my sites belonging to various sectors and running on various platforms were defaced. Majority of the web defacements in this quarter was due to Joomla! reset password vulnerability. Joomla! is a popular content management systems based on PHP and is widely used to deploy portals in the country. MyCERT had released an alert on this vulnerability to all System and Web Administrators to patch or upgrade to the latest version of Joomla!

The alert is available at:

MA-136.082008: MyCERT Special Alert - Critical Joomla! reset password vulnerability

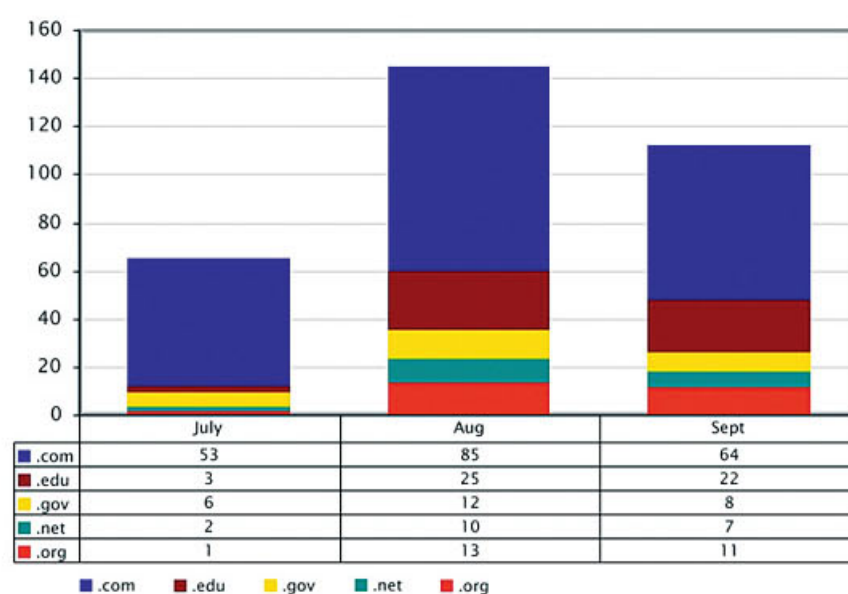
<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/595/index.html>

Besides the above vulnerabilities, some of these defacements were also caused by other web application vulnerabilities such as remote file inclusion, SQL injection and unpatched third party add-ons.

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

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

MyCERT had also produced statistics on breakdown of defaced .MY sites by domains, as seen on the right:



Statistics on .MY web defacement by domains for Q3 2008

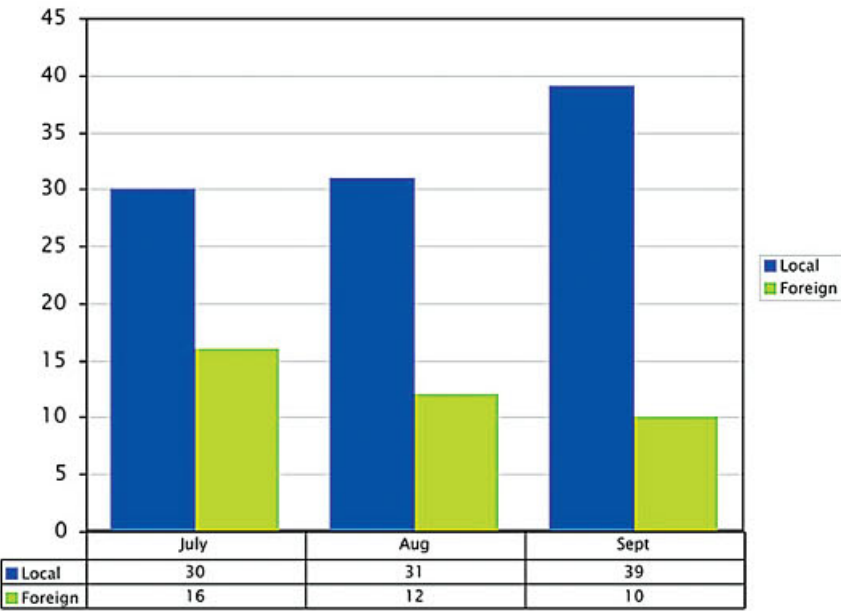
Harassment

MyCERT had handled 12 incidents under the category of harassment this quarter. The nature of the harassment cases includes email threats to defamatory messages/pictures/photos on internet forums and social networking websites. The majority of harassment cases were handled successfully.

Fraud

There is an increase in terms of the number of reports involving fraud reported to MyCERT this quarter with an increase to about 26.21%, which comprised of 260 reports compared to 206 reports in previous quarter. Majority of fraud incidents reported were phishing incidents -involving local and foreign financial institutions or brands. In this quarter, we observed a surge on phishing reports which includes reports on phishing emails and phishing sites impersonating local/foreign financial institutions or brands.

“ MyCERT had received 331 reports related to intrusion in this quarter, which represents more than 100% increase compared to the previous quarter.”



Breakdown of phishing sites between local and foreign brands in Q3 2008

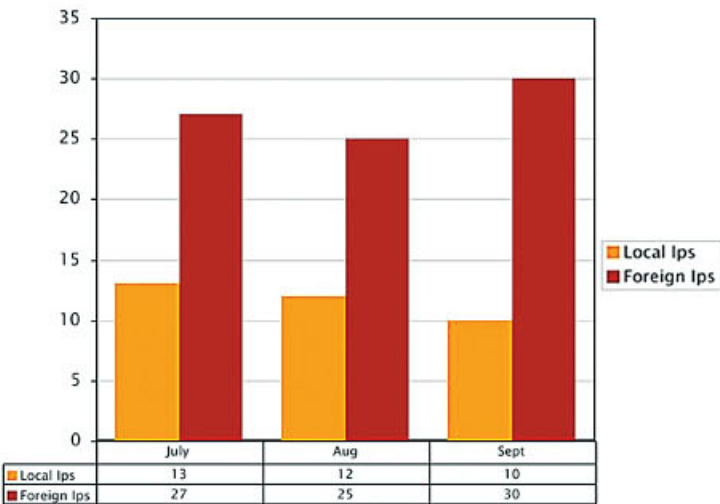
A tremendous increase in phishing sites that targeted local financial institutions was recorded in this quarter with more than 50 phishing sites. We observed phishers actively using the fast-flux techniques for a more advanced and sophisticated phishing tactics. In normal phishing attacks, the domain in the phishing link for example [www.abc.com](#) will resolve to IP w.x.y.z, which is the IP address of the evilserver. When users click the phishing link, they'll be connected directly to it. However, in fast-flux, attackers can abuse round-robin DNS, sending responses for [www.abc.com](#) and mapping the site to several IP addresses.

Details on fast-flux is available at:

 http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1288441,00.html

MyCERT had handled the phishing reports by communicating with respective parties and in most instances, the phishing sites were put offline or removed to shutdown within 24 - 48 hours.

We also observed in this quarter, 35 IP addresses belonging to local constituency that were found to be hosting phishing sites that imitated foreign financial institutions and 85 IP addresses belonging to foreign constituency were found to be hosting phishing sites imitating local financial institutions, as shown in the below graph.



Statistics on phishing sites hosted on local and foreign IP address

Based on our observation, we believe majority of IP addresses hosting phishing sites belong to compromised hosts and may had been infected with bots. We had advised the respective administrators to investigate and rectify the affected hosts accordingly before it is put online.

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

In this quarter, we had also received several reports on cheating cases involving online transactions. MyCERT would like to advise users to be extra careful when they plan to purchase items online to avoid being cheated by irresponsible parties. They must be extra careful with whom they are dealing when purchasing the item. It is also advisable to purchase items with authorized or licensed online traders who can guarantee the delivery of items to buyers.

Besides this, we had also received several reports involving "Nigerian scam". MyCERT advise users to be extra careful when dealing with people who request cash or deposits as pre-requisites for a particular transaction. They must not bank-in any money to unknown parties without proper verification.

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

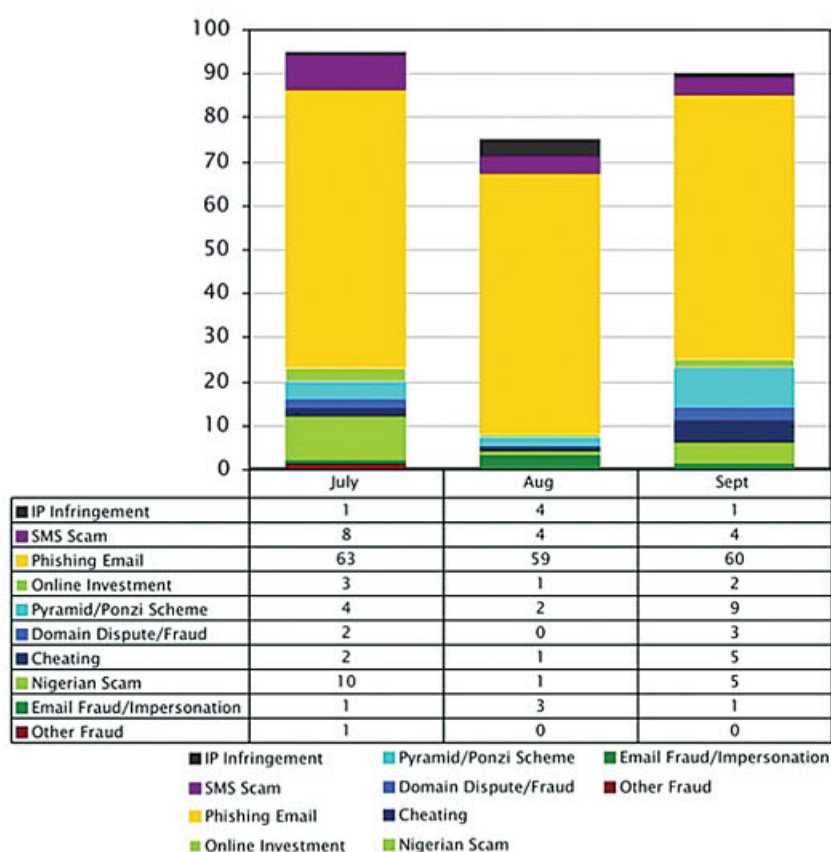
Tips and Guidelines on Scam Preventions

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

In this quarter, MyCERT had handled 7 incidents involving issues or disputes related to domain names. The issues/disputes involved mainly suspicious activities. MyCERT had advised the affected organizations to obtain Legal advise from their Legal Department by referring to the relevant domain dispute resolution policies before taking any action.

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





Breakdown of types of fraud incidents in Q3 2008

Vulnerabilities Reported

In this quarter MyCERT also received 9 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 owners to fix the vulnerabilities to prevent any unwanted incidents.

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

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

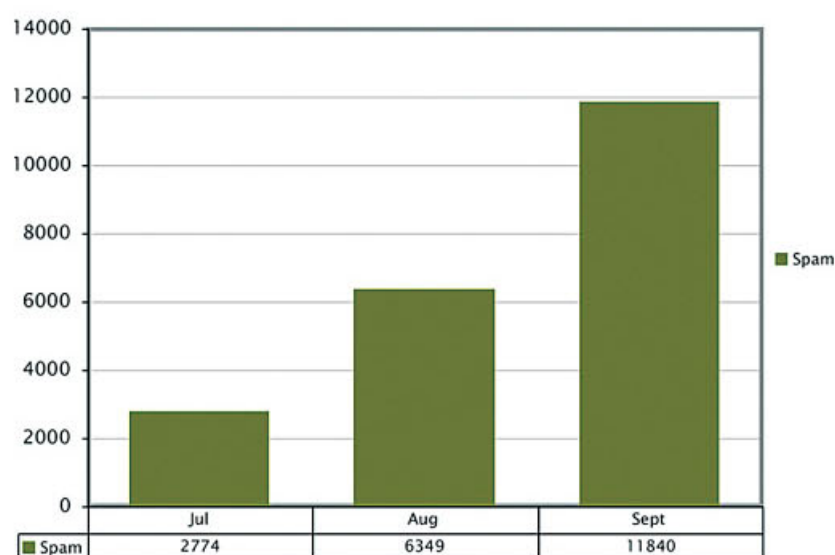
Spam Watch

MyCERT had observed that spam related incidents had increased to 26.73% in this quarter compared to the previous quarter. A total of 20963 incidents were received compared to 16542 reports in the previous quarter. Spam incidents remains as the incident with highest number of reports received compared to other incidents.

From our observation based on the monthly spam statistics, we noticed spam emails were higher when there is an outbreak of a certain security threat. The top categories of spam emails detected for this quarter are the mass mailer worm emails which recorded the highest, trojan emails and phishing emails. Majority of mass mailer worm emails are related to the different variants of Mytob worm, the Mytob.KQ and Mytob.NK. Most of Trojan emails are related to the Trojan.Fakealert and Trojan.Goldrun. Phishing emails mainly involved spoofed domains related to banks.

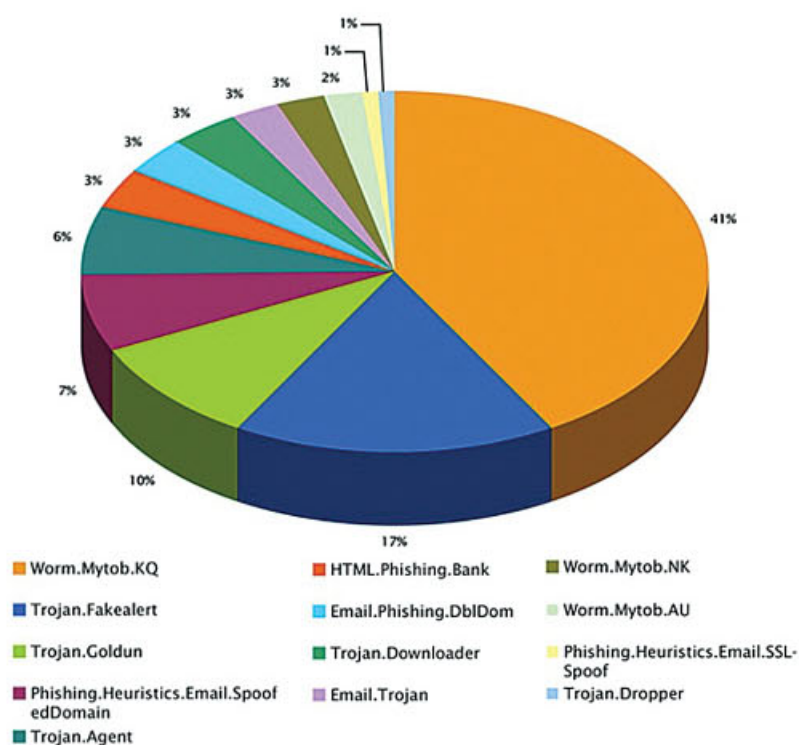
Other categories of spams are related to scam emails such as the Nigerian scam, Lottery scam, get rich schemes. Promoting or selling of products/services still remains as one of the main contributor to spam.

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 as this serves only to further propagate spam activities. MyCERT encourages users to report spam so that proper action can be taken against the owner of the computer sending out the spams.



Statistics on spam incident in Q3 2008





Spam payload detected by ClamAV in Q3 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:

MA-140.092008: MyCERT Special Alert - Festive Season and Long Holiday Alert (26/09/2008)

<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/607/index.html>

MA-139.092008: MyCERT Special Alert - Vulnerability in WordPress blog publishing application (23/09/2008)

<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/602/index.html>

MA-138.092008: MyCERT Special Alert - Vulnerability in Microsoft Windows GDI+ (22/09/2008)

<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/601/index.html>

MA-136.082008: MyCERT Special Alert - Critical Joomla! reset password vulnerability (14/08/2008)

<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/595/index.html>

MA-135.072008: MyCERT Special Alert - Multiple Vendor DNS vulnerabilities (25/07/2008)

<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/594/index.html>

MA-134.072008: MyCERT Special Alert - Vulnerabilities in Microsoft Products (15/07/2008)

<http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/591/index.html>

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

US-CERT: Mozilla Releases Firefox 3.0.2 (24 September 2008)

http://www.us-cert.gov/current/index.html#mozilla_releases_updates_to_vulnerabilites

US-CERT: Cisco Releases Security Alerts (24 September 2008)

http://www.us-cert.gov/current/index.html#cisco_releases_security_alerts

AL-2008.0082 - DNS cache poisoning vulnerability information allegedly leaked to the public (22 July 2008)

<http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/593/index.html>

US-CERT: Microsoft Office Snapshot Viewer ActiveX Vulnerability (07 July 2008)

<http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/592/index.html>

Activities from Research Network

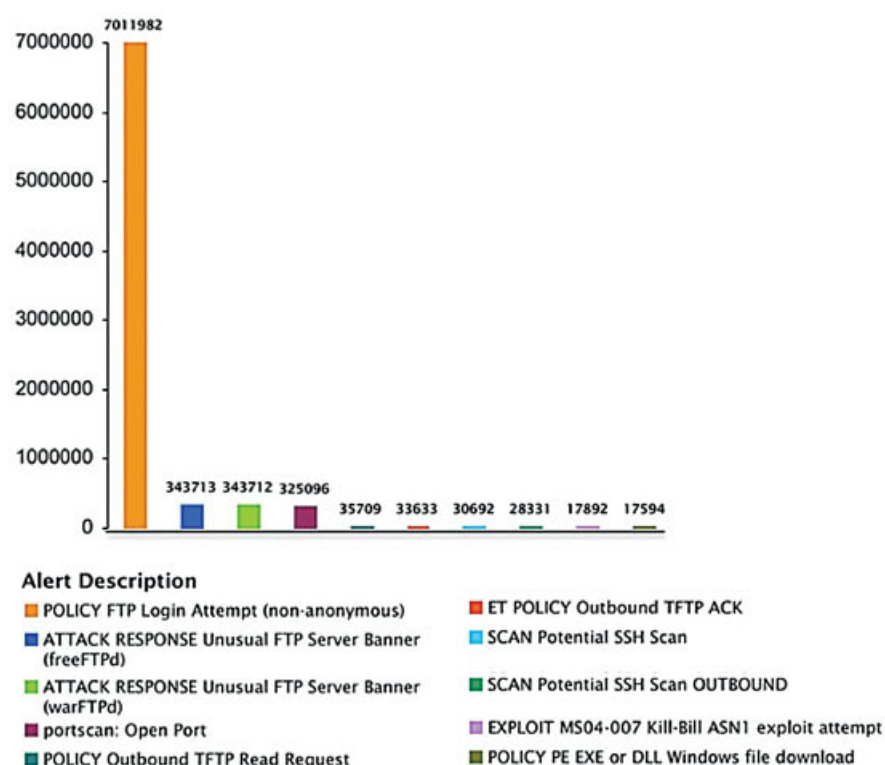
The CyberSecurity Research Network monitoring objectives are:

- 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.

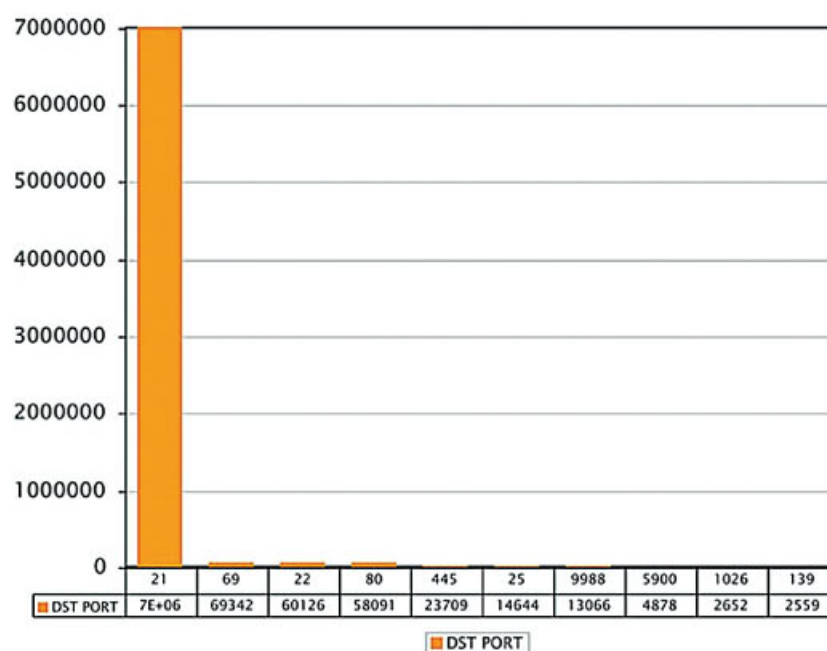
The following is a summary derived from MyCERT's research network for Quarter 3 2008.

The top alert generated by our research network is FTP Login Attempt (non-anonymous), Attack Response Unusual FTP Server Banner (freeFTPD) and Attack Response Unusual FTP Server Banner (warFTPD). While the top ten TCP Destination Port Scanned graph show FTP port is the highest port being scanned at the Research Network environment.

Based on our observation, this is a common port that is constantly scanned by attackers. It showed that port FTP is the most common port targeted for malicious or hacking activities. Port FTP is being targeted because of being part of the most popular file upload mechanism while misconfigured FTP servers can turn global /tmp directory for people to share data with each other for example "warez".



Top 10 alerts generated by our sensor



Top 10 destination ports attacked in Q3 2008

Conclusion

Overall, the number of incidents reported to MyCERT had increased by 27.73% compared to the previous quarter with incidents mainly contributed by spam incidents. Other reports that contributed highly to the number of incidents received this quarter are intrusion, fraud, malicious codes which consists of reports of botnets, command and control & command server, drone activities hosted on local machines. MyCERT would like to advise system and security administrators to take precautions on these activities and prevent their machines from becoming 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:

Postal Address

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

Business Hours

Mon - Fri 08:30 -17:30 MYT

Phone

+603 - 89926969

(monitored during business hours)

Handphone

+6019 - 2665850

(24x7 call incident reporting)

SMS

+6019 - 2813801

(24x7 SMS reporting)

Fax

+603 - 89453442

(monitored during business hours)

Email

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

Feedbacks can be directed to MyCERT.

Produced on 14 October 2008 by MyCERT, CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI).

Revision History:

Initial Release 14 October 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>

A Peek at the Digital Forensics Windows Vista's Recycle Bin

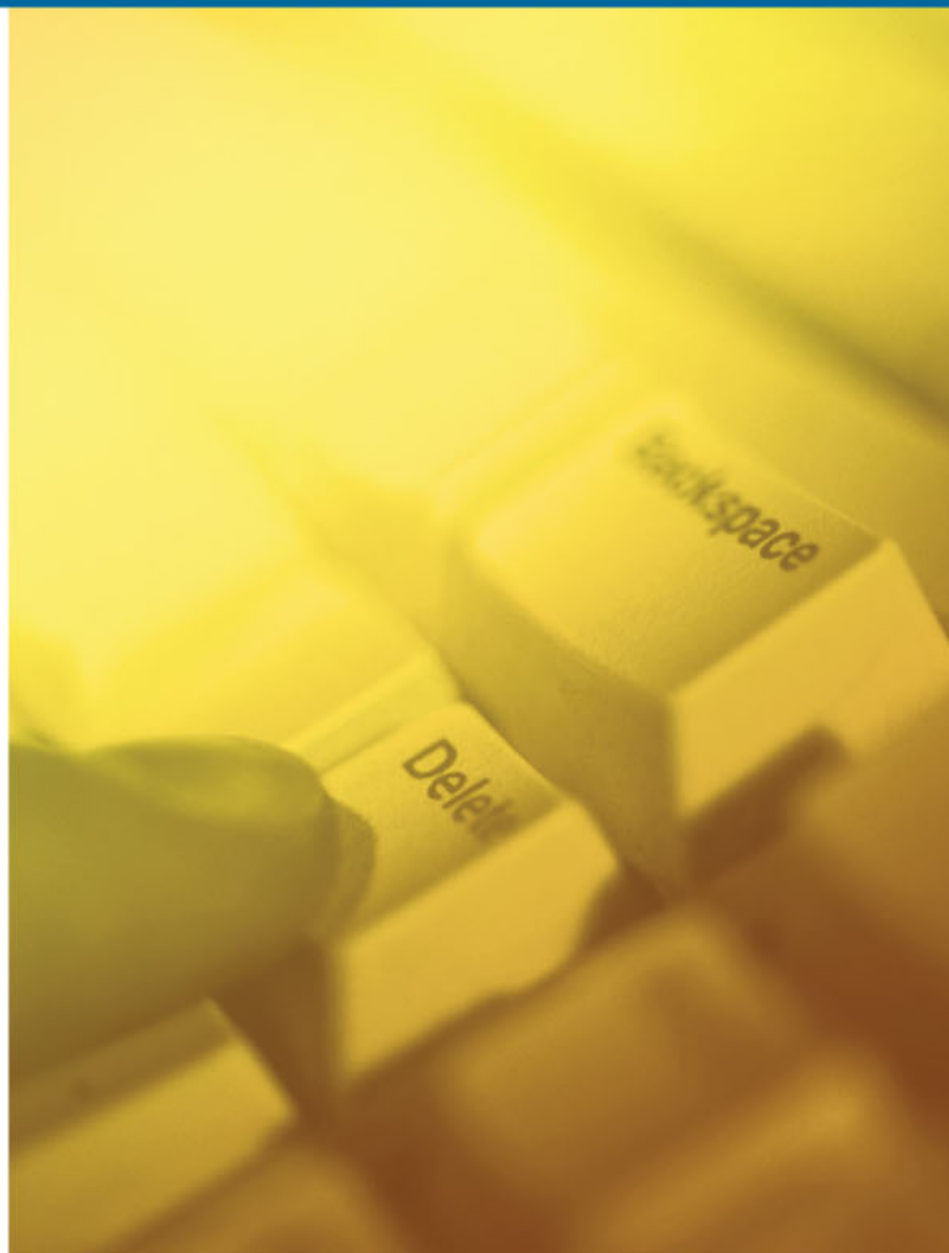
Introduction

Microsoft introduced Recycle Bin in Windows 95 operating system. The Recycle Bin keeps files that have been deleted, whether accidentally or intentionally. Users can review the contents of the Recycle Bin before deleting the items permanently. In previous Windows operating systems and in MS-DOS, undeletion was the only way to recover accidentally deleted files. The Recycle Bin holds data that not only lists deleted files, but also the date, time and the path of those files. The Recycle Bin is opened like an ordinary Windows Explorer folder and the files are viewed similarly. Deleted files may be removed from the Recycle Bin by restoring them with a command, or by deleting them permanently [Wikipedia, 2008].

Apparently Microsoft has changed the underlying structure of Recycle Bin on Vista in comparison to XP which will effectively change the way forensics analysts work. No longer does the Recycle Bin rely on a single INFO / INFO2 file as a database for the Recycle Bin. Instead, an index / deleted file pair now resides in the Recycle Bin [conservativebooktalk.com/forensic, 2008]. The recycle bin is a very important location on a Windows file system to understand. It can help analysts when accomplishing a forensics investigation as every file that is deleted from a Windows recycle bin aware program is generally put in the recycle bin. The recycle bin is a hidden folder on the system and can be accessed from the root directory [SANS Institute, 2007].

In Windows XP, when a user deletes a file, his unique **SID (security identifier)** will be used to create a subfolder in the "Recycler" directory the first time he deletes a file. Also, internal to the directory is another hidden binary file called INFO2 that maps the recycle bin filename to the time and date that the file was deleted as well as the true filename of the file.

Take note that the files in the recycle bin are not named by their normal names that they were deleted by. The names of the files and the paths are kept in another file. The time and date stamps on the files though will be the same. The deleted time can be viewed by the Recycle Bin Utility; there are a number of tools available on the Internet that can be used to analyze recycle bin.



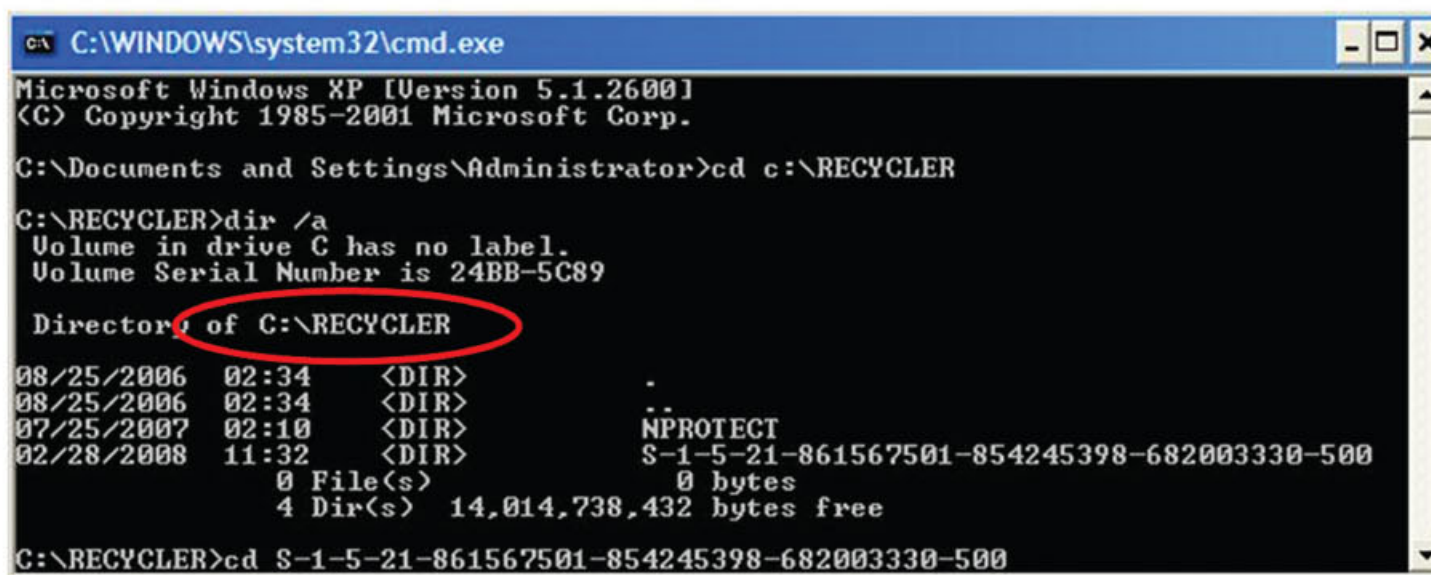
As mentioned earlier, there is a hidden file in the recycle bin directory under each specific SID directory that was created during a file deletion. This hidden file, named INFO or INFO2 contains the full path name, time and date of the files that are in the directory. When Windows explorer sends a file or folder to the recycle bin, the item's data clusters do not move. Instead, explorer simply moves the item's directory entry into the appropriate physical bin folder on the same drive, and then renames the directory entry. Windows stores the original names and locations in a hidden index file named INFO2, which is stored in each physical bin folder. The names of items within folders sent to the recycle bin are not changed and are not stored in the index file [SANS Institute, 2007].

c Analysis of

One may ask what happens if the INFO2 file was deleted? Well, all is not lost if the suspect emptied his/her recycle bin thus removed any contents that may be sitting in the INFO2 file. It is possible to perform HEX based searches on the image by looking at the file and searching for similar fragments on the system. We know that the INFO2 file has dates, times and the original filename [SANS Institute, 2007].

Investigating Vista's Recycle Bin

A quick look at the XP's recycle bin shows that XP stores deleted files under `C:\Recycler\<User SID>` (refer to figure 3.23 below). It is a known fact that XP does not create a recycle bin folder for a user until the user deletes a file for the first time on the machine.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd c:\RECYCLER

C:\RECYCLER>dir /a
Volume in drive C has no label.
Volume Serial Number is 24BB-5C89

Directory of C:\RECYCLER
08/25/2006  02:34    <DIR>          .
08/25/2006  02:34    <DIR>          ..
07/25/2007  02:10    <DIR>          NPROTECT
02/28/2008  11:32    <DIR>          S-1-5-21-861567501-854245398-682003330-500
               0 File(s)              0 bytes
               4 Dir(s)  14,014,738,432 bytes free

C:\RECYCLER>cd S-1-5-21-861567501-854245398-682003330-500
  
```

Figure 3.23: XP stores deleted files under `C:\Recycler\<User SID>`

So how do we determine which recycler belongs to which user? The Security Identifier (SID) which looks something like `S-1-5-21-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxx` is used to differentiate the users. The last 3 or 4 digits of the SID are the significant digits to differentiate the users. If the SID ends with `-500` then it belongs to the administrator user. If they end with `-50x` (x can vary from 1 to 9) then they are the built-in Windows accounts. The user accounts end with `-100x` (x can vary from 1 to 9).

A peek at Vista’s recycle bin revealed some information on the changes implied on Vista by Microsoft. Figure 3.24 below shows the Vista’s recycle bin.

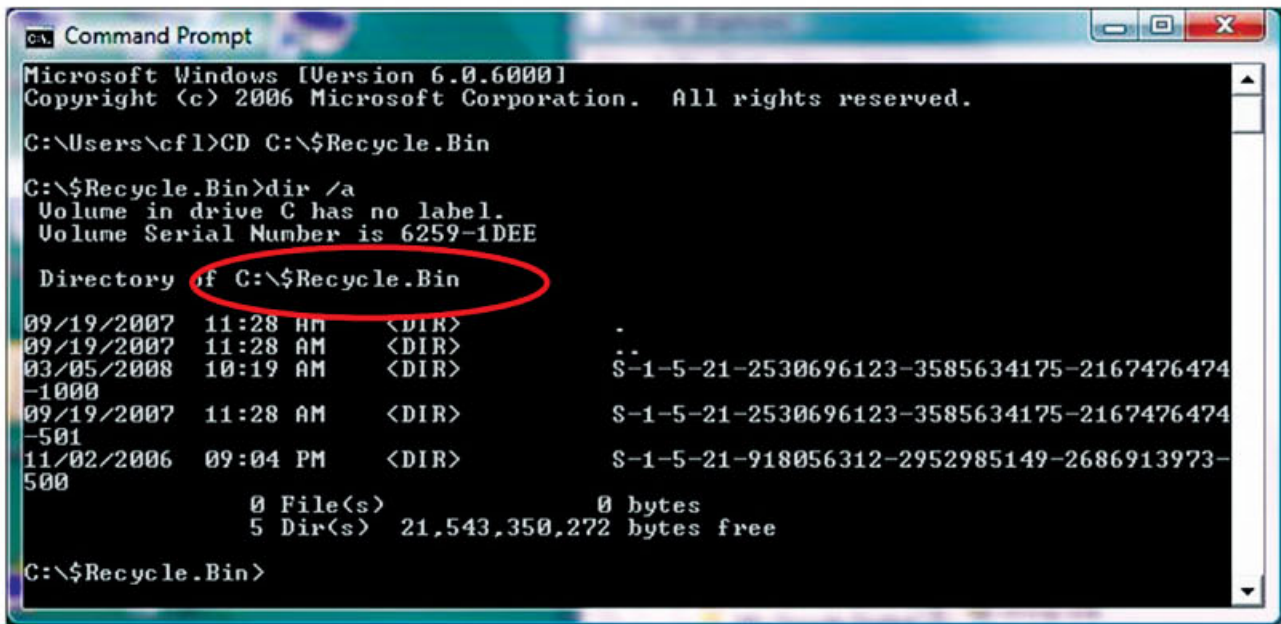


Figure 3.24: Vista stores deleted files under C:\\$Recycle.Bin\<User SID>\

On Vista the recycle bin folder is called \$Recycle.Bin and no longer Recycler. However, other attributes such as the SID orientation all remain similar to XP. Note that the -500 account is the administrator account and the -1000 account is the main user account. Figure 3.25 below is Vista’s recycle bin viewed via EnCase.

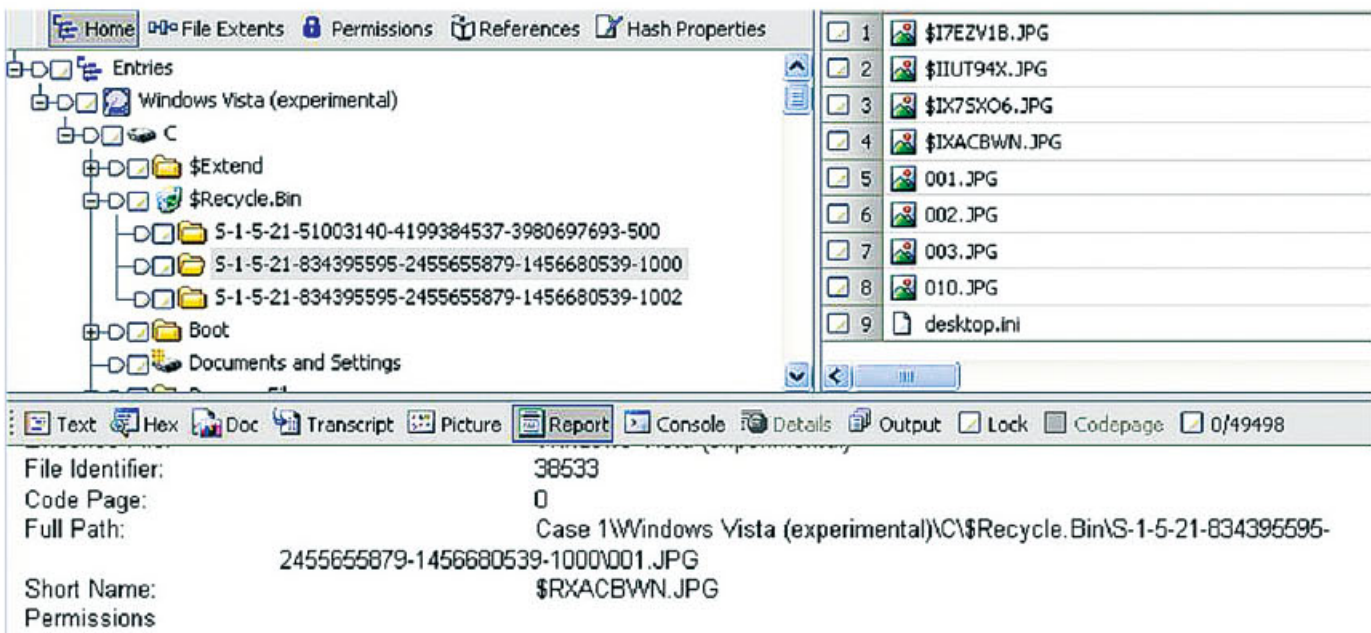


Figure 3.25: Vista’s recycle bin viewed via EnCase

Now, let’s investigate how deleted files are managed in each OSes? Figure 3.26 on the right shows the inside of a XP’s administrator recycle bin. Note that each deleted files receives a new name. File extensions remain unchanged but the filename change to something like DCxx.<ext> (x can be a digit from 0 to 9 which signify some sort of sequential number). A file named “Tax97.doc” may appear as “Dc17.doc” in the Recycler. If a user deletes another text file, then the deleted text file will appear as “Dc18.txt”. There are a few suggestions for the “DC” naming convention. Some experts suggested that the letter “D” stands for “deleted” and the letter “C” indicate the drive or partition the file was deleted from. Some also suggested that the letter “D” stands for the name “drive” and the letter “C” for the drive or partition that the file was deleted from.


```

C:\WINDOWS\system32\cmd.exe
C:\RECYCLER\S-1-5-21-861567501-854245398-682003330-500>dir /a
Volume in drive C has no label.
Volume Serial Number is 24BB-5C89

Directory of C:\RECYCLER\S-1-5-21-861567501-854245398-682003330-500

03/05/2008  18:04    <DIR>          .
03/05/2008  18:04    <DIR>          ..
02/05/2008  14:06             3,573,176  Dc23.mp3
02/05/2008  14:05             4,417,664  Dc24.mp3
01/22/2008  11:10             3,259,459  Dc42.zip
01/22/2008  10:24    <DIR>          Dc50
02/01/2008  11:39    <DIR>          Dc51
01/30/2008  16:15             788  Dc52.lnk
02/16/2008  15:43            2,359,350  Dc56.bmp
02/16/2008  15:40             22,208  Dc57.bmp
02/15/2008  18:01            2,359,350  Dc58.bmp
02/19/2008  10:15            1,280,373  Dc61.flv
02/20/2008  10:23            307,254  Dc64.bmp
02/20/2008  10:22            307,254  Dc65.bmp
02/22/2008  17:13             27,433  Dc68.mp3
02/22/2008  17:20             2,754  Dc69.zip
02/16/2008  15:48            2,359,350  Dc73.bmp
02/21/2008  10:55             28,424  Dc74.bmp
02/22/2008  16:54            726,528  Dc78.ppt
02/22/2008  16:53            182,272  Dc79.xls
02/18/2008  14:10            8,373,426  Dc80.bmp
02/27/2008  15:46             969  Dc82.gif
01/31/2008  12:00    <DIR>          Dc83
02/04/2008  10:13             65 desktop.ini
03/05/2008  18:04            50,420  INFO2
                20 File(s)      27,638,517 bytes
                 5 Dir(s)   14,031,876,096 bytes free

C:\RECYCLER\S-1-5-21-861567501-854245398-682003330-500>

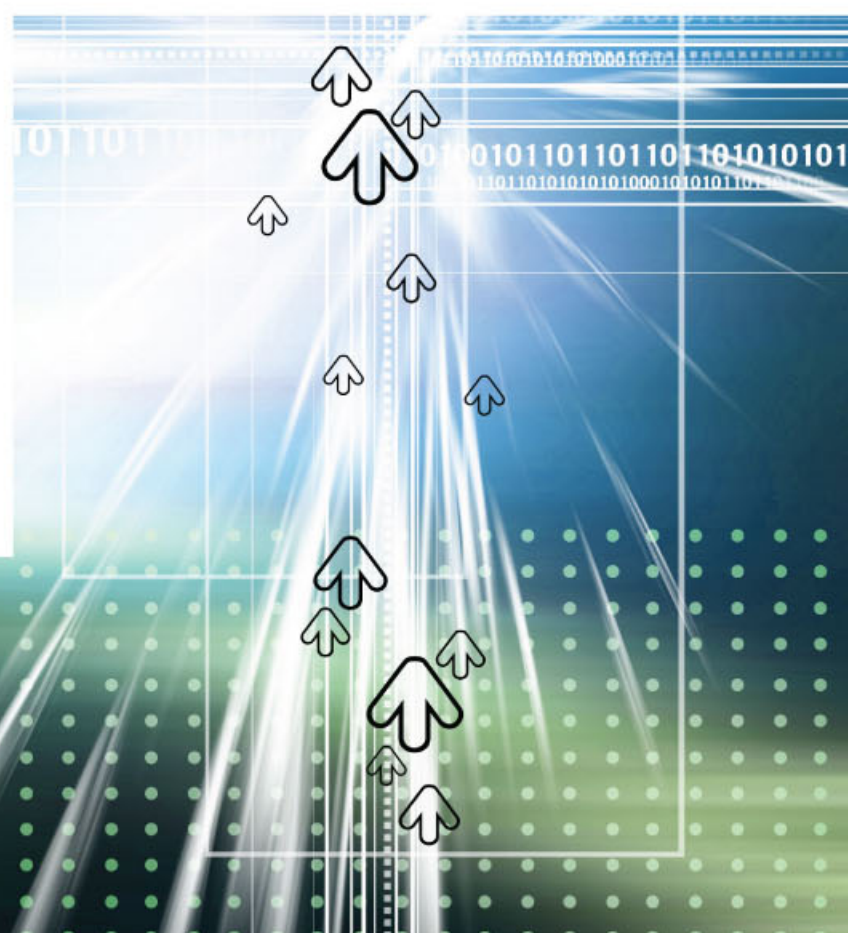
```

Figure 3.26: The content of a XP Administrator's recycle bin

XP enters the file information such as deletion date, size, filename and path into a file called INFO2 (circled in red in Figure 3.26 above). When XP sends a file or folder to the recycle bin, the item's data clusters do not move. Instead, XP simply moves the item's directory entry into the appropriate physical bin folder on the same drive, and then renames the directory entry. XP stores the original names and locations in INFO2, which is stored in each physical bin folder. The names of items within folders sent to the recycle bin are not changed and are not stored in the index file [SANS Institute, 2007].

Investigating the inside of Vista's \$Recycle.Bin folder reveals some significant changes on the way the deleted data are managed. Figure 3.27 on the next page shows the content of Vista's \$Recycle.Bin folder. The biggest difference is that Vista does not use INFO2 file anymore to keep track of the deleted files and folders. However, one attribute remains the same; i.e. each deleted file receives a new name while maintaining the extension but the naming convention is different from XP though. Vista uses the naming convention of \$Rxxxxx.<ext> and \$Ixxxxx.<ext> where the letter x represents 5 random alphanumeric characters. Now a file named "Tax97.doc" may look like "\$R31NRDB.doc" in \$Recycle.Bin.

The interesting part here is that when a file is deleted, an index file is also created. From the earlier example, the deleted Tax97.doc file will receive an index file called "\$I31NRDB.doc". This shows that when a file is deleted, a paired file is created which apparently are the original file with modified filename and an associated index file. If an analyst tries to view the file pairing via windows explorer, he will not be able to see the file pairs; instead he can only see the files with their original filename. The only way to see the file pairs is to navigate to the appropriate folder via the command prompt.



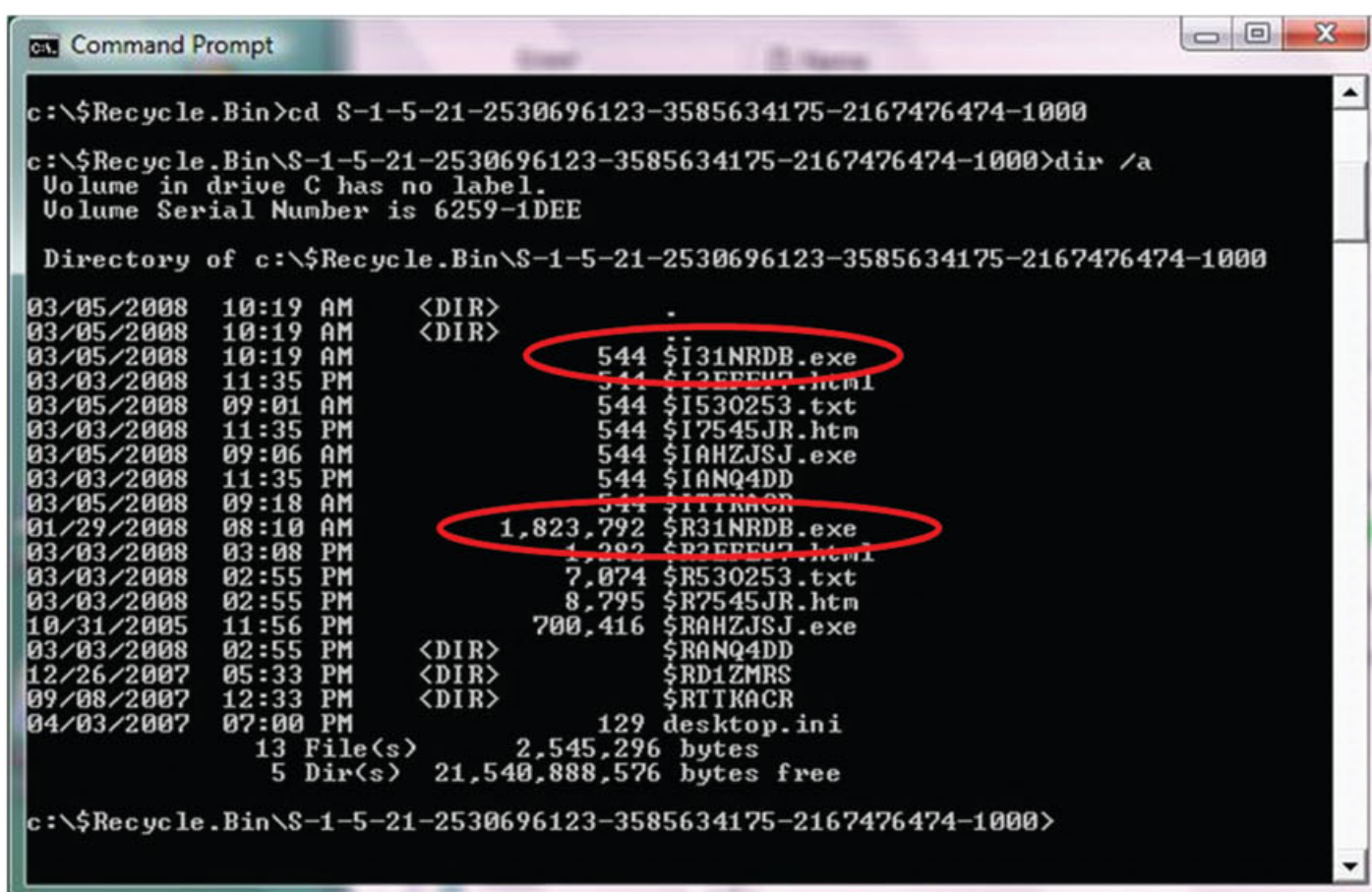


Figure 3.27: The content of Vista's \$Recycle.Bin folder

Notice that the index file is always the same size of 544 bytes. Figure 3.28 below shows the content of an index file (\$I04929L.jpg) viewed through EnCase. It is clear that the index file contains information such as the filename, the original path of the file, MAC time and so on. Figure 29 below shows the original file (\$R04929L.jpg) which the index file represents. If we scrutinize the original file, we can see that it still holds all the information of the file, in this case it is a JPEG image file.

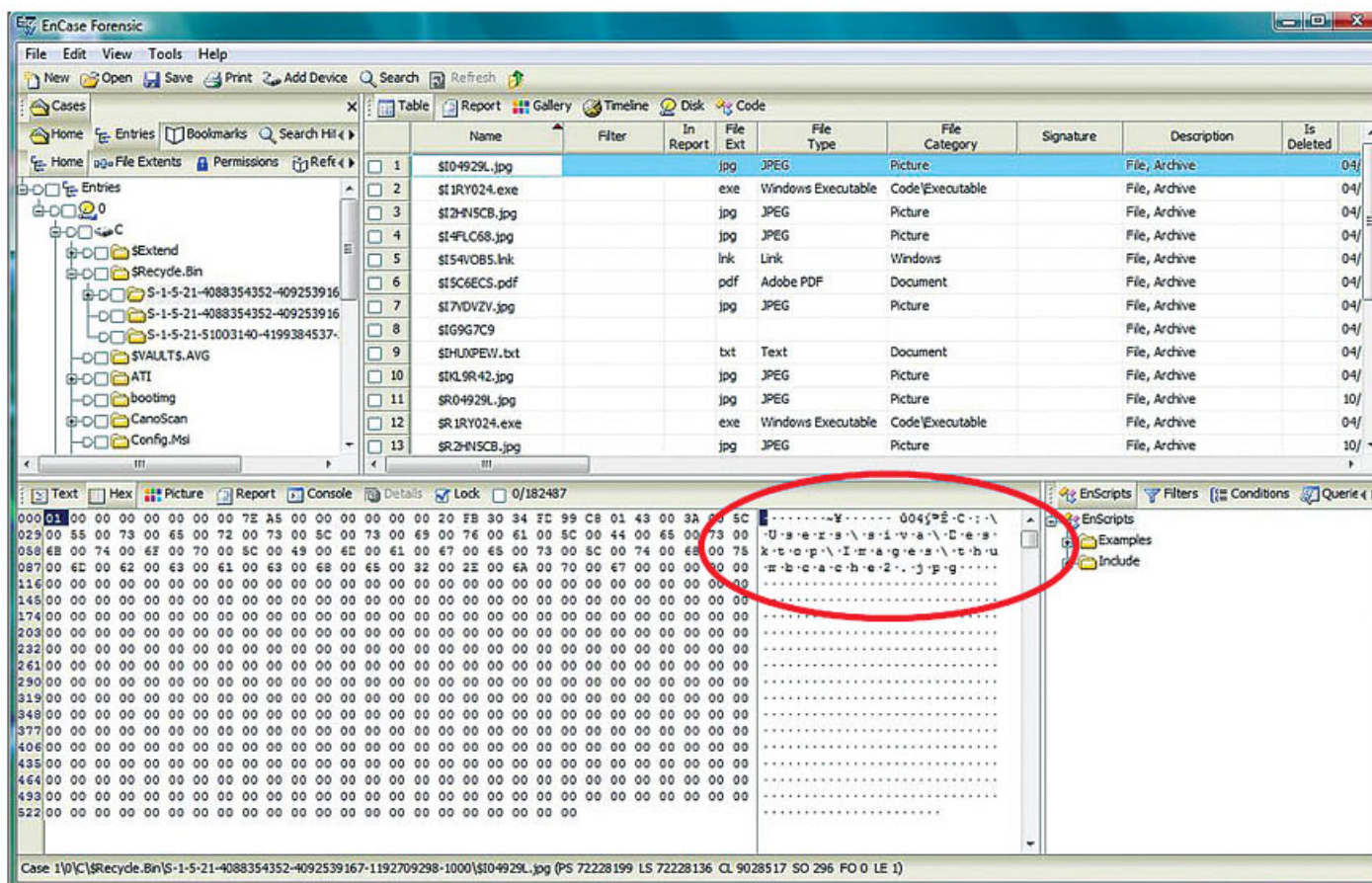


Figure 3.28: Index file viewed through EnCase

Rogue Security Applications Dominate Fortinet's Most-Reported Threats for August 2008

MALAYSIA, 4 September 2008 – Fortinet - the pioneer and leading provider of unified threat management (UTM) solutions - today announced the top 10 most reported high-risk threats for August 2008. Malware W32/Multidr.JD!tr and HTML/Agent.HFZ!phish, disguised as security software AntiVirus XP 2008 and XP Security Center, claimed the top two positions in Fortinet's Top 10 with nearly 20 percent of the month's activities. W32/Multidr.JD was especially prolific with a one-day attack in late August that dislodged pesky mass mailer Netsky from its persistent No. 1 position. HTML/Agent.HFZ!phish arrived in users' in-boxes as a purported UPS email with rogue XP Security Center attached, claiming to be an important document.

"Cyber criminals are clearly trying to take advantage of users' security concerns with an intense campaign for rogue security applications this past month," said Derek Manky, security researcher for Fortinet. "This is a popular, emerging area that provides a new social engineering approach -- black hats posing as white hats."

Fortinet's FortiGuard Global Security Research Team compiled this report based on intelligence gathered from FortiGate multi-threat security systems in production worldwide. Customers who use Fortinet's FortiGuard Subscription Services are already protected against the threats outlined in this report.

Other malware trends observed during this period include the following:

- Virut.A, a virus that infects executable files, refuses to back down, remaining in the top five position for seven consecutive months;
- Mytob and Pushdo mass mailers slid out of the top 10, but remain relevant;
- Iframe traffic redirectors remain strong, moving up one position to sixth place from the July edition of this report.


Following are the Top Ten individual threats and Top Five threat families in August. Top 100 shifts indicate positional changes compared to July'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/Multidr.JD!tr	Trojan	10.02	new
2	HTML/Agent.HFZ!phish	Trojan	8.15	new
3	W32/Netsky!similar	Mass mailer	5.95	-2
4	JS/Agent.WMA!tr.dldr	Trojan	5.9	new
5	W32/Virut.A	Virus	4.65	-3
6	JS/Iframe.DR	Trojan	4.19	+1
7	W32/Agent.KG!tr	Trojan	3.36	new
8	HTML/Iframe.DN!tr.dldr	Trojan	2.59	-3
9	HTML/Iframe_CID!exploit	Exploit	2.12	+17
10	JW32/Agent.HKR!tr	Trojan	1.98	new

Top Five Families

Rank	Malware Family	Percentage	Top 10 Shift
1	Netsky	9.5	+1
2	OnlineGames	7.7	-1
3	MyTob	5.8	-
4	Virut	5.4	-
5	Pushdo	3.0	+6

To read the full August report, please visit:

 http://www.fortiguardcenter.com/reports/roundup_aug_2008.html

For ongoing threat research, bookmark the FortiGuard Center

 <http://www.fortiguardcenter.com>

or add it to your RSS feed by going to

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

To learn more about FortiGuard Subscription Services, visit

 <http://www.fortinet.com/products/fortiguard.html>

FortiGuard Subscription Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help enable protection against threats on both application and network layers. FortiGuard Services are updated by the FortiGuard Global Security Research Team, which enables Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. These updates are delivered to all FortiGate, FortiMail and FortiClient products.



MySQL Forensics Case Study: Online Financial Investment



Case Background

When I juggled through Google search engine, I found a lot of research and studies in Oracle forensics field. However, my search in MySQL forensics seems to find a dead end when I tried to look for such information over the Internet. I have tried to search for books, research papers and forums over the Internet discussing this issue, but to no avail.

With some knowledge and experience in MySQL, along with reference from MySQL manual, I tried to find the best solutions to deal with MySQL forensics cases.

On 2nd of April 2008, I was handed over a digital forensics case from a law enforcement agency. The case was related to illegal online financial investment, offered by a Malaysian company via its website. The case was categorized under financial fraud by Digital Forensics Department, CyberSecurity Malaysia.

The instructions from the client were to extract database records and to look for other relevant data.

The case required extraction of the website database content, and to analyze the database logs. The case had nothing to do with hacking crimes or database malicious program; it was a straight forward case.

In this article, I will specify forensically sound methods in handling the MySQL database case.

cyberspace

The Method

→ Acquisition

The evidence received by the Digital Forensics Department was a unit of hard drive with size of 250GB. A bit to bit copy of the evidence was made by using a forensic tool. The hash value of the hard drive was calculated and was documented in the case work note.

The analysis was done on the image copy of the evidence. The evidence was preserved and stored in evidence room.

→ Analysis

The environment of the case study (or the evidence) was Windows platform and the version of the MySQL was 5.0.51b-community-nt. The analysis on the case was done by adopting the same environment.

The focus of the analysis was to discover the following information:

- Part A: The database record
- Part B: The logs files

PART A: The database records

Let's focus on the first part of the analysis; the database content. The following describes steps of how I extracted the content of the database and presented the records to the client.

Step 1

Copy data folder, .ibd and ibdata into working machine
data folder, .ibd files and ibdata file from mysql folder (from imaged copy) were copied into mysql folder in my working machine.

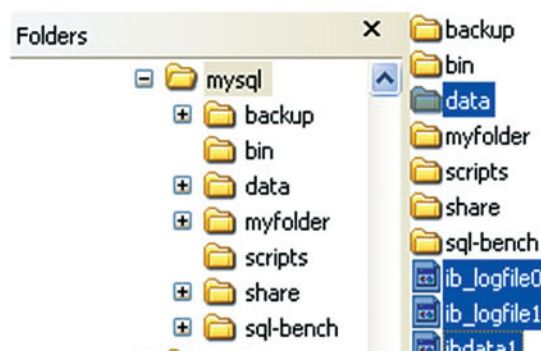


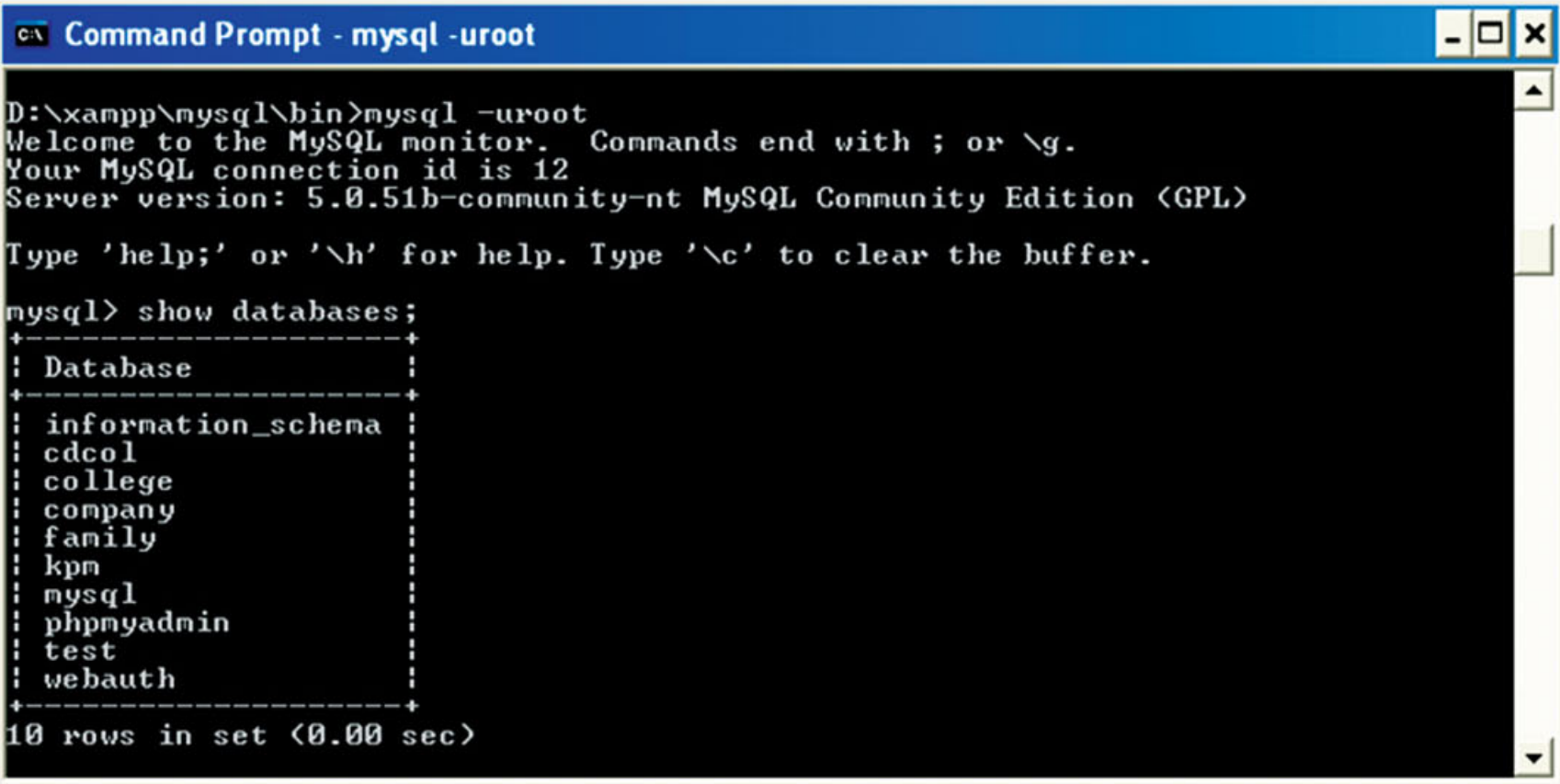
Figure 1.0: MySQL Directory

MySQL, by default, creates a *mysql* folder under C directory when user installs the program. Regardless which storage engine it uses, MySQL will create *data* folder under *mysql* directory. The folder contains .frm file or format file for the tables of the database.

.ibd and ibdata are files created when user creates a table with InnoDB storage engine. By default, MySQL uses MyISAM storage engine. Unlike InnoDB, MyISAM stores all database related files in the *data* folder.

Step 2
Run the MySQL service and the application

Next, I started the MySQL service then launched the application by using the following commands:



*Figure 2.0: Commands of running the MySQL and listing the existing database.
Note that the databases that are shown in Figure 2.0 do not represent the real case.*

Other option for accessing the database content, rather than using the command line is to install SQLyog, a GUI for MySQL program, which can be downloaded for free from www.webyog.com. It provides a simpler and graphical representation of the database.

Step 3
View and Extract the Data

Viewing the content of the database can easily be done by using SQL statement. Some examples of SQL statements that I used to view the content of the data are listed in table below.

Instruction	Statement
To view all data from a table:	SELECT * FROM table1;
To join table and view all data:	SELECT * FROM table1, table2 WHERE table1.id = table2.id
To count the total records from a table:	SELECT COUNT(*) FROM table1;

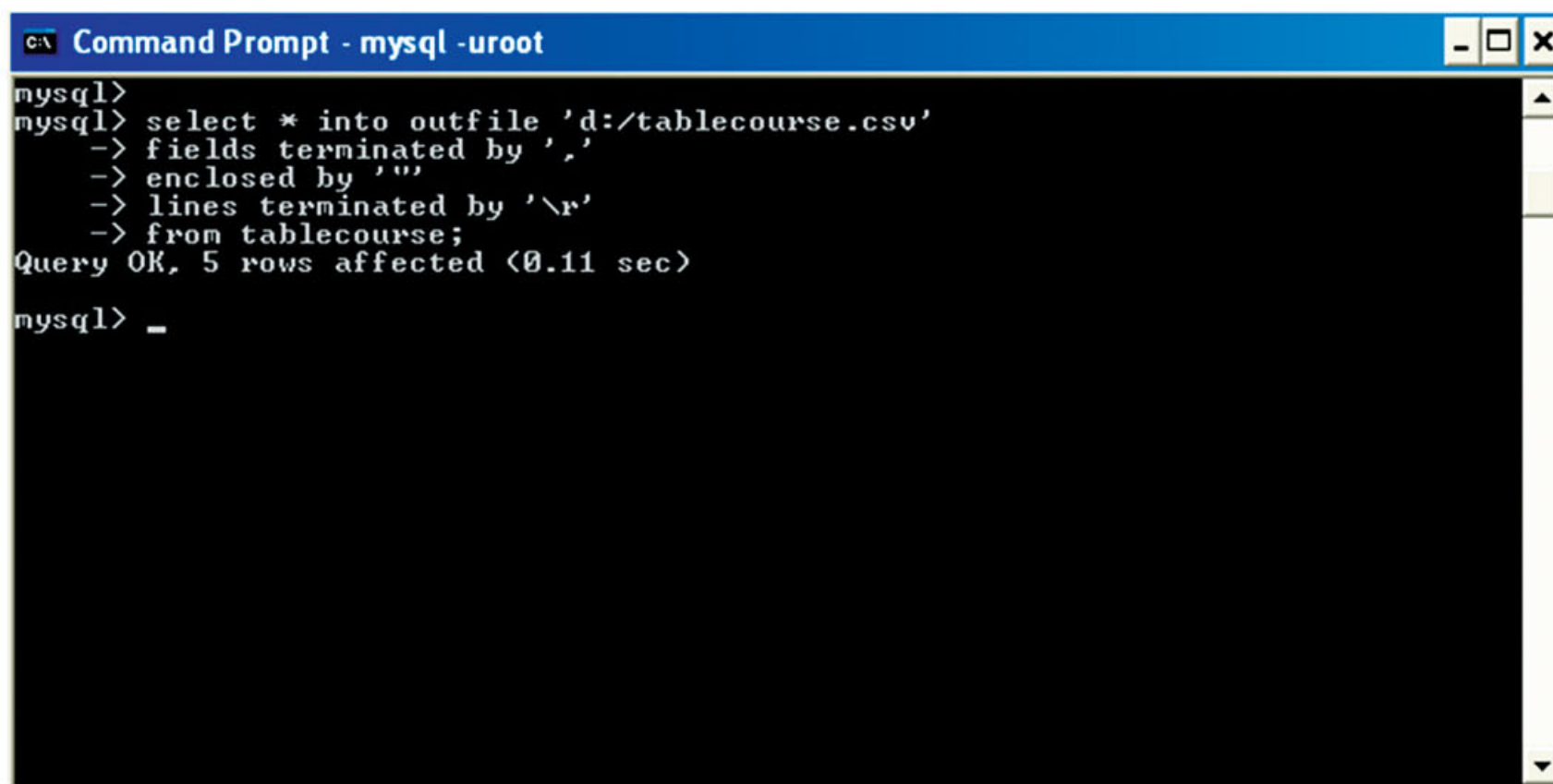
Table 1.0: A sets of instruction and SQL statements

The extraction of the data depends on the client’s needs, sometimes you need to join several tables together to get more readable and meaningful data, and sometimes you just need to extract a particular table only.

The data can be extracted into several formats; CSV, HTML, XML, Excel XML or even SQL format.

Before the data was extracted, the total numbers of records for all tables in the database were recorded.

The command that I used to extract the data into CSV format was:



```
mysql>
mysql> select * into outfile 'd:/tablecourse.csv'
        -> fields terminated by ','
        -> enclosed by '"'
        -> lines terminated by '\\r'
        -> from tablecourse;
Query OK, 5 rows affected (0.11 sec)
mysql> _
```

Figure 3.0: MySQL command for exporting data into CSV file

CSV file can be viewed by using MS Excel, OpenOffice.org Calc or Gnumeric. Some application has limitation in the number of the total rows. MS Excel, for example, can only support 65,536 numbers of rows.

In my case, the client was using MS Excel application to view the data. Tables with more than 65,536 records were extracted into HTML format, rather than CSV.

PART B: Log files

MySQL by default stores its log files in the mysql directory. The log files that MySQL created were:

1. **Status File**
2. **General Query Log**
3. **Binary Log**
4. **Slow Query Log**
5. **Error Log**

Using this knowledge, I began searching and analyzing each log that was created pertaining to the forensic case.

Status Files

This log records the server process ID in a PID file. By default, the PID filename is *host_name.pid* in *data* directory.

The Status File of the case, which was located at the *data* directory, provided me with the host name of the server machine.

1

Error Log

The error log records messages about normal and abnormal startups and shutdowns. It also provides information about the version of the MySQL application. The default name is *host_name.err*, located in *data* directory.

The case that I received contained one related error log file with the size of 20kb. That particular error log provided me with information about the MySQL version, the date and time of the server startups and its last shutdown.

2

General Query Log

This log contains a record of when the clients connect and disconnect, and the SQL statements that the server receives from clients. By default, the name is *hostname.log* and it is located at *data* directory. This log will not be created unless the user specifies it.

Referring to the case that I analyzed, there was no general query log file at all.

3

Slow Query Log

It contains SQL statements that take a long time to execute and the execution status information. This log has to enable by the user by executing some command. The default name is *host_name-slow.log*, created under *data* directory.

The slow query log in this case was disabled.

4

Binary Log

This log records SQL statements that modify data. It is disabled by default. The default name is *host_name-bin.log*.

This case did not enable the binary log.

5

Presenting Information

The information that I gathered during the acquisition and analysis were presented in a report. The areas that I focused were:

- The evidence details – hash value, size of hard disks, serial number
- Case background
- Data of each table and total number of records
- Logs information
- Hypothesis






The report was then submitted to the client.

Summary

In 2006, there were 225 database security breaches reported in US, and between 1st January to 31st March 2007; a 90 day period, there were 85 breaches cases reported to the government. The statistic shows that the database security cases have increased over the years. Realizing the increasing threats, California State, US has passed the Database Security Breach Notification Act in 2003. More states in the US states have passed similar legislation with more set to follow.

In summary, MySQL forensics is a new and exciting area to be ventured into. While the focus of database forensics is now more on Oracle Database, more research need to be done towards other database application.

References

- [1] MySQL 5.0 Reference Manual,
 <http://dev.mysql.com/doc/refman/5.0/en/>,
 viewed on 25/8/08.
- [2] Oracle Forensics,
 <http://www.databasesecurity.com/oracle-forensics.htm>,
 viewed on 25/8/08.
- [3] Implementing the Oracle DB Forensic Response Process,
 http://www.dba-oracle.com/forensics/t_forensics_response.htm,
 viewed on 26/8/08.
- [4] MySQL Forums,
 <http://forums.mysql.com/>,
 viewed 28/8/08.
- [5] Oracle Forensics in a Nutshell, Paul Wright,
 <http://www.databasesecurity.com/oracle-forensics.htm>,
 viewed 25/8/08.



Secure Coding

Introduction

Basically, information security is based on these following pillars:

- **Confidentiality:** ensuring that information is accessible only to those authorized user
- **Integrity:** ensuring that information is not tampered or altered by unauthorized users
- **Availability:** ensuring that information is available to authorized users when it is needed

We have to bear in mind, that security is an important feature. It should not be regarded as an additional feature of product development. Instead, we should design security into all of our applications. We should not treat security merely as a background task, added only when it's convenient to do so. Each and every product functional specifications should include a section outlining security implications of their feature.

Security must be stressed from the onset. Conversely, if security is approached subsequently after the design phase, it might change the way how we implement features and application interface and the eventually of unlocking codes relied upon by the current interface. Hence, bugs that are found would be hard to fix while exposing the vulnerability of the product to attacks.

Building a secure system, free of bugs and vulnerability seems an impossible target to attain. Therefore, it is pivotal for developers to build an application which can be manipulated, stored, and, hopefully, protect the confidentiality of user and corporate data. The application should eliminate users employing such application systems from the fear of data loss or attack on privacy.

How to secure your code

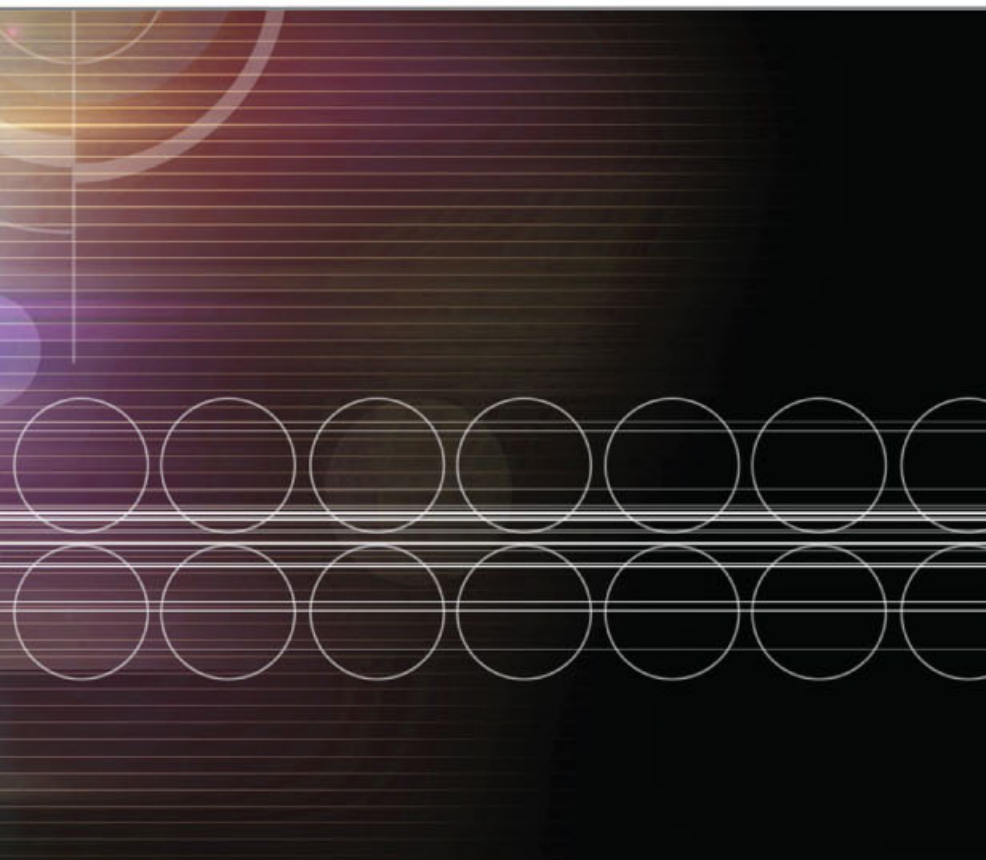
Writing secure code is the first step in producing secure applications. Understanding security threats and vulnerabilities in existing products will help developers to design a better-informed decision on patching while enabling them to develop further strategies of the application secure.

There are many ways to secure your code. Before we begin to think on security, we first have to understand the threat possibilities to the application or system. Once, identifying the threats concerned, we then must work towards avoiding these threats. For these reasons, application developer must have a deep understanding concerning security issues.

→ Input validation

Input validation is a process of validating all the input to an application before using it. It is absolutely critical to security application and numerous risks involved on infected input at various level.

Data must be validated as it crosses the boundary between entrusted and trusted environments. Data from an external entity or client should never be trusted. Michael Howard, in his famous book Writing Secure Code said, "All Input is Evil". Unfortunately, the rule is hard to be realized by developers, developing complex applications that require large number of input data.



Failure to properly validate input coming from the client or the environment before using is the most common application security weakness. This weakness is a recipe for disaster. An attacker simply could apply cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks and file system attacks. It also may cause buffer overflows.

Not all, incorrect input data sources comes from attackers. There are also the possibilities it arising from typos. So, it is useful for having error messages (including warnings, confirmations, questions, and status) as a notification when a problem has occurred, an explanation of why the problem has occurred, and a probable solution to fix the problem. In addition, this method is also a means to validate input data from user.

→ **Keep It Simple!**

Developer should design their application as simple as possible. The more lines of code that we have, the more security vulnerabilities will be created.

Complex designs will increase errors in their implementation, configuration, and use. Thus, more effort is required to achieve an appropriate level of assurance security. Developers should also avoid the use of double negatives and complex architectures when a simpler approach would suffice.

→ **Encryption, Hashes, and Digital Signatures**

Privacy is confidentiality. In achieving such goal, encryption is usually performed. This method can be used to protect a user's secrets from others, either during data transmission or when the data is stored.

Application developers need not to store the secret itself. Instead, we can store a verifier, which often takes the form of a cryptographic hash of the secret. For example, if an application needs to verify that a user knows a password, we can compare the hash of the secret entered by the user with the hash of the secret stored by the application. In this case, the hash of secret was stored by the application and not a secret key itself.

The hashing process involves passing data through a cryptographic function. When a recipient receives data with a hash attached, he can verify the data by comparing newly created hash with the hash attached to the data. If the two hashes are the same, the data was not altered with. However, this method was not definitely correct. An attacker might have changed the data and then recalculated the hash. This is one of the reasons why digital signatures are important.

Digital signature is a mechanism by which a message is authenticated to prove that a message is effectively coming from a given sender.

Digital signature process involves submission of hashed data with private key that only known to the sender, which is used to encrypt the hash. The recipient can verify the signature by using the public key associated with the sender's private key, decrypting the hash with the public key, and then calculating the hash. If the results are the same, the recipient knows that the data has not been tampered with and that it was sent by someone who has the private key associated with the public key.

→ **Use effective quality assurance techniques**

Source code audit, penetration testing, and fuzz testing, should be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. They can identify and correct invalid assumption with independent perspective.

Common Vulnerability

→ Buffer Overflow

A buffer overflow occurs when data written to a buffer beyond the boundaries of a fixed-length buffer.

It is probably caused by the programming mistake that is most widely exploited by hackers. Usually, buffers contained a finite amount of input data and the extra information. An attacker can overwrite these buffers by injecting some codes that can cause unwanted executions of application. Worse situation will occur when attacker has successfully taking over the machine.

Buffer overflows can be prevented by checking on the length of input variables, arrays, and arguments. This task is for developer. Developer should build the application system which is enabled to check the length of the input data before copying to the buffer. If the input data exceeds the buffer size, an exception should be logged and program flow changed. There are many tools that can automatically identify this condition. However, these tools only identify the problem, but the developer or programmer still has to go through the results and fix each one.



→ Format String vulnerabilities

Strings are a common type of input and because of many string-handling functions have no built-in checks for string length, strings are frequently the source of exploitable buffer overflows. The `strcpy` function merely writes the entire string into memory, overwriting data whatever came after it. The `strncpy` function truncates the string to the correct length, but without the terminating null character. When this string is read, it will cause all of the bytes in memory following it, up to the next null character, might be read as part of the string. Only the `strncpy` function is fully safe, truncating the string and adding the terminating null character. These problems can be eliminated by proper input validation and exception checking in the code.

→ Authentication & authorization

Authentication is the most critical component of any security system. It is a process for verifying the identity of user. The most common mistake with authentication is to use weak authentication records that would allow an attacker to brute force the authentication records, such as a password. Therefore, it is always recommended that passwords should contain at least 8 characters in length and include alphanumeric and special characters.

Authentication is often necessary over a network. Therefore, developer should make sure the transaction of sending and receiving data was safe. Digital certificates are often used for this purpose.

Authorization is the process of allowing, or disallowing, access and performs a restricted operation and particular resource based on the identification of an authenticated principal. Once authenticated, the user can access to the resource as long as authentication is provided. However, attacker can exploit this method to enter the system. For example, the Web server set a Javascript variable to an account number. By simply changing account number, attacker was able to view and edit other accounts.

Conclusion

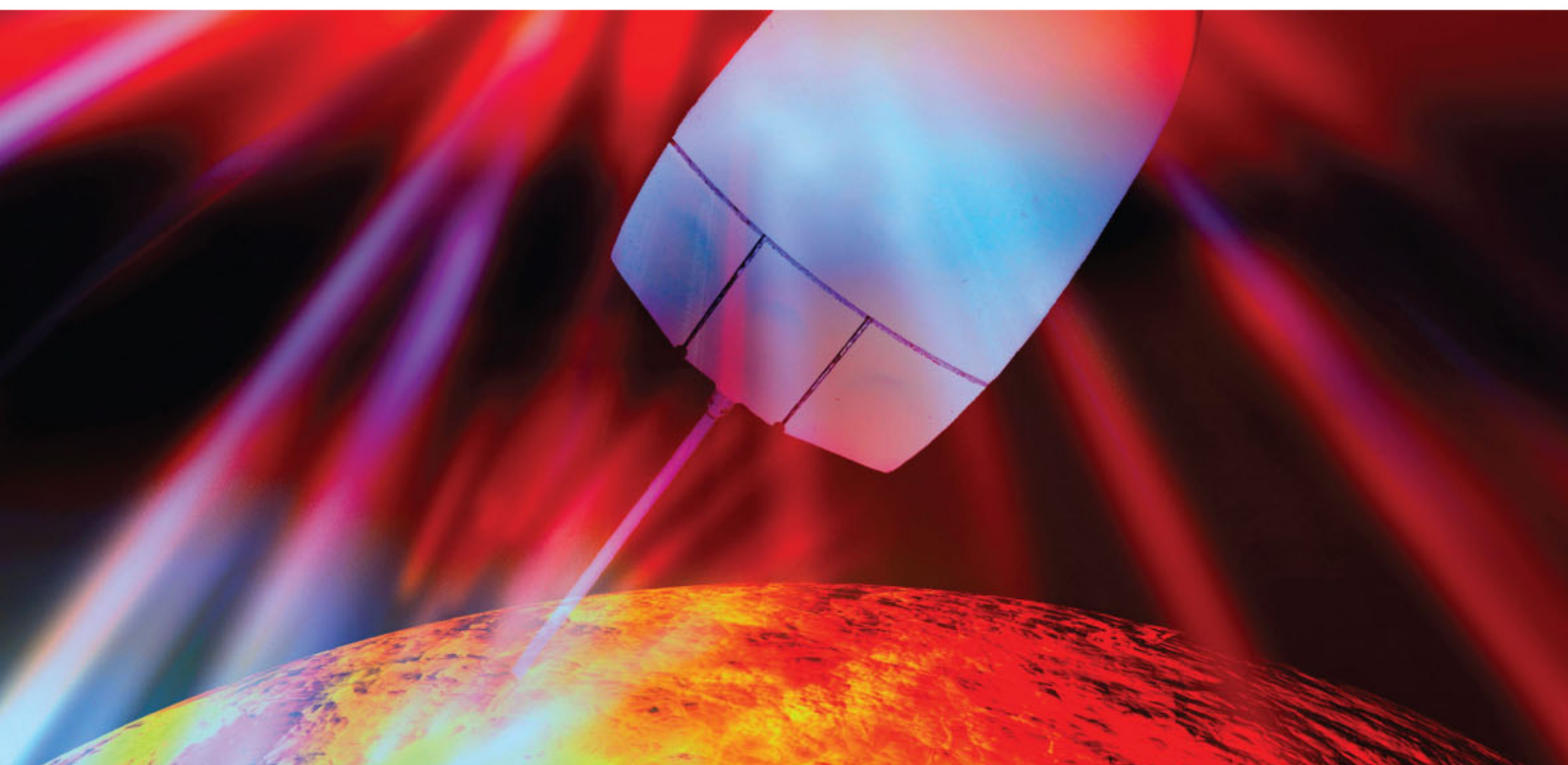
It is not an easy task to write software, not to mention how to make it safe. However, with the increasing number of attacks on software today, it makes writing secure software is an essential task to do. The resources required to build secure software is high. Nevertheless, by educating programmers with knowledge in code security can avoid common security mistake. Performing security code reviews, and testing applications for security bugs can eliminate many of the vulnerabilities commonly exploited today.

References

-  Michael Howard: **"Writing Secure Code"**, Microsoft Press.
-  Secure Coding Guide by Apple Inc., <http://developer.apple.com/documentation/Security/Conceptual/SecureCodingGuide/SecureCodingGuide.pdf>
-  Secure Coding Principles 101 by Laura Taylor, http://www.intranetjournal.com/articles/200401/ij_01_20_04a.html
-  Secure Coding Principles, http://www.owasp.org/index.php/Secure_Coding_Principles

Further reading

-  Michael Howard: **"Writing Secure Code"**, Microsoft Press.
-  John Viega, Gary McGraw: **"Building Secure Software: How to Avoid Security Problems the Right Way"**, Addison-Wesley Professional Computing Series
-  Secure Coding Guide by Apple Inc. <http://developer.apple.com/documentation/Security/Conceptual/SecureCodingGuide/SecureCodingGuide.pdf>



Mobile Phone Forensic: The

Investigating mobile phones has always surprised me. Sometimes, and often so it can lead to unexpected findings.

To date, more than 100 phones were analyzed by Digital Forensics Lab. As time passed by, I've realized that as I venture deeper in understanding the phone's memory, I found that there were other valuable information that could not be obtained by logical extraction.

In this article, I will discuss about how we can retrieve information about Bluetooth transactions on mobile phone and how this information can help in digital forensics investigation.

The idea of studying Bluetooth communication via phones came up right after the country was shocked with news of postmortem pictures of a little girl being disseminated across the country. Some suspects were detained and while some were released. One of the issues in questions was, "Can you actually prove that pictures stored on mobile phones were captured by using the phone's camera or was it sent via Bluetooth from another phone?"

This article is intended to somewhat answer that. However, it should be stated here, that the method depicted here is not the only proven way to authenticate the origin of a picture on a mobile phone, but it can surely assist investigation officers in searching for additional clues.

Bluetooth Address of a Mobile Phone

In general, a Bluetooth-enabled device has a unique 48bit address to enable it to communicate and exchange data with other Bluetooth-enabled devices, be it a mobile phone, computer or other peripherals such as headset or even a mouse. Each byte carries certain meanings to uniquely identify a device in a Bluetooth network.

Now, how do we look for a Bluetooth address of a mobile phone? For a Bluetooth-enabled mobile phone, certain key press will display the Bluetooth address. For example, the Bluetooth address of a Nokia phone can be checked by just pressing *#2820# (*#BTA0#).

So, what does the address mean? To explain a little bit about the Bluetooth address, let's see the Bluetooth address of a Nokia N95 in Figure 1. The first 3 bytes (00:1A:DC) of the address are registered by IEEE to Nokia N95, meaning that all Nokia N95 mobile phones shall have



the identical first 3 bytes. The rest of the address (D3:E3:D3) are assigned by the manufacturer, in this example a Nokia N95 was used, and should be different for each Nokia N95 phone.

00	1A	DC	D3	E3	D3
Registered to Nokia N95 by IEEE			Assigned by manufacturer - should be different between each N95 model		

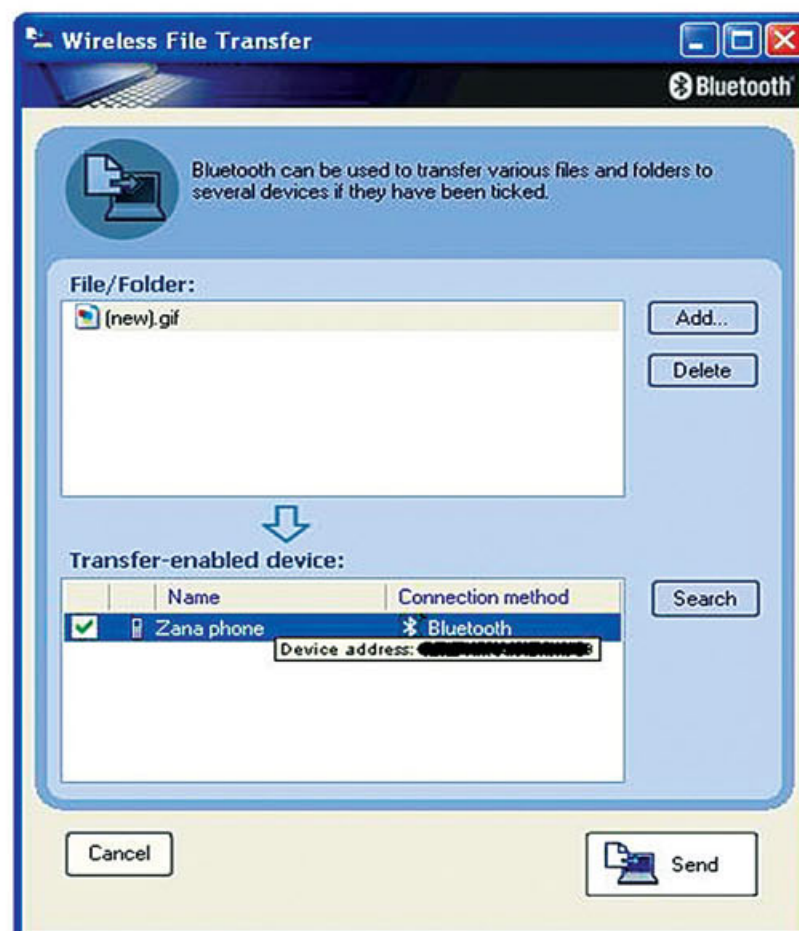
Figure 1. Bluetooth address of a Nokia N95

Tooth that Leaves Trails (Part I)



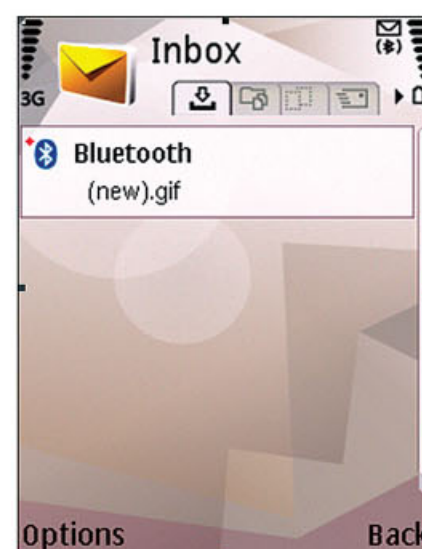
How to Search for Clues?

Here is a simple examination that I have done, to prove that a picture found on a phone was not actually originated from the phone itself, but was sent via Bluetooth. To start with, I sent a picture from my laptop to my Nokia N95 phone via Bluetooth. The process can be simplified in Picture 1.



Picture 1: A picture named (new).gif was sent to a Nokia N95 (Zana phone) via Bluetooth

On my Nokia N95, the picture (new).gif was received as a new message. I saved the picture in the phone's memory while I deleted the message. The sequence of the process can be seen below:



1. A picture (new).gif was received via Bluetooth.



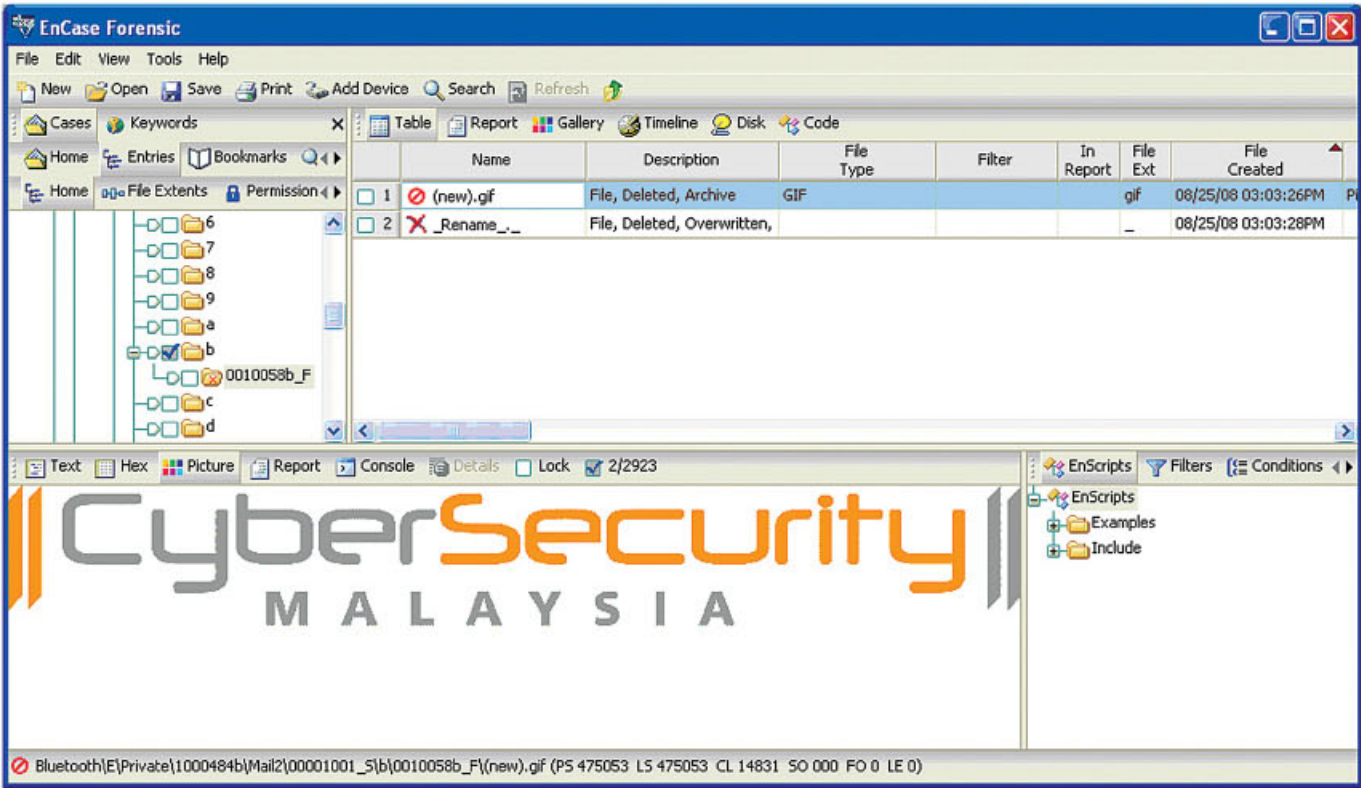
2. The picture was saved on the phone's memory.
3. The message was deleted.

After the message being deleted, the memory card of my mobile phone was imaged (bit-to-bit copy).

Found Gold

In general, messages are stored in a specific directory which is hidden from the user. It means that a normal user cannot see the folder using his/her phone. This folder can only be seen utilizing special software. In Picture 2, I had used a forensic tool to display all hidden directories that contain messages stored on the memory card.

This was not the only findings. It appears that after having deleted the message, the process did not completely remove the said message from the memory card, shocking huh?



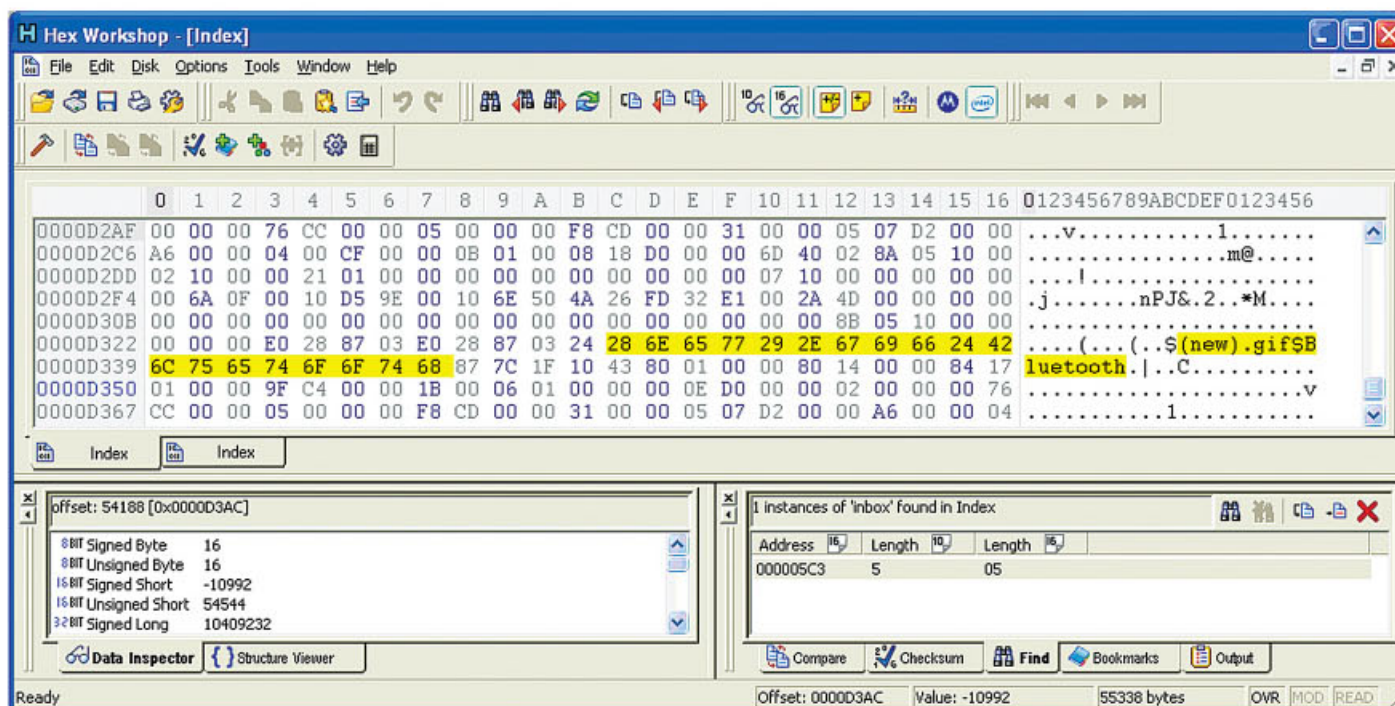
Picture 2: On the Left Pane is the Directories where Messages are Stored and on the Right and Down Panes are the Deleted Message

However, these findings failed to prove that the (new).gif picture was sent to my phone via Bluetooth.

This is where the interesting part begins!

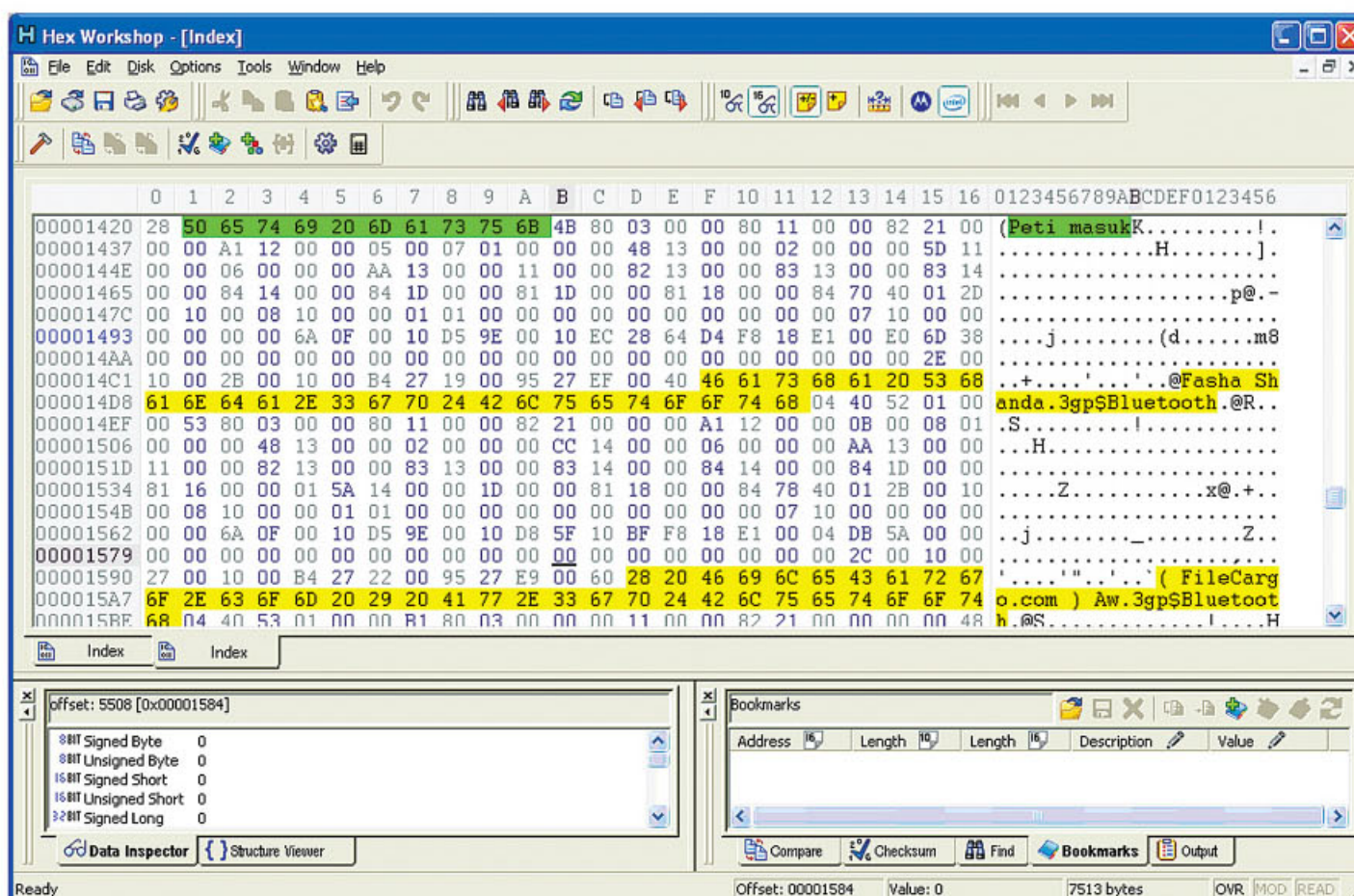
In one of the directories, contains an Index file. This particular file receives or sends messages that were stored on the phone. These messages re organized by the mobile phone's operating system in a consistent pattern in which the pattern can determine whether these messages were received from or sent to the phone.

Similarly, each files received via Bluetooth is saved and organized by the operating system in a unique pattern too. In Picture 3, a pattern can be seen where a 'Bluetooth' tag is marked after the filename (new).gif.



Picture 3: Evidence showing (new).gif was received via Bluetooth on a Nokia N95

I have also checked against another phone, a Nokia 7610, and similar pattern was found. As in Picture 4, again, a 'Bluetooth' tag is marked after the filename, where in this case, they are two 3gp files. What was interesting this time around was that these 3gp files were found after the 'Peti masuk' (Inbox) tag (highlighted in green). This clearly demonstrates that these files were sent to the Nokia 7610 via Bluetooth.



Picture 4: Evidence showing two 3gp files received via Bluetooth on a Nokia 7610

Please look forward for further discussions on my findings featured in Part II of my article.

Pengaruh Laman Web

You Tube

di Serata Dunia

Laman web perkongsian video YouTube adalah antara laman web yang popular di seluruh dunia ketika ini. Diwujudkan pada Februari 2005, YouTube membolehkan pengguna Internet di seluruh dunia berkongsi klip video dengan memuat naik dan turun klip video tersebut melalui laman web, blog, e-mel dan peranti mudah alih seperti telefon bimbit.

Laman web YouTube mengandungi pelbagai jenis klip video yang bersifat peribadi dan umum. Penerbitan atau penghasilan klip video itu pula mempunyai tujuan yang berbagai-bagai; antaranya, sebagai hiburan seperti lagu dan humor, atau sebagai media untuk penyebaran maklumat, baik yang bersifat umum mahupun khusus seperti politik. Baru-baru ini semasa Pilihan Raya Umum ke-12, parti-parti politik telah menggunakan YouTube sebagai wadah penyebaran maklumat dan berkempen bagi menarik perhatian penyokong mereka.

Kemudahan alat perakam video yang semakin murah, canggih dan mampu dimiliki oleh sesiapa sahaja seperti telefon bimbit berkamera, menambah keghairahan pengguna Internet berkongsi klip video di YouTube. Namun keghairahan tersebut kadangkala membawa padah apabila ia mula disalahgunakan. Seperti juga kemudahan lain di Internet seperti e-mel, laman web dan blog yang menjadi mangsa penyalahgunaan, YouTube juga tidak terkecuali.

Tahun lalu, Malaysia digemparkan dengan penyebaran klip video 'Negaraku' yang dianggap menghina lagu kebangsaan dan berunsur perkauman. Klip video yang dihasilkan oleh pelajar Malaysia di Taiwan itu mencetuskan polemik sehinggakan kerajaan terpaksa mengambil tindakan.

Namun tindakan kerajaan Malaysia masih boleh dianggap lembut berbanding tindakan oleh kerajaan di beberapa negara lain. Beberapa negara seperti Indonesia, China, Thailand, Pakistan, Maghribi, Turki dan Iran pernah menyekat akses ke laman web YouTube berikutan penyiaran klip video yang dianggap sensitif, bertentangan dengan undang-undang dan budaya negara berkenaan.

Awal tahun 2008, ketika dunia dilanda kontroversi penerbitan klip video filem 'Fitna' arahan ahli politik

Belanda, Geert Wilders, kerajaan Indonesia telah mengarahkan penyedia perkhidmatan Internet (ISP) utamanya menyekat sementara akses ke laman web YouTube untuk memastikan rakyat Indonesia tidak menonton klip video filem tersebut.

Tindakan tersebut diambil setelah kerajaan Indonesia memberi kata dua kepada Google agar mengeluarkan klip video filem tersebut daripada laman web YouTube dalam tempoh 48 jam. Keengganan Google menuruti arahan tersebut menyaksikan laman web YouTube serta beberapa lagi laman web kendalian Google iaitu MySpace dan Google Video disekat oleh ISP di negara berkenaan.

Sebelum itu, kerajaan China pada 16 Mac 2008 telah menyekat akses ke laman web YouTube berikutan penyiaran beberapa klip video bantahan rakyat Tibet terhadap pemerintahan China. Menurut laporan agensi berita AP, tindakan sekatan tersebut adalah salah satu usaha kerajaan negara komunis itu mengawal apa yang 'dilihat dan didengar' oleh rakyat negara tersebut mengenai insiden yang meletus di Lhasa, Tibet pada 14 Mac 2008. Selain laman web YouTube, laman-laman web British Broadcasting Corporation (BBC), Cable News Network (CNN) dan Yahoo News turut menjadi mangsa tindakan keras kerajaan China. Walaubagaimanapun, sekatan ke atas laman web YouTube ditarik balik pada 23 Mac 2008.

Tindakan sekatan ke atas laman web YouTube pada 16 Mac 2008 bukanlah kali pertama diambil oleh kerajaan China. Pada 14 Oktober 2007, kerajaan China pernah menyekat akses ke laman web YouTube selama 2 minggu sempena mesyuarat Kongres ke-17 Parti Komunis Kebangsaan.

Terdahulu, pada 8 Mac 2008, Thailand menyekat akses ke laman web YouTube ekoran penyiaran ucapan bekas

Perdana Menteri, Thaksin Shinawatra di laman web berkenaan. Namun begitu laman web YouTube boleh diakses semula pada hari yang sama. Sekatan tersebut bukanlah pertama kali dilakukan oleh kerajaan Thailand. Pada 3 April 2007, laman web YouTube disekat aksesnya di Thailand berikutan keengganan pemilik laman web tersebut, Google, mengikut arahan kerajaan Thailand untuk mengeluarkan klip video yang dianggap menghina Raja Bhumibol Adulyadej. Sekatan tersebut ditarik balik pada 30 Ogos 2007 setelah Google bersetuju menapis kandungan laman web tersebut agar pengguna Internet di Thailand tidak dapat mengakses klip video berkenaan.

Pada 24 Februari 2008, Pakistan menyekat akses ke laman web YouTube kerana mendapati laman web tersebut menyiarkan kandungan yang menyinggung perasaan umat Islam antaranya kartun yang mempersendakan Nabi Muhammad S.A.W dan trailer filem pendek, 'Fitna'. Sekatan tersebut ditarik balik pada 26 Februari 2008.

Pada 25 Mei 2007 pula akses ke laman web YouTube disekat di Maghribi ekoran penyiaran klip video rakaman demonstrasi di Sahara Barat, wilayah yang dikuasai oleh Maghribi semenjak 1975.

Walaupun bagaimanapun, pihak penyedia perkhidmatan Internet, Maroc Telecom menafikan sekatan tersebut ada kaitannya dengan klip video berkenaan sebaliknya ia berlaku kerana masalah teknikal. Sekatan tersebut ditarik balik pada 29 Mei 2007 setelah mendapat bantahan pengguna Internet di negara berkenaan.

Sementara itu, mahkamah di Turki pada 6 Mac 2007 telah mengarahkan agar laman web YouTube disekat aksesnya berikutan penyiaran klip video yang melabelkan rakyat Turki dan bekas pemimpinnya, Mustafa Kamal Atartuk, sebagai homoseksual. Klip video tersebut telah dikeluarkan daripada laman web YouTube setelah mendapat bantahan daripada pengguna Internet di Turki. Namun, mahkamah tetap memutuskan agar akses ke laman web berkenaan disekat. Pada 9 Mac 2007, sekatan tersebut ditarik balik.

Sepanjang tahun 2008 sahaja, mahkamah di Turki telah mengarahkan laman web YouTube disekat pada 18 Januari, 24 Januari dan 19 Mac 2008 atas sebab yang sama.

Pada 3 Disember 2006, akses ke laman web YouTube dan beberapa lagi laman web telah disekat di Iran setelah kerajaannya menganggap laman-laman web berkenaan 'tidak bermoral'.

Menurut laporan media, antara punca laman web YouTube disekat ialah penyiaran klip video adegan seks seorang pelakon negara berkenaan dan klip video yang mempersendakan pemimpin-pemimpin Iran seperti Presiden Mahmoud Ahmadinejad, Ayatollah Khamenei, bekas Presiden Rafsanjani dan bekas pemimpin Basij, Mohsen Rezaee. Laman web YouTube di Iran masih disekat sehingga ke hari ini.

Beberapa negara lain seperti Armenia, Brazil, Arab Saudi dan Emiriah Arab Bersatu (UAE) turut pernah menyekat akses ke laman web YouTube atas alasan laman web berkenaan menyiarkan kandungan yang sensitif dari sudut politik, sosial dan agama negara-negara berkenaan.

Berdasarkan senario yang berlaku di beberapa negara berkenaan, jelas bahawa YouTube mempunyai pengaruh yang kuat sehinggakan kerajaan di negara-negara berkenaan mengambil tindakan keras menyekat akses ke laman web berkenaan.

Walaupun tindakan tersebut dianggap bertentangan dengan kebebasan media dan bersuara terutama oleh negara-negara Barat, kerajaan di negara-negara berkenaan enggan tunduk dengan tekanan tersebut. Sebaliknya kerajaan-kerajaan ini tegas dan tegar dengan pendirian mereka kerana menganggap klip video yang disebarkan di YouTube bertentangan dengan amalan budaya, agama dan politik negara masing-masing.

Kenyataan dan pandangan yang terdapat di dalam artikel ini adalah pendapat peribadi penulis dan bukan pandangan rasmi CyberSecurity Malaysia.





Towards ISO/I

Information security is an important issue in today's business. In the era of globalization, information has been flowing with no geographical boundaries. Every business depends heavily on information which becomes one of the most critical assets in many organizations. Thus, information should be prudently managed by protecting its confidentiality, integrity and availability. Unsecured or misuse of information can lead to loss of integrity that gradually tarnishes image and reputation of an organisation.

Information security management can no more be done by merely a set of hardware and software. Rather, it requires a complete end-to-end system. Managing information security is as important as managing the business itself. For some countries, organizations are expected to comply with certain regulations, along with implementation of an information security management structure in its business. Thus, it is crucial for organisation to have the information security framework established and objectives accomplished. Threats are no longer in physical aspects alone, but also from other various sources with the most common are internal threats. Without proper system established in any organisation, information is continuously being threatened to be lost, stolen, unauthorized accessed, misused, blocked or destroyed by people, viruses, malwares or natural disasters.

In the process of establishing the environment for Information Security governance, many organizations are aware that it is preferable to follow some type of internationally recognized reference framework for establishing such environment, rather than doing it in an ad hoc manner. There are several possible reference frameworks which can be used, one of them is ISO/IEC 27001:2005 (ISO 27001); an international standard on establishing the information security framework.



EC 27001:2005 Certification

What is ISO/IEC 27001:2005?

International Standard Organisation (ISO) has published ISO/IEC 27001 that provides a robust model in implementing information security framework within an organisation. This standard specifies requirement for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) in an organisation. Together with ISO/IEC 27002 on Codes of Practice for information security management, ISMS governs risk assessment, security design and implementation of security controls, security management and reassessment. It also emphasizes on the continuous improvement on business processes within an organisation. Establishment of such framework within an organisation requires special focus and participation from all levels of employees with full commitment and responsibilities.

Implementing the ISMS provides an opportunity for organizations to identify and deal with issues that are often overlooked. For example, if an organisation deals a lot with secret information; the organisation may need to classify its information and manage it in accordance with its classification. Different levels of classification of information require different ways in managing them by addressing each level of criticality. This certainly provides guidance for employees in handling their information.

Organizations need to build ISMS by combining all the bits and pieces as per their organisational needs. In this context, ISMS provides a systematic approach in adopting the best practice controls, quantifying the level of acceptable risks and implementing appropriate measures to preserve the confidentiality, integrity and availability of information assets. Through Plan-Do-Check-Act (PDCA) model, the whole cycle consists of Plan (to establish an ISMS), Do (to implement and operate the ISMS), Check (to monitor and review the ISMS) and Act (to maintain and improve the ISMS). It also insists on 'Third Party Audit' in acquiring ISO 27001:2005 certification in the same way as ISO 9000 series quality certification.

In Malaysia, certification against ISO 27001:2005 is mainly conducted by SIRIM QAS International, a certification body accredited by United Kingdom Accreditation Service (UKAS) and other bodies that comply with internationally recognized standards.



Objectives of certification

Some organizations only deal with ISMS at the implementation level. However, some even go further to become ISMS certified. To date, there are 26 organisations that are ISO/IEC 27001:2005 certified nationwide (<http://www.iso27001certificates.com>). Many organisations aim for ISMS certification against ISO/IEC 27001:2005 to build credibility and competitive advantage against their competitors. Certification allows organisation to be positioned globally that indirectly announce it's internationally acceptance with other similar certified organizations worldwide. From a business perspective, this can be a significant criterion for foreign investment to come in, as ISO certification provides a high level of assurance, trust and confidence to ensure the success of business ventures.

Another dimension of looking at why organisations aim for ISO certification is the ability it has in inculcating the “information security” culture within the organizations through the ISMS implementation process. This is especially true when the ISMS process include all supporting and non technical departments and divisions, beyond the IT department. For many organisations, it is crucial that this culture is developed and embedded within the organisation. Having this culture instilled in every employee does not only meet the objective of the certification, but also will assist them in their daily life when they were not at their work place. Employees tend to be more careful from the aspect of information security.

Certification Success factors

Success factors include commitment and support from top management. Relevant policies need to be endorsed and supported by procedures to ensure policies are enforced throughout the organisation. Top management commitment on the financial and morale support is very much required as it does not only instil the enthusiasm element in the driver but also assist the driver in achieving the objective of the organisation to implement it.

Another success factor is the needs to have a dedicated team who have the enthusiasm and strong support by the management to drive the implementation and ensure on its success. Awareness is another critical success factor especially when the scope of certification encompasses the whole organisation and requires participation from many departments and divisions. Policies and procedures must be consistently and prudently communicated in a manner in which employees feel comfortable on doing it. Thus, awareness programs for all shall be developed and communicated to ensure all employees get the right message.

Challenges

In implementing new ideas and approaches in any organisation, there is bound to be plenty of challenges. Despite being successfully ISMS certified, the hard work need to continue. The most challenging part is gaining buy-in from top management. Given top management support,, working on the whole process becomes easy as it is largely a top down approach. In the contrary, employees will be reluctant to participate in the process without the support from top management.

For organizations that choose to include the whole organization in the process, they will require involvement from various business functions and a high number of employees. When implementing new controls, personnel require time to adjust to new ways of doing things. Changing mindset involves managing the human factor. Management support and innovative awareness program are fundamental to train the thinking process within the personnel to be aware and embrace the process in place.



In conclusion, ISMS implementation and ISO27001:2005 certification is not a onetime affair. It provides a process for continuous improvement in planning and implementation to ensure compliance with proven standards. Most important of all, being ISMS certified provides a level of assurance that information security remains as one of the areas of priority in an organisation.

OPC SECURITY: PART 1

In year 2005, a study on National Cyber Security Policy (NCSP) which was conducted by MOSTI has determined that Control Systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) are among the critical systems that require national protection.

These systems are used by our critical infrastructure sectors such as Electricity, Oil & Gas, Water and Waste treatment, Transportation and Manufacturing industries, to operate their daily services and production for the nation.

The effective functioning of these infrastructures is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. There is an increasing risk to the critical infrastructure sectors that rely on these systems that can be damaged or disrupted by both intentional and unintentional cyber incidents. Such incidents could potentially have a significant and potentially overwhelming impact on the national economy, security and public safety.

The security issue for SCADA or DCS systems has increased due to the interconnection of SCADA network and corporate network that rely on common operating systems such as Microsoft Windows. The usage of these systems increasingly relied on commercial information technologies (IT) such as Ethernet™, TCP/IP and Microsoft products, creates more risks to their existing known vulnerabilities.

“The wide-spread adoption of OLE for Process Control (OPC) standards for interfacing systems on both the plant floor and the business network is a classic example of both the benefits and risks of adopting IT technologies in the control world. OPC is an industrial standard based on the Microsoft Distributed Component Object Model (DCOM) interface of the Remote Procedure Call (RPC) service. Due to its perceived vendor-neutral position in the industrial controls market, OPC is being increasingly used to interconnect Human Machine Interface (HMI) workstations, data historians and other servers on the control network with enterprise databases, ERP systems and other business-oriented software. Furthermore, since most vendors support OPC, it is often thought of as the one of the few universal protocols in the industrial controls world, adding to its widespread appeal.”¹

What Is OPC?

As defined by OPC Foundation, a non-profit corporation has established a set of standard Object Linking and Embedding/Component Object Model (OLE/COM) interface protocols intended to foster greater interoperability between automation/control applications, field systems/devices, and business/office applications in the process control industry.²

OPC (OLE for Process Control) is a set of vendor-neutral specifications created by the OPC Foundation to facilitate the inter-operation of process control products.³ It draws a line between hardware providers and software developers. It provides a mechanism to provide data from a data source and communicate the data to any client application in a standard way. A vendor can now develop a reusable, highly optimized server to communicate to the data source, and maintain the mechanism to access data from the data source/device efficiently. Providing the server with an OPC interface allows any client to access their devices.

To connect clients and servers OPC uses DCOM (a technology for distributed inter-process communications) which is in turn layered on top of Microsoft's Remote Procedure Call (MSRPC) service. Both DCOM and MSRPC are Microsoft proprietary protocols so most of the developed servers run on the Windows platform, although solutions exist to implement OPC on other Platforms.

Typical usage of OPC client/server is shown in the diagram 1.⁴

¹ OPC Security White Paper #1, Understanding OPC and How it is Deployed, Byres Research (2007)

² OPC Overview 1.00, OPC Foundation, (1998)

³ OPC Server Security Considerations, Lluís Mora, Neutralbit, Spain

⁴ See the “DCOM on Non-Microsoft Platforms” article on the OPC Foundation website

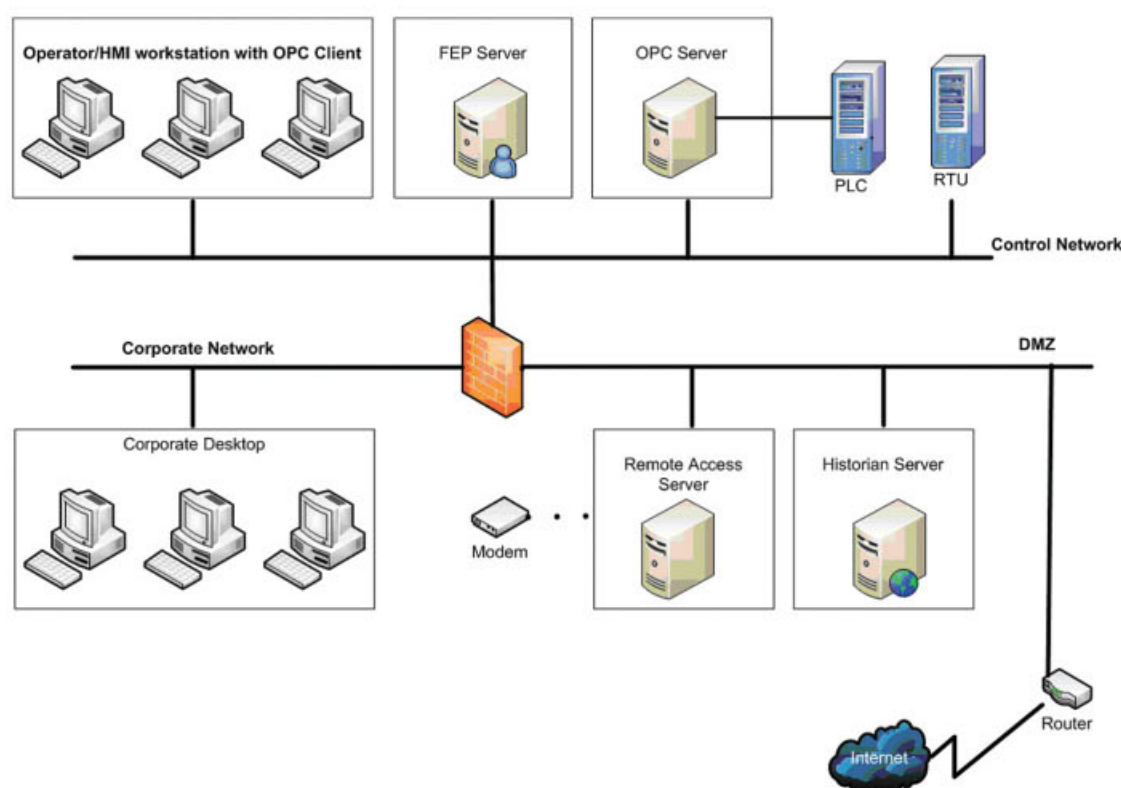


Diagram 1: OPC implementation in typical Control Systems Network Architecture

OPC Threats And Risks

OPC is an interface used within SCADA or DCS applications to access data from a networked server. The OPC architecture allows a client application to access data from many OPC servers provided by many different OPC vendors.

Possible risks and vulnerabilities that may incur in deploying OPC in a control systems environment include the following:

(a) Weaknesses of Microsoft RPC/DCOM services:

The use of OPC connectivity in control systems and servers leads to the possibility of RPC/DCOM-based protocol attacks disrupting control systems operations.

“Although MSRPC services have been widely tested for security vulnerabilities, the tests have centered around the transport layer and not on the application layer that DCOM implements. OPC testing revolves around the study of the protocol and the identification of weaknesses, identifying various new vulnerabilities in the process. The main innovation is in analyzing DCOM from the interface point of view and automating discovery and testing of OPC servers.”⁵

Virus and worm attacks may be increasingly focusing on the underlying RPC/DCOM protocols used by OPC.

“Over the past few months, the two attack vectors that we saw in volume were against the Windows DCOM (Distributed Component Object Model) interface of the RPC (remote procedure call) service and against the Windows LSASS (Local Security Authority Subsystem Service). These seem to be the current favorites for virus and worm writers, and we expect this trend to continue.”⁶

(b) Open Protocol With Free Available Specifications

OPC specifications are to facilitate the development of OPC Servers in C and C++, and to facilitate development of OPC client applications in the language of choice. The architecture and design of the interfaces are intended to support development of OPC servers in other languages as well.

“... it is our belief that the most serious issue for OPC is securely deploying OPC applications has proven to be a challenge for most engineers and technicians. While OPC is an open protocol with the specifications freely available, engineers must wade through a large amount of very detailed information to answer even basic security questions. There is little direct guidance on securing OPC, and our research indicates that much of what is available may actually be ineffective or misguided. All things considered, there is little doubt that some clear advice for the control engineer on how best to secure OPC systems would be very useful.”⁷

⁵ OPC Exposed – Part I, a research paper presented by Lluís Mora of Neutralbit, Spain at Proceedings of the SCADA Security Scientific Symposium (S4) 2007.

⁶ Bruce Schneier, “Attack Trends” QUEUE Magazine, Association of Computing Machinery, June 2005

⁷ OPC Security White Paper #1, Understanding OPC and How it is Deployed, Byres Research (2007)

(c) Misconfiguration of OPC Server or Client

Common misconfiguration vulnerabilities found in OPC server or client computers both at the operating system and OPC application level.

“In it, they have detailed the vulnerabilities typically found in OPC hosts, based on OPC’s current architecture (such as the use of DCOM) and the typical underlying operating system. They also investigated common misconfiguration vulnerabilities found in OPC server or client computers both at the operating system and OPC application level. Finally, using the vulnerabilities uncovered, they discuss four possible risk scenarios for OPC-based attacks.”⁸

(d) Expose to Denial-of-Service attacks

Several DoS attacks have proven effective against OPC servers that could be carried out by attackers with no technical background or by malware.

“After having seen several OPC servers in real production environments crash for no apparent reason, we did some investigation in OPC server stability and how OPC design features could be exploited either by malware or by an attacker. For proof of concept, we implemented the attack methods described in a small Windows application, called OPC Security Checker. As the impact of each attack method depend on environmental factors (OS release, security patch, specific OPC server product), users of this software have the opportunity to check the consequences of an attack for the specific setup.”⁹

(e) Security Flaws in Commercial Software and Devices

Researchers at Neutralbit have discovered previously unreported security flaws in commercial softwares and devices. Although most of these vulnerabilities were discovered during a vendor engagement (and thus stay within the boundaries defined in the particular contract) some of their findings were the result of independent research projects.

A complete list of security vulnerabilities published in Neutralbit’s advisory as follows:¹⁰

- Multiple vulnerabilities in Takebishi Electric DeviceXplorer HIDIC OPC server
- Multiple vulnerabilities in Takebishi Electric DeviceXplorer MELSEC OPC server
- Multiple vulnerabilities in Takebishi Electric DeviceXplorer FA-M3 OPC server

- Multiple vulnerabilities in Takebishi Electric DeviceXplorer MODBUS OPC server
- Multiple vulnerabilities in Takebishi Electric DeviceXplorer SYSMAC OPC server
- Multiple vulnerabilities in NETxEIB OPC server

Other researchers at Tenable Network Security have released 32 plugins for Nessus 3 which specifically tests SCADA devices. These plugins were the result of a four month research contract between Tenable Network Security and Digital Bond. Among the OPC vulnerabilities found are:¹¹

- **Matrikon OPC Explorer** - Identifies hosts running Matrikon's OPC Explorer tool. These hosts may also have additional diagnostic tools and trust relationships.
- **Matrikon OPC Server for ControlLogix** - Identifies hosts running a Matrikon OPC Server for Allen-Bradley Control Logix PLC.
- **Matrikon OPC Server for Modbus** - Identifies hosts running a Matrikon OPC Server for Modbus devices and used to access data from PLCs, RTUs, and IEDs. OPC servers are commonly used in SCADA and DCS systems to exchange data between different vendor systems and disparate applications.
- **OPC DA Server** - Identifies hosts running the OPC Data Access Server.
- **OPC Detection** - Finds hosts with OPC application components installed.
- **OPC HDA Server** - Identifies hosts running an OPC Historical Data Access Server.

Conclusion

The risks of deploying OPC are very much due to the weaknesses of the protocols design underlying the current OPC specifications as well as implementation choices made by vendors, such as DCOM configuration settings. It is also exposed to operating system vulnerabilities that could adversely affect the security of the OPC application.

More study and analysis on the most critical vulnerabilities will be provided in the next release (OPC Security: Part 2).

⁸ OPC Security White Paper #2, OPC Exposed, Byres Research, (2007).

⁹ OPC Exposed – Part II, a research paper presented by Ralph Langner of Langner Communications AG at Proceedings of the SCADA Security Scientific Symposium (S4) 2007.

¹⁰ Refer to <http://www.neutralbit.com/en/rd/advisories/>

¹¹ Refer to http://blog.tenablesecurity.com/2006/12/nessus_3_scada_.html

Let's Make The Internet A Safer Place

www.esecurity.org.my

NiC

PxL