CyberSecurity MALAYSIA

e-Security

MOSTI

Volume 13 - (Q4/2007)

You can't consider the problem of defense without first understanding the problem of attack.

Doug Tygar, a professor of computer science and information management at UC Berkeley

Contributors

MyCERT 4th Quarter 2007 Summary Report
MyCERT
CyberSecurity Malaysia

Windows VISTA File System Forensics (PART 2)
By Sivanathan Subramaniam
Digital Forensics
CyberSecurity Malaysia
siva@cybersecurity.org.my

Fortinet Announces Top Reported Threats for November 2007
By Fortinet

Implementing Security Awareness Programme for Organisations
By Raj Kumar
Training & Outreach
CyberSecurity Malaysia
raj@cybersecurity.org.my

Risky Business: Consumers in the Workplace
By Victor Lo
Principal Consultant - Technology
Trend Micro (M) Sdn Bhd

Strategic Initiatives to Protect Control Systems (SCADA)
By Nor' Azuwa Muhamad Pahri
Security Assurance
CyberSecurity Malaysia
azuwa@cybersecurity.org.my

Menacing Threats in Cyber Security
By Yaslinda Mohamad Yassin
Strategic Policy & Cyber Media Research
CyberSecurity Malaysia
yaslinda@cybersecurity.org.my

Threat Chaos Predictions for 2008
By Fortinet

Preventing Leaks of Confidential Information in Email
By Noor Aida Idris
Security Management & Best Practices
CyberSecurity Malaysia
nooraida@cybersecurity.org.my

Roaming Users - Safety On the Go
By Victor Lo
Principal Consultant - Technology
Trend Micro (M) Sdn Bhd

ISSN 1985-1995

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

From the Editor's Desk

vphilip@cybersecurity.org.my

Guess what? It is the end of 2007. It has been quite a year and an exciting one indeed for us here at CyberSecurity Malaysia. First, let me wish our readers a very Merry Christmas and to our Muslim readers, Selamat Hari Raya Haji. The big one is, Welcome 2008, a Happy New Year to all of you.

This issue is packed with exciting articles as usual. Don't forget to read on the Windows Vista Forensics Part 2. We also have articles on 2008 cyber threat predictions, awareness for your organisation, one on SCADA, safety for roaming users, preventing confidential information leak in emails and more.

So, what's new? Well, if you have read our CEO's message, it was an exciting event in November 2007 with the NICE event and we had 3 successful programs. We had embarked on the strategic alliance with Maybank and we hope to continue to extend this alliance with other banks to further educate all Internet Banking users in Malaysia.

What's coming up? Well, on the 23rd & 24th February, we will be participating at the Malaysian Education Fair 2008 at Mid Valley. Come catch us there. Also from the 11th - 13th March, we will be participating at MNCC's conference and exhibition "IP Technology Convergence Conference & Exhibition" at Sheraton Subang. CyberSecurity Malaysia will also be conducting a Wireless Workshop and participating at the exhibition.

For all you security professionals out there, we will be having our first CISSP/SSCP exam on the 23rd February 2008. Our first class for 2008 will be in April 2008. Check out our 2008 schedules for all our training at out website at http://www.cybersecurity.org.my.

Out first INFOSEC.my will be held in March 2008. Check out our website for updates and details for registration. Also, we would like to inform you all that World Congress on Information Technology (WCIT 2008) will be held from the 18th - 22 May 2008. In conjunction with WCIT 2008, a satellite event, World Cyber Security Summit 2008 will also take place. CyberSecurity Malaysia will be having its 2-day conference from the 21st - 22nd May 2008 at the JW Marriot and details will be up soon. So, book your time for this event.

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. Don't forget to check out our awareness portal www.esecurity.org.my for new stuff.

Philip

Philip Victor
Editor

A Message From the Head of CyberSecurity Malaysia

Another year coming to an end, marking 12 months of exciting events and activities for us here at CyberSecurity Malaysia. In our mission and quest to continue to make our cyberspace a safer place, we continue in our proactive measures in enhancing our services.

In November 2007, we were glad to be part of the inaugural National Innovation Conference & Exhibition (NICE) held at the Putra World Trade Centre. CyberSecurity Malaysia had organized the annual Critical Infrastructure Information Protection (CIIP) Workshop. We were honoured to have Y. Bhg. Dato' Abdul Hanan bin Alang Endut, Secretary General of the Ministry of Science, Technology & Innovation to give the keynote address.

To further make this workshop a success, we had distinguished speakers and panelist such as Prof. Howard Schmidt, En Mahdi Mohd Arrifin (Bank Negara), Mr Deepak Pillai (Haryati Deepak) & Prof Pauline Reich. It was indeed a fruitful session and many areas within the CNII were discussed.

Another successful event that was held during NICE was our CIO roundtable and INFOSEC.my Technical Forum. Once again, with a list of distinguished and experienced cyber security experts, it was a knowledge filled event for the participants.

In our continuous effort to educate the ICT users in Malaysia, CyberSecurity Malaysia had formed a Strategic Alliance with Maybank to educate their Internet Banking users in cyber security. The exchange of documents was witnessed by our Prime Minister, YAB Datuk Seri Abdullah Ahmad Badawi. This is only to show that the government is committed in its efforts to make the Internet a safer place for us all.

As we move to 2008, I would like to take this opportunity to thank all those who have contributed to this newsletter and made our publication in 2007 a success and I truly hope your will continue to impart your knowledge and I also welcome new contirbutors. Your knowledge and sharing will definitely benefit our readers to equip themselves with such valuable knowledge in the cyber world. Thank you all.

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

Table of Contents

03 MyCERT 4th Quarter 2007 Summary Report

12 Windows VISTA File System Forensics (Part 2)

18 Fortinet Announces Top Reported Threats for November 2007

22 Implementing Security Awareness Programme for Organisations

25 Risky Business: Consumers in the Workplace

26 Strategic Initiatives to Protect Control Systems (SCADA)

32 Menacing Threats in Cyber Security

34 Threat Chaos Predictions for 2008

36 Preventing Leaks of Confidential Information in Email

38 Roaming Users - Safety On the Go

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

PUBLISHED BY

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

PRODUCED BY

Ilham Design (001690307-U)
No 7302 Jalan 18/11
Taman Sri Serdang
43300 Selangor Darul Ehsan
Tel/Fax: +603 8948 2843

PRINTED BY

Percetakan Tujuh Lapan Enam Sdn Bhd (564108-K)
No18, Lengkungan Brunei, 55100 Pudu, Kuala Lumpur
Tel: 03-27321422
KKDN License Number: PQ 1780/3724

MS-123.102008: MyCERT Quarterly Summary (Q4) 2007
Original Issue Date: 15th January 2008

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during that quarter. This report highlights statistics of attacks or incidents reported to MyCERT, as well as other noteworthy incidents and new vulnerability information. MyCERT believes these statistics are only a tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order for us to assist those affected.

In addition, this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardening techniques.

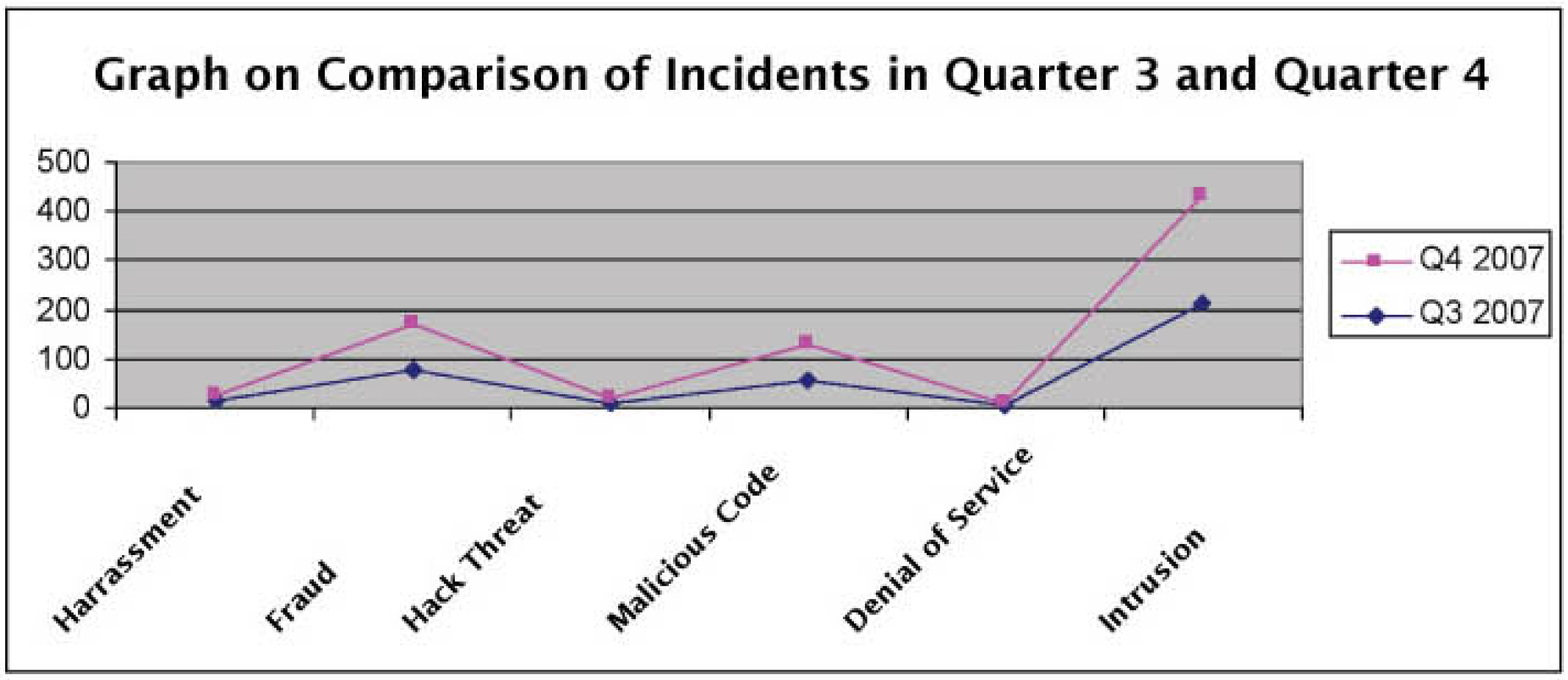
Recent Activities

In the quarter Q4 2007, a total of 9086 incidents were reported to MyCERT representing a 3.37 increase compared to Q3 2007, where we saw a decrease in incidents. About 95.92% of total incidents reported this quarter is contributed by spam reports. No major outbreak was observed this quarter and no significant increase in any particular incidentWe observed 3 types of incidents reported increased and another 3 types of incidents reported had decreased. The other 1 incident remained same as was in previous quarter. Incidents that had increased in this quarter are fraud, malicious code and spam. Other incidents that showed decrease in this quarter are harassment, hack threat and denial of service. Intrusion remained same as was in previous quarter.

Attached is the table of figure:

	Q3 2007	Q4 2007	%
Harassment	15	12	-20
Fraud	79	94	18.99
Hack Threat	12	11	-8.33
Malicious Code	58	72	24.14
Denial of Service	7	1	-85.71
Intrusion	216	216	9.722
Spam	9099	9400	3.31
Total	**9486**	**9486**	**3.37**

Table of Figure for Q1 2007 and Q2 2007



Graph on Harassment, Fraud, Hack Threat, Malicious Code, Denial of Service, Intrusion for Q2 and Q3

Increase in Fraud Incidents

This quarter saw an increase in fraud incidents to 18.99%, which comprised of 94 reports compared to 79 reports in previous quarter. The majority of the fraud incident reported to us are mainly phishing incidents impersonating local and foreign financial institutions, with majority of the phishing sites impersonating foreign banks. Other types of fraud incidents reported to us are suspicious online investments, suspicious ponzi or pyramid schemes and misuse of organization's Intellectual Property such as logo, URL, domain name for promoting illegal activities on the net.

In this quarter we received several reports from foreign observers regarding suspicious ponzi schemes sites, about 15 sites hosted in our constituency. However, MyCERT had escalated the reports to the Enforcements for investigation/verification of such schemes before the closure of the sites. Other than that MyCERT also received several reports from home users on suspicious online investment schemes and online fraud activities. More than 10 such reports were received.

In this quarter, we also received several reports regarding Intellectual Property infringement. Several organizations logo/trademark/domains/URLs were misused without the owners' permission for suspicious activities on the net.

MyCERT had notified the respective ISPs, in which the sites are hosted, mainly in foreign countries for removal of materials that infringes the Intellectual Property. In addition, the respective organizations were also advised to refer to their Legal Departments.

As precautions against online fraud activities, computer users should be careful about disclosing confidential, personal or financial information online unless they know that the request for such is legitimate and users are also advised not to deposit or make payment to unknown third party's account.

User may refer to the following guide on safeguarding against fraudulent emails and phishing attempts:

http://www.mycert.org.my/other_resources/phishing.html

Increase in Malicious Code Incidents

Malicious code incidents continue to increase in this quarter compared to previous quarter. A total of 72 incidents were reported compared to 58 in previous quarter. In this quarter, we received many reports from foreign CERTs and foreign security organizations regarding drones/bots, control & command (C&C) server of botnets and malicious files hosted on machines hosted in Malaysia. Some of these reports contained IPs that had been repeatedly reported to us previously. In all of the instances, MyCERT had notified the respective machines' administrators.

When it comes to botnet activities,There were only a handful of cases involving botnet C&C hosted in Malaysia. The majority of the reports involved bot infected computers, most of which are home user machines. Since these bots are normally used to carry out malicious activities such as spamming, ddos attacks, phishing and spreading malware.

In this quarter, MyCERT also received several reports from a foreign CERT regarding some details found on servers at their side which was used by keylogging trojans to log keystrokes. This is made possible when PCs are compromised with keylogging trojans, that captures users keystrokes, primarily user ID and password. These keylogging trojans will send out information captured to specific servers. The particular account usernames/passwords captured belong to critical industries, such as ISPs and internet bankings.

We advise users to safe-guard their PCs against Trojan, backdoor and worm infections. Users may refer to the below guidelines:

i. Ensure computers are installed with anti-virus software and are frequently updated with the latest virus signatures. Users without anti-virus installed on their PCs may download commercial or free anti-virus from the following site:

http://www.mycert.org.my/anti-virus.htm

ii. Ensure computers are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in computers.

iii. Enable personal/host-based firewalls on PCs.

iv. PC users are also advised not to view, open or execute any e-mail attachment unless it is expected or its purpose known to the recipient.

Decrease in Hack Threat Activities

Incidents involving hack threat decreased to 8.3343% in this quarter. A total of 11 reports were received on hack attempts for this quarter compared to 12 in the previous quarter. Majority of hack threat reports were received from foreign organizations with the source of the hack threats are from IPs belonging to our constituency. Hack threats targeted mainly organizations' systems/networks involving network and host scanning activities. Besides organisations' systems/network, home PCs are also becoming popular targets of hack threat activities.

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). Port scans are actively done once a new bug or exploit is released publicly, using either automated or non -automated tools. Attackers are also scanning for programmes and applications that are vulnerable or exploitable.

Decrease in Denial of Service Incidents

In this quarter, reports on denial of service had decreased to about 85.71%. The number had decreased from 7 incident in previous quarter to 1 incident in this quarter. The denial of service attack consists of sending huge, continuously to a system, causing the system to slowdown or choked. In distributed denial of service attacks, the source of the attacks mostly come from various multiple IPs and majority of denial of service attacks originate from 1 single IP address.

Decrease in Harassment Incidents

Number of incidents received on harassment had decreased to 12 compared to 15 in previous incidents which represents 20% decrease. Harassment incidents reported to us this quarter involved harassments via emails, web forums. This involves sending of constant threatening or defamatory emails to victims and posting defamatory pictures and messages on web forums against victims with malicious intent. In most incidents, the defamatory pictures and messages were removed after MyCERT notified the respective ISPs and source of most harassing emails were traced by the ISP. However, majority of harassment incidents were referred to the Law Enforcement Agencies for their further investigation.

Intrusion Incidents Remains

Incidents on intrusion remained same as was in previous quarter, with 216 reports. Majority of intrusion incidents are web defacements which mainly involve .my sites. Some of the web defacements are re-defacements of the same sites over the year.

In this quarter, we also received several reports on intrusion involving .my websites that especially exploited the RFI as well as the SQL injection and PHP.

Some quick workarounds that can be done to prevent future web defacements are:

---

[1] Using mod_security to prevent generic attacks - SQL injection, XSS, and (RFI). On Apache web server.
Please refer at:

Modsecurity - http://www.modsecurity.org/

---

[2] Checking permission - making sure directories have correct permissions.

2.1 To Check Permision on Linux

shell> ls –alh
shell> drwx-rwx-rwx owner owner_group size_of_file date_created file_name/dir_name

Please make sure the permission files is not configure to allow all permission

(rwxrwxrwx)

2.2 To Check Permision on Windows

Right click and select properties

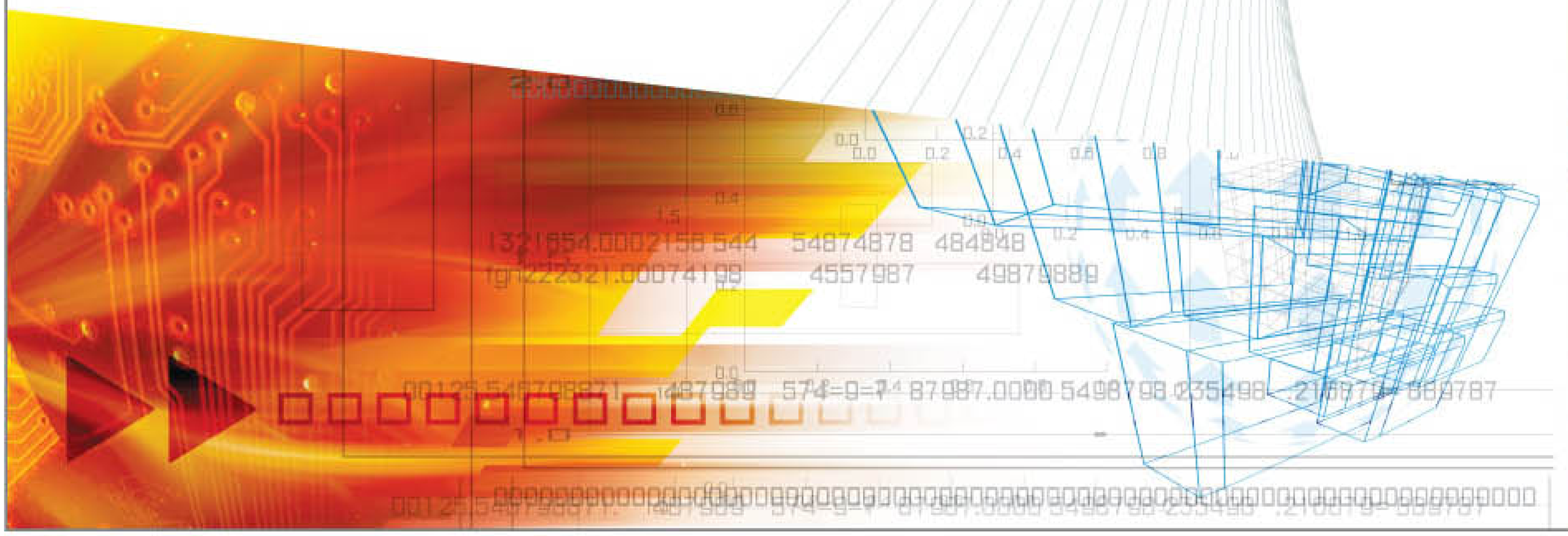
Please refer at:

Checking web permission - http://www.w3.org/Security/Faq/wwwsf3.html

---

[3] Please refer to PHP security checklist for workarounds on PHP.

PHP security checklist - http://aymanh.com/checklist-for-securing-php-configuration



[4] Secure the webserver byreferring to the below checklist.
Web server security checklist

IIS - http://msdn2.microsoft.com/en-us/library/aa302351.aspx

Apache - http://httpd.apache.org/docs/2.0/misc/security_tips.html

[5] We also advise you to audit your web applications to check if there are any flaws on them and reectify them immediately, if yes.

[6] If you are running SQL, we advise you to use input VALIDATION to prevent your website being defaced via the SQL Injection.

[7] If you are running an older version of PHP Script, you need to patch or upgrade it to the latest version which is PHP 4.3.10. The latest version of PHP can be downloaded at:

http://www.php.net/downloads.php

In addition to the above preventive measures, we also advise System Administrators to check their system in case it has been installed with any backdoors or Trojan programs.

Simple guides are as follows:

1. System administrators are advised to regularly monitor / check their systems.

2. Check for any newly added user account in the userlist. You may check at the shadow file, sam file etc.

3. Check for any suspicious connection on the open ports, esp on bigger port number.

4. Scan your server for any kind of backdoor. Use tripwire to check for any signs of backdoor or trojan. This will only be effective if your version of the software is clean prior to applying tripwire.

   Please refer to:
   http://www.tripwiresecurity.com

5. Check and look for any suspicious shell programs.

6. Use URLScan to filter HTTP requests. Many IIS exploits, the Code Red family, use maliciously formed HTTP requests in directory traversal or buffer overflow attacks. The URLScan filter can be configured to reject such requests before the server attempts to process them.

   The URLScan filter can be downloaded separately from Microsoft at

   URLScan Filter

   http://www.microsoft.com/technet/security/tools/urlscan.asp.

7. Download and use IIS Lockdown Tool version 2.1.Running the IIS Lockdown Wizard in "custom" or "expert" mode will allow you to make the following recommended changes to an IIS installation:

   a. Disable WebDAV (unless your environment absolutely requires it for web content publishing).
   b. Unmap all unnecessary ISAPI extensions (including .htr, .idq, .ism, and .printer in particular).
   c. Eliminate sample applications.
   d. Forbid the web server from running system commands commonly used in a compromise (e.g., cmd.exe and tftp.exe).

   IIS Lockdown can be downloaded

   http://www.microsoft.com/technet/security/tools/locktool.mspx

   Note: If some applications requires these services which had beenpreviously removed by Lockdown, the setup can be restored by having the undo files located at n32\inetsrv\oblt-log can be used to recover previous settings.

8. Close all unnecessary services or ports.

9. Close all unnecessary applications.

Please check on the above vulnerabilities and make sure measures are taken to fix any such vulnerability that may present in your system. We advise/urge System Administrators to contact MyCERT immediately if they detected defacement to their websites or detected any attempts to deface their sites and forward us a copy of the "intrusion log" for analysis and consolidation.

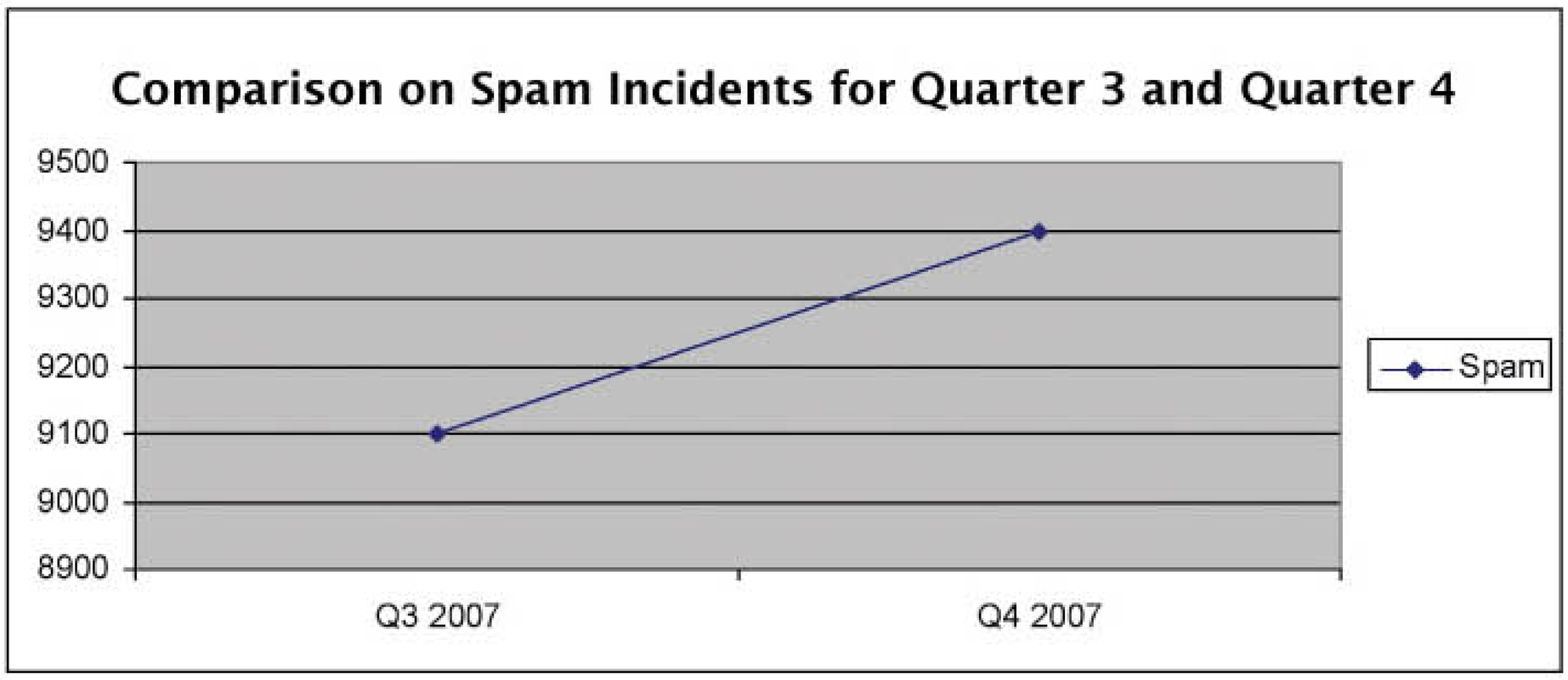
Other Activities

» Spam

Spam incidents had increased slightly to 3.31% in this quarter compared to the previous quarter. A total of 9400 reports were received compared to 9099 reports in previous quarter. Spam incidents remains as the incident with highest number of reports received compared to other incidents. Spam has developed from a mere nuisance into an epidemic that threatens end users and organizations. Spam threats are also fast developing with sophisticated spam techniques and tools moreover with programs like spambots designed to collect email addresses from the Internet. The email addresses are collected in order to build mailing lists for sending unsolicited e-mail/spams. A spambot is a type of webcrawler that can gather e-mail addresses from Web sites, newsgroups, special-interest group (SIG) postings, and chat-room conversations. Because e-mail addresses have a distinctive format, spambots are easy to write.

There are also spambots used to post spam links to guestbooks, wikis, blogs, forums and any other web forms to boost search engine ranking. This category of spambot has gained considerable notoriety since November of 2006, with the introduction of XRumer a forum and wiki spambot which can often bypass many of the safeguards administrators use to reduce the amount of spam posted.

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.



Graph on Spam

» Alerts & Advisories

In this quarter, we had released two advisories related to critical vulnerabilities that exist in two commonly used softwares, the Apply Quicktime and the RealPlayer. They are the Apple Quicktime - RTSP "Content-Type" Header Buffer Overflow and the RealPlayer - ActiveX Arbitrary Command Execution.

The advisories are available at:

Apple Quicktime - RTSP "Content-Type" Header Buffer Overflow

http://www.mycert.org.my/advisory/MA-121.112007.html

RealPlayer - ActiveX Arbitrary Command Execution

http://www.mycert.org.my/advisory/MA-120.102007.html

» Research Network Activities

The CyberSecurity Research Network monitoring objectives are:

1) To monitor the network for suspicious traffic as well as to monitor for the occurrence of known malicious attacks.

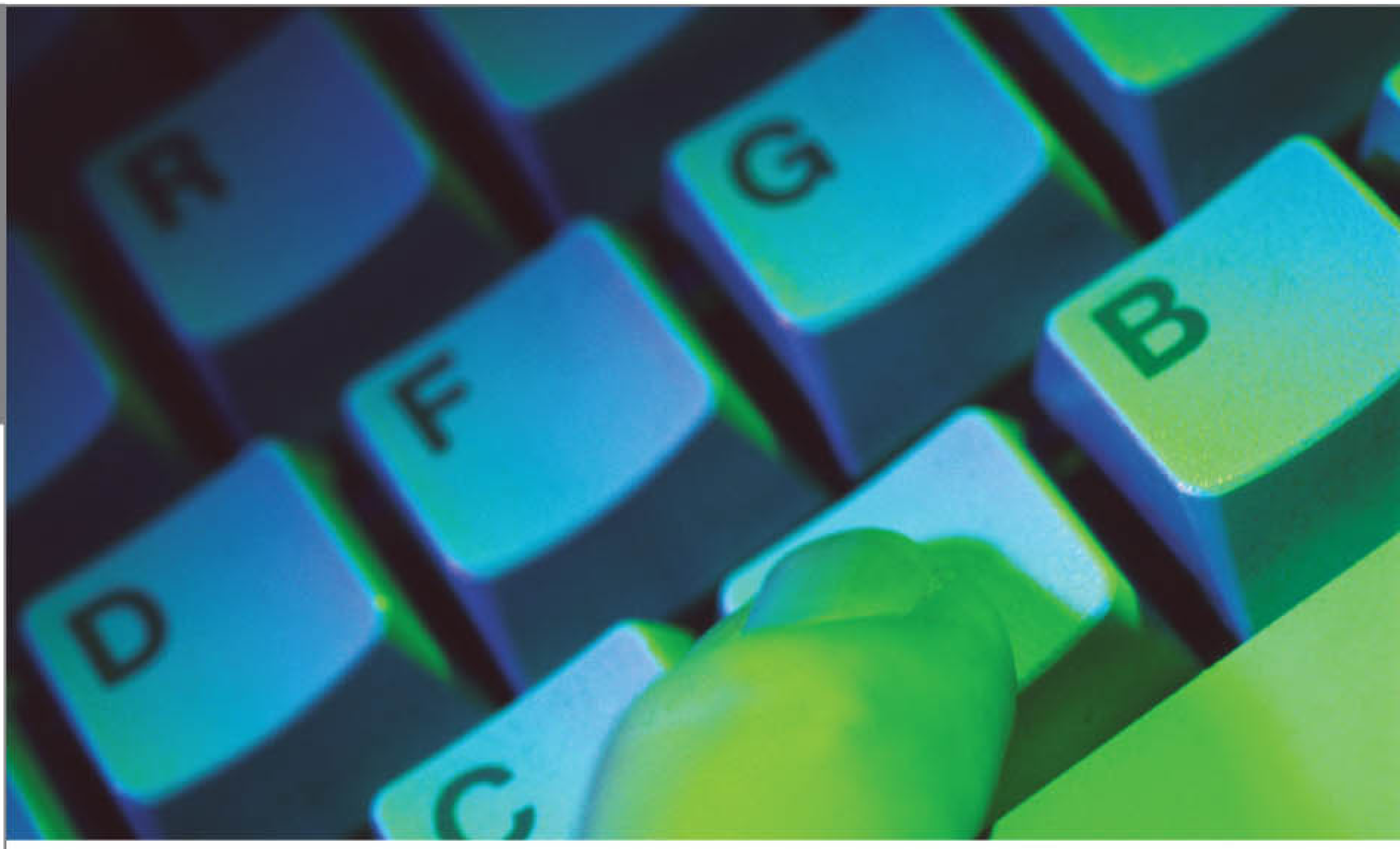
2) To observe attacker behaviour in order to learn new techniques being deployed, to determine the popular techniques that are currently being used as well as to confirm the continued use of old and well known attack techniques.

3) 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.

Attached some traffic analysis that we produced based on our observation on our Research Network for this quarter.

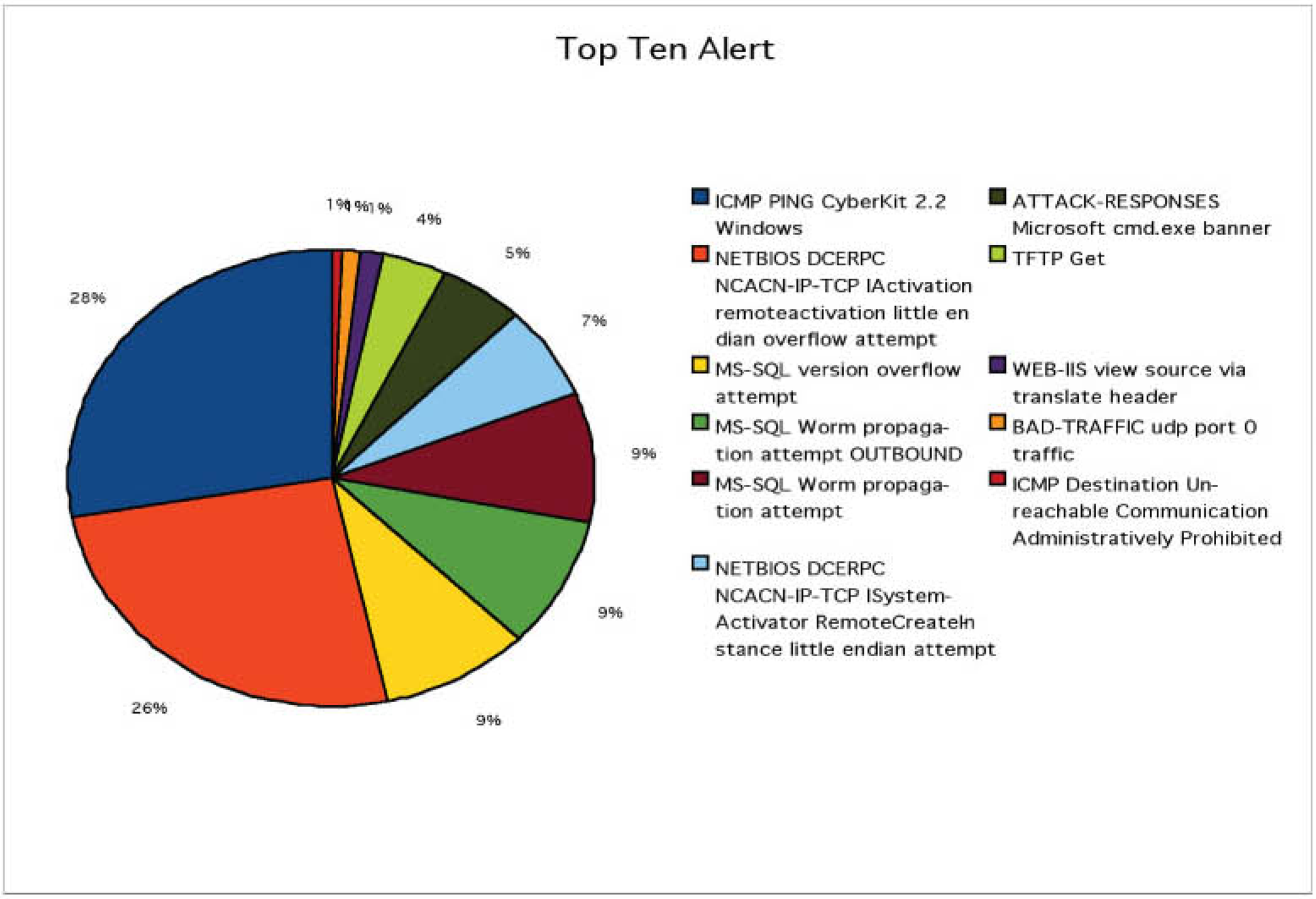
Top Ten Attacking IPs by Countries

Attacking IPs	Countries
58.124.XX.XX	Korea
60.11.XX.XX	China
62.118.XX.XX	Russia
69.43.XX.XX	United States
83.10.XX.XX	Poland
84.54.XX.XX	Iraq
87.23.XX.XX	Italy
88.87.XX.XX	Ireland
89.137.XX.XX	Romania



Top Ten Alert Generate

Alert Description	Count
ICMP PING Cyberkit 2.2 Windows	2433
NETBIOS DCERPC NCACN-IP-TCP IActivation remoteactivation little endian overflow attempt	2246
MS-SQL version overflow attempt	810
MS-SQL Worm propagation attempt OUTBOUND	810
MS-SQL Worm propagation attempt	810
NETBIOS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance little endian attempt	572
ATTACK-RESPONSES Microsoft cmd.exe banner	458
TFTP Get	351
WEB-IIS view source via translate header	119
BAD-TRAFFIC udp port 0 traffic	94
ICMP Destination Unreachable Communication Administratively Prohibited	62



Conclusion

Overall, the number of incidents reported to us had increased to 3.20% compared to previous quarter with incidents mainly contributed from spam incidents. Other reports that contributed highly to the number of incidents received are frauds consistingof phishings, suspicious online investments, ponzi schemes and malicious codes which consists of reports of botnets, control & command server, drone activities hosted on local machines. We advise System Administrators to take precautions on these activities and prevent their machines to become targets. Neither crisis nor outbreak was observed this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. We strongly advise users/organizations to report and seek assistance from MyCERT in the event of any security incidents.

MyCERT can be reached at:

E-mail : mycert@mycert.org.my
Phone : +603 89926969
(monitored during business hours)
Fax : +603 89453442
(monitored during business hours)
Handphone : +60 19 2665850
(24x7 call incident reporting)
SMS : +60 19 2813801 *(24x7 SMS reporting)*

Business Hours : Mon - Fri 08:30 -17:30 MYT
Web : http://www.mycert.org.my
Postal : 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

WINDOWS VISTA

FILE SYSTEM FORENSICS (PART 2)

INTRODUCTION

This is the sequel to my article that was published in the previous newsletter titled "Windows Vista File System Forensics (Part 1)". In the article, I highlighted that Microsoft has introduced significant amount of changes to its Windows Vista compared to its predecessor Windows XP. In this article, I am going to focus on one of the major changes in Vista that I found during the course of my research; i.e. the changes in the Thumbs.db database files. What follows hereinafter are only my findings from my research and I will include the analysis and discussion on my findings in the next newsletter.

THUMBS.DB ANALYSIS ON WINDOWS VISTA?

On a Windows Vista Ultimate machine, I created a directory called Vista and copied 10 JPEG image files into the directory. To my surprise the viewing mode on Vista has changed significantly. The view options are no longer like in XP. The options available are "**Extra Large Icons**", "**Large Icons**", "**Medium Icons**", "**Small Icons**", "**List**", "**Details**" and "**Tiles**" (refer to Figure 0).

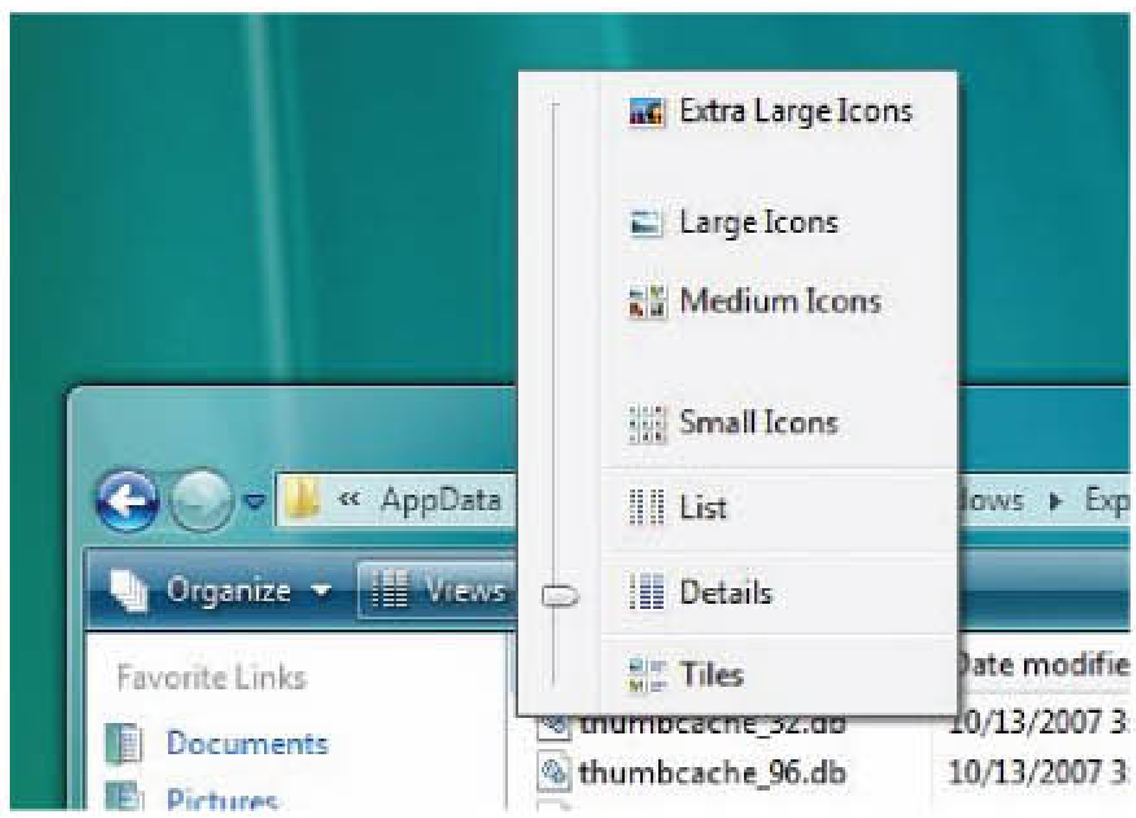


Figure 0: Explorer view options in Vista

THUMBS.DB ANALYSIS ON WINDOWS VISTA?

When I set the directory to thumbnail view mode (**View > Extra Large Icons** or **View > Large Icons**) there was no Thumbs.db file created, like in XP. Thus, I made a search for *.db files (Start > Search) and it returned a few hits. Among all the hits, I noticed a few *.db files that look similar to Thumbs.db files but with different names; i.e. **thumbcache_xxx.db**. Figure 1 below shows the files and the location of the files.

The path: C:\Users\siva\AppData\Local\Microsoft\Windows\Explorer

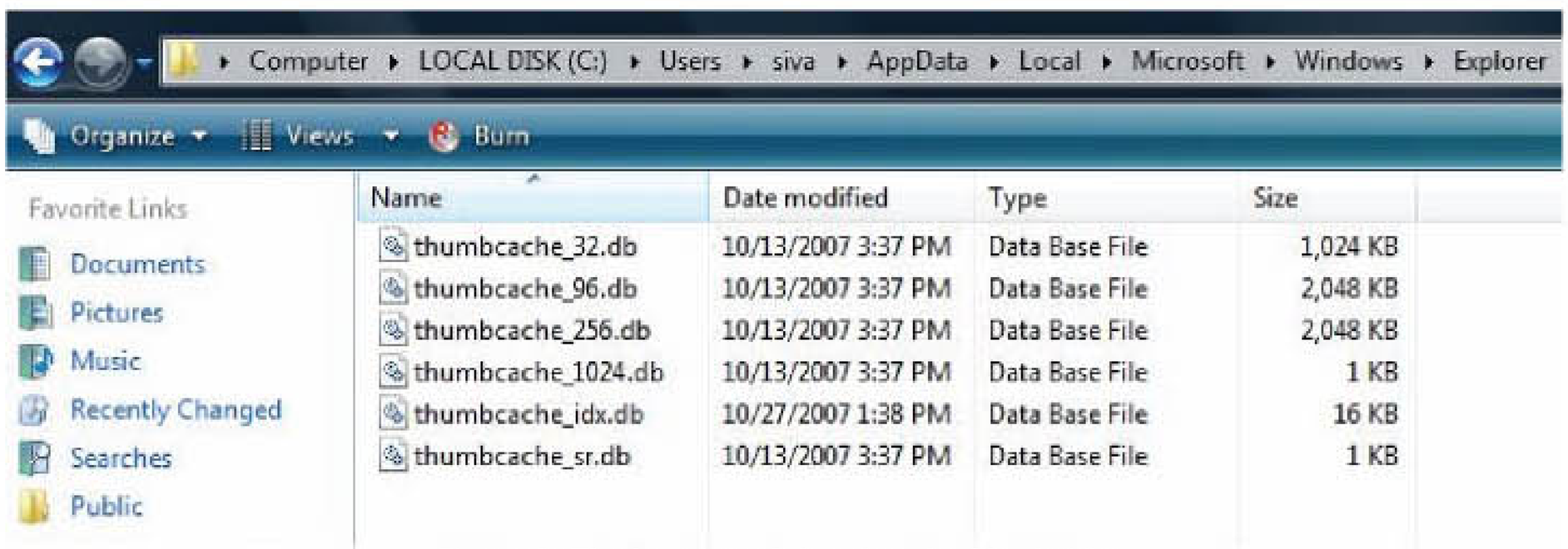


Figure 1: The location of thumbcache files in Vista

I tried to open these files with WFA (Windows File Analyzer – www.mitec.cz) but to no avail. WFA could not open the files and returned an error message saying *"thumbcache_xxx.db is not a thumbnail database"*. This appalled me and I tried opening the files using EnCase instead and I noticed a significant change in the file signature of thumbcache files. Figure 2 to Figure 7 below depict the snapshot of the file signatures of all the thumbcache files shown in Figure 1.

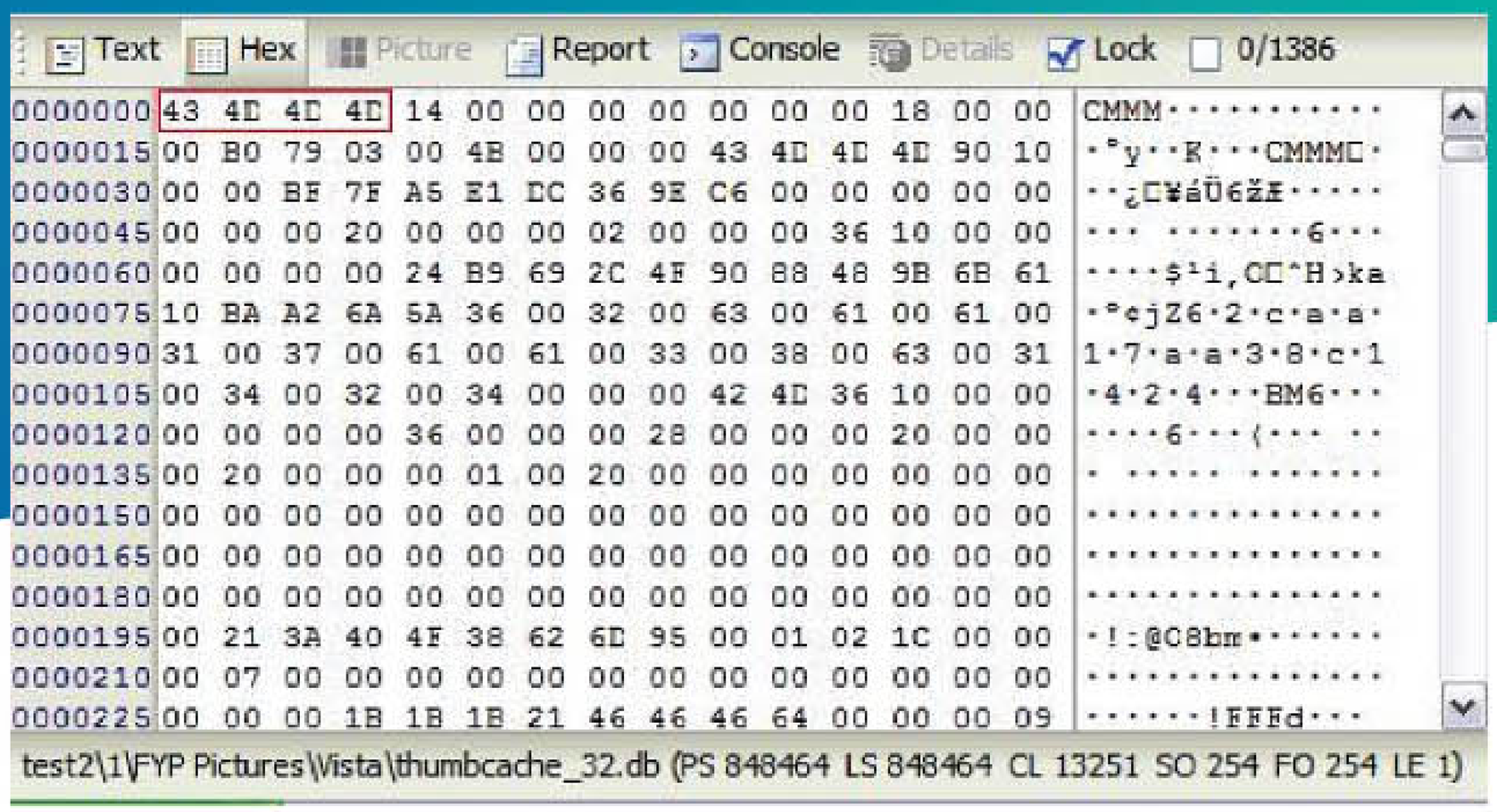


Figure 2: File signature of thumbcache_32.db

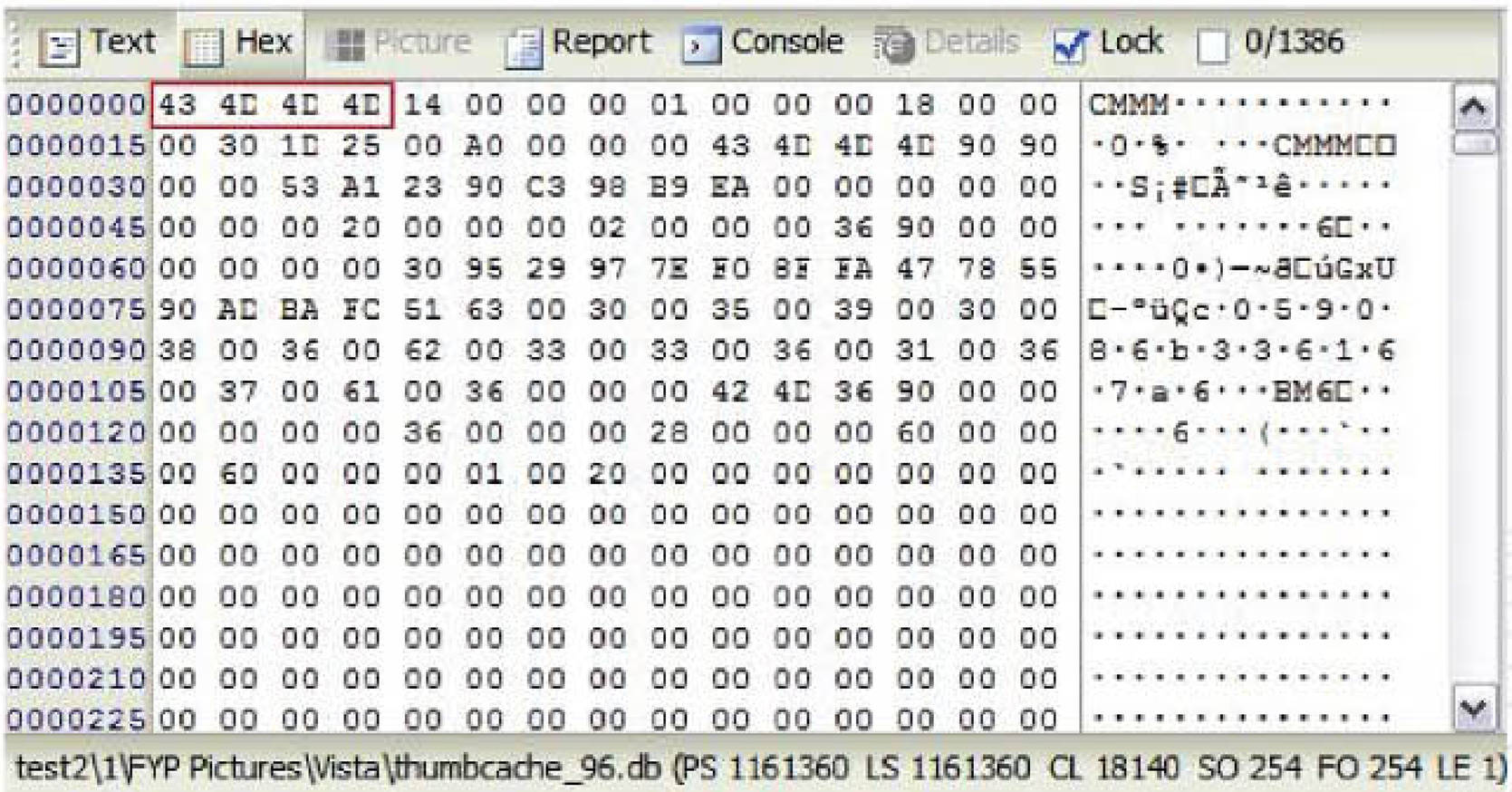


Figure 3: File signature of thumbcache_96.db

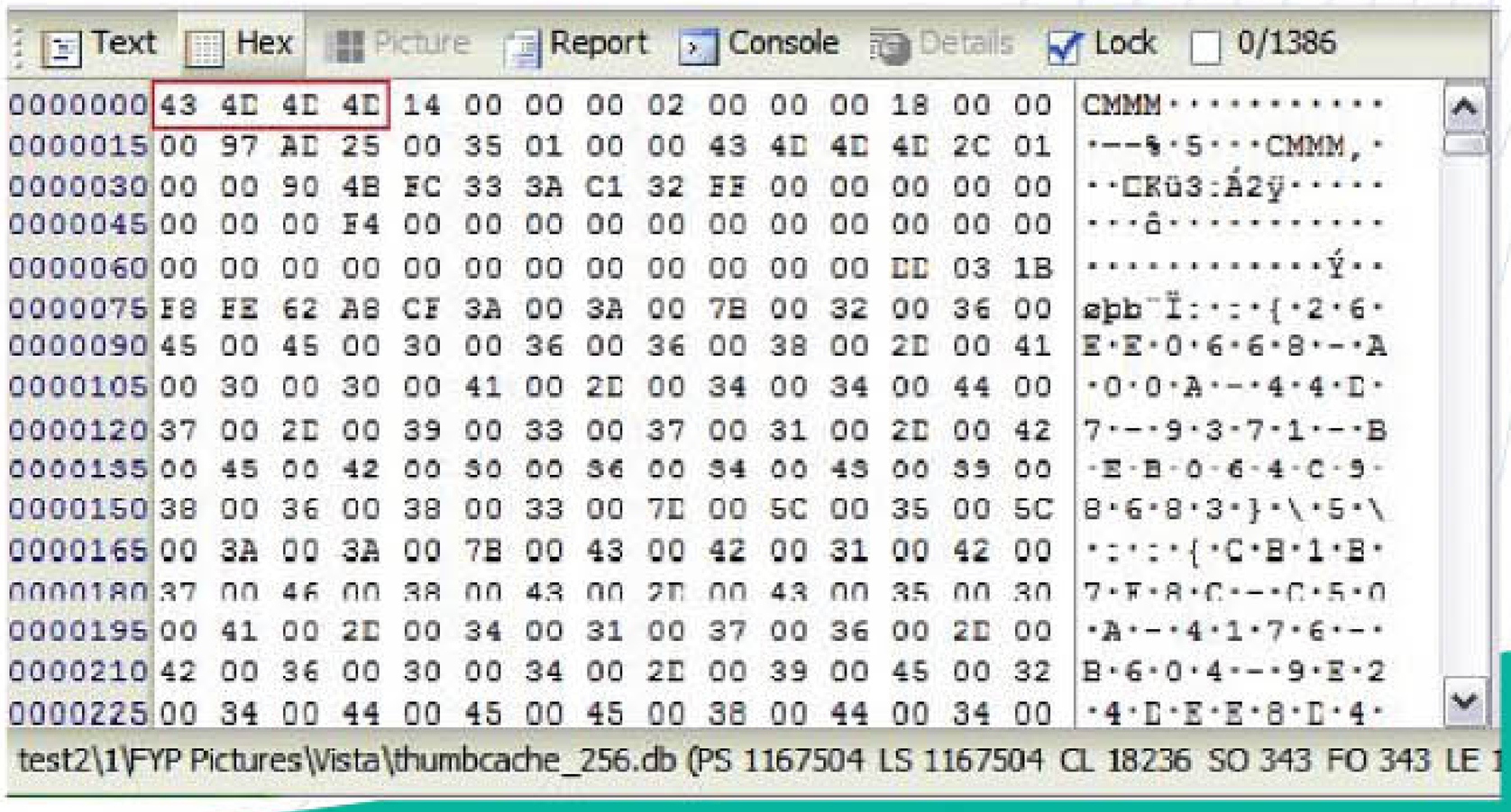


Figure 4: File signature of thumbcache_256.db

Text Hex Picture Report Console Details Lock 0/1386

```
00000 43 4D 4D 4D 14 00 00 00 03 00 00 00 18 00 00 00  CMMM............
00016 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00032 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00096 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00112 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00128 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00192 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00208 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00224 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

test2\1\FYP Pictures\Vista\thumbcache_1024.db (PS 1173648 LS 1173648 CL 18332 SO 350 FO 350 LE

Figure 5: File signature of thumbcache_1024.db

Text Hex Picture Report Console Details Lock 0/1386

```
00000 49 4D 4D 4D 14 00 00 00 00 00 00 00 37 01 00 00  IMMM........7...
00016 94 01 00 00 00 00 00 00 16 AB 4D C5 10 E7 54 77  ”........«MÅ·çTw
00032 00 54 06 AE 14 92 C7 01 00 00 00 00 00 50 03 00  ·T·®·’Ç......P··
00048 10 44 24 00 3B DF 23 00 FF FF FF FF FF FF FF FF  ·D$·;ß#·ÿÿÿÿÿÿÿÿ
00064 A5 89 1D 49 37 C6 30 0D 00 67 AA EA 60 10 C8 01  ¥‰·I7Æ0 ·gªê`·È·
00080 01 00 00 00 FF FF FF FF FF FF FF FF 0D DC 05 00  ····ÿÿÿÿÿÿÿÿ Ü··
00096 FF FF FF FF FF FF FF FF 3B 83 C1 C6 B7 F6 A0 44  ÿÿÿÿÿÿÿÿ;ƒÁÆ·ö D
00112 00 5F C5 20 BC DF C7 01 00 00 00 00 FF FF FF FF  ·_Å ¼ßÇ····ÿÿÿÿ
00128 FF FF FF FF F8 00 25 00 FF FF FF FF FF FF FF FF  ÿÿÿÿø·%·ÿÿÿÿÿÿÿÿ
00144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00192 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00208 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00224 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

test2\1\FYP Pictures\Vista\thumbcache_idx.db (PS 1173712 LS 1173712 CL 18333 SO 302 FO 302 LE 1)

Figure 6: File signature of thumbcache_idx.db

Text Hex Picture Report Console Details Lock 0/1386

```
00000 43 4D 4D 4D 14 00 00 00 04 00 00 00 18 00 00 00  CMMM............
00016 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00032 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00096 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00112 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00128 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00192 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00208 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00224 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

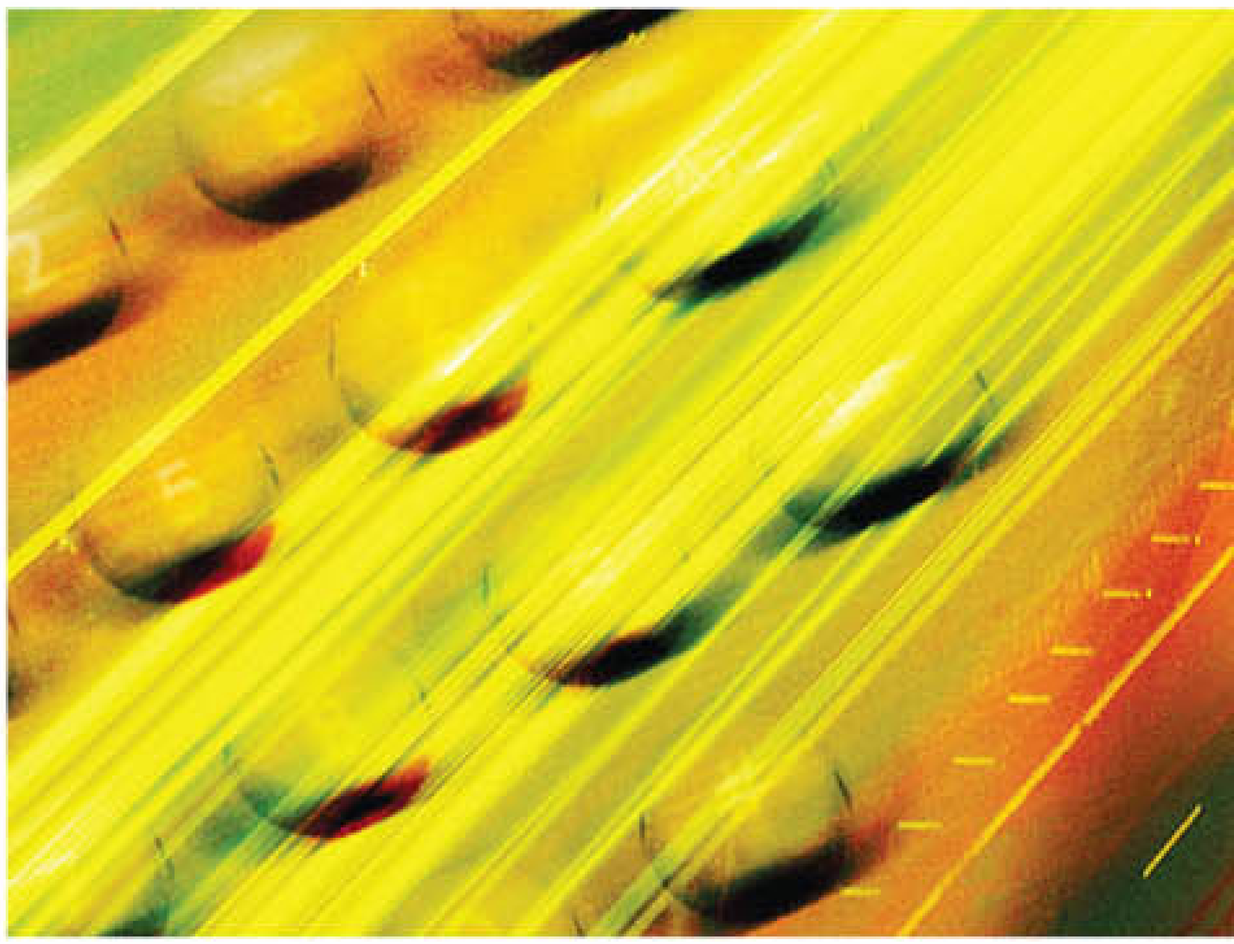
test2\1\FYP Pictures\Vista\thumbcache_sr.db (PS 1173776 LS 1173776 CL 18334 SO 286 FO 286 LE 1)

Figure 7: File signature of thumbcache_sr.db

Table 4.1 below summarizes the file signature of each and every thumbcache files found in the central repository directory.

Thumbcache File Name	File Signature
Thumbcache_32.db	43 4D 4D 4D
Thumbcache_96.db	43 4D 4D 4D
Thumbcache_256.db	43 4D 4D 4D
Thumbcache_1024.db	43 4D 4D 4D
Thumbcache_idx.db	49 4D 4D 4D
Thumbcache_sr.db	43 4D 4D 4D

Table 1: File signatures of thumbcache_xxx.db files



From the file signature analysis however, I could not conclude or find anything so I copied 37 more JPEG image files into the directory to inspect if there are any changes in any of the thumbcache_xxx.db files. The result was that the size of thumbcache_96.db file changed from 2,048KB to 3,072KB but the modified date of the file did not change as depicted in Figure 8 below.

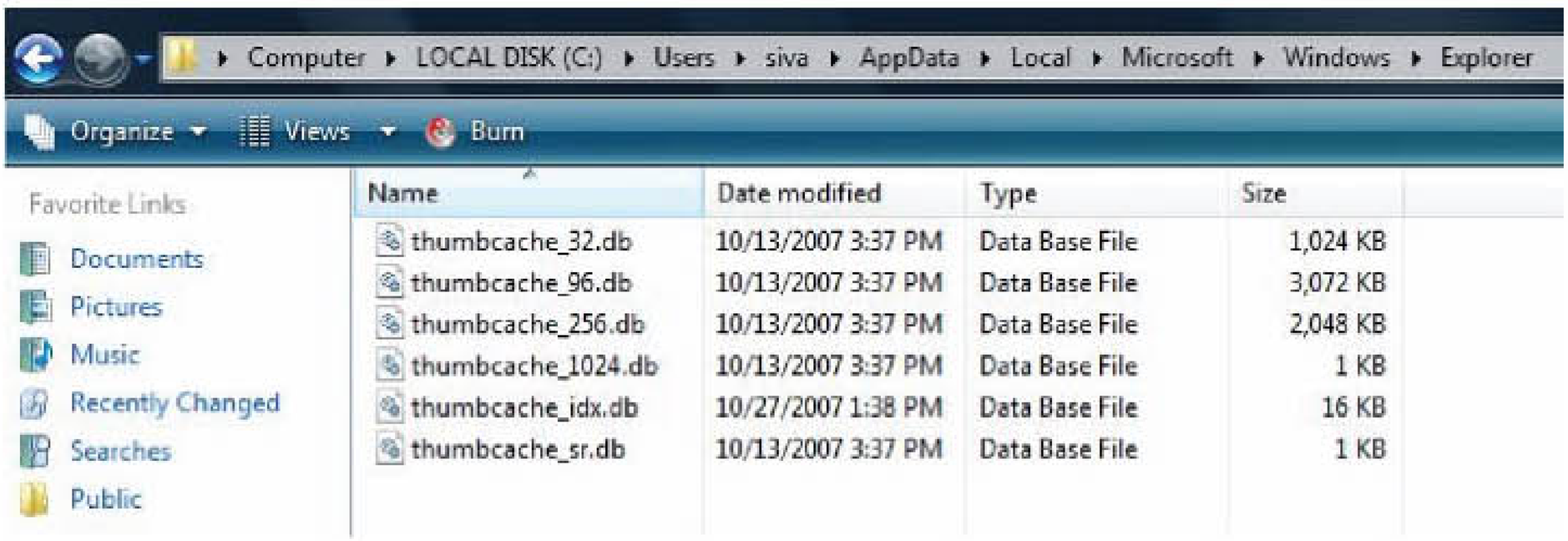
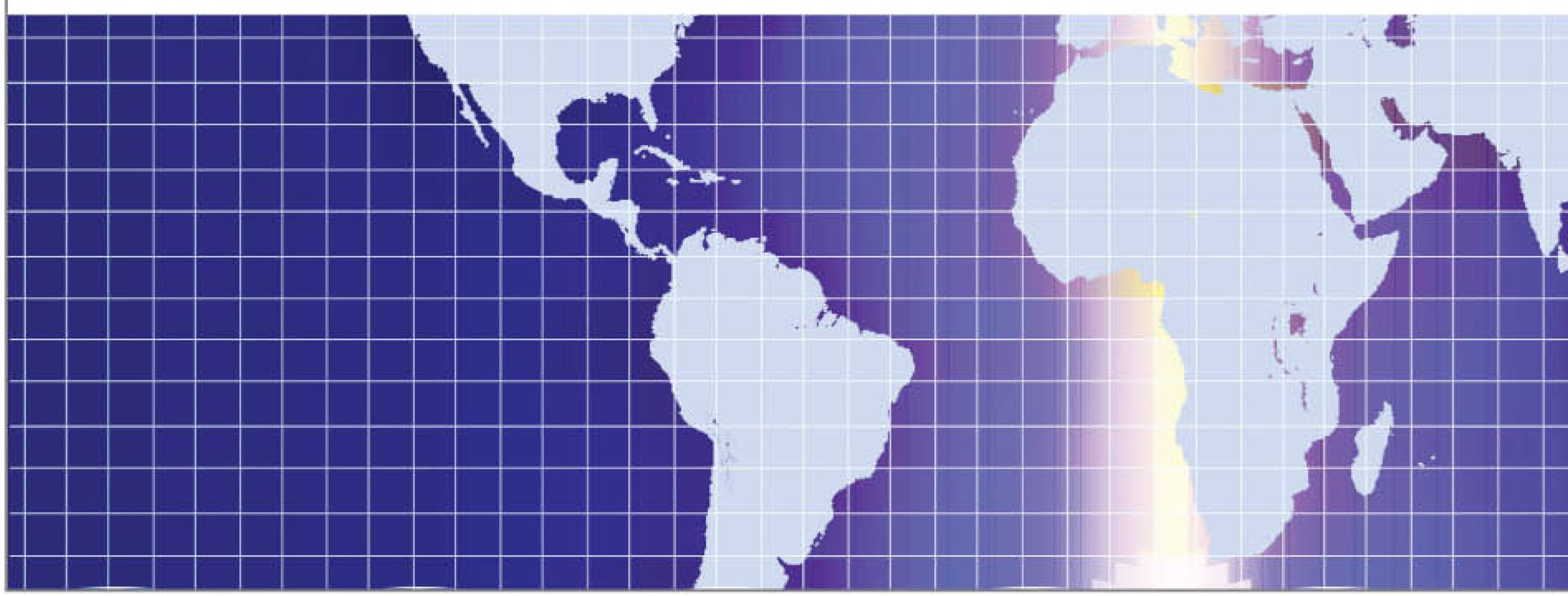
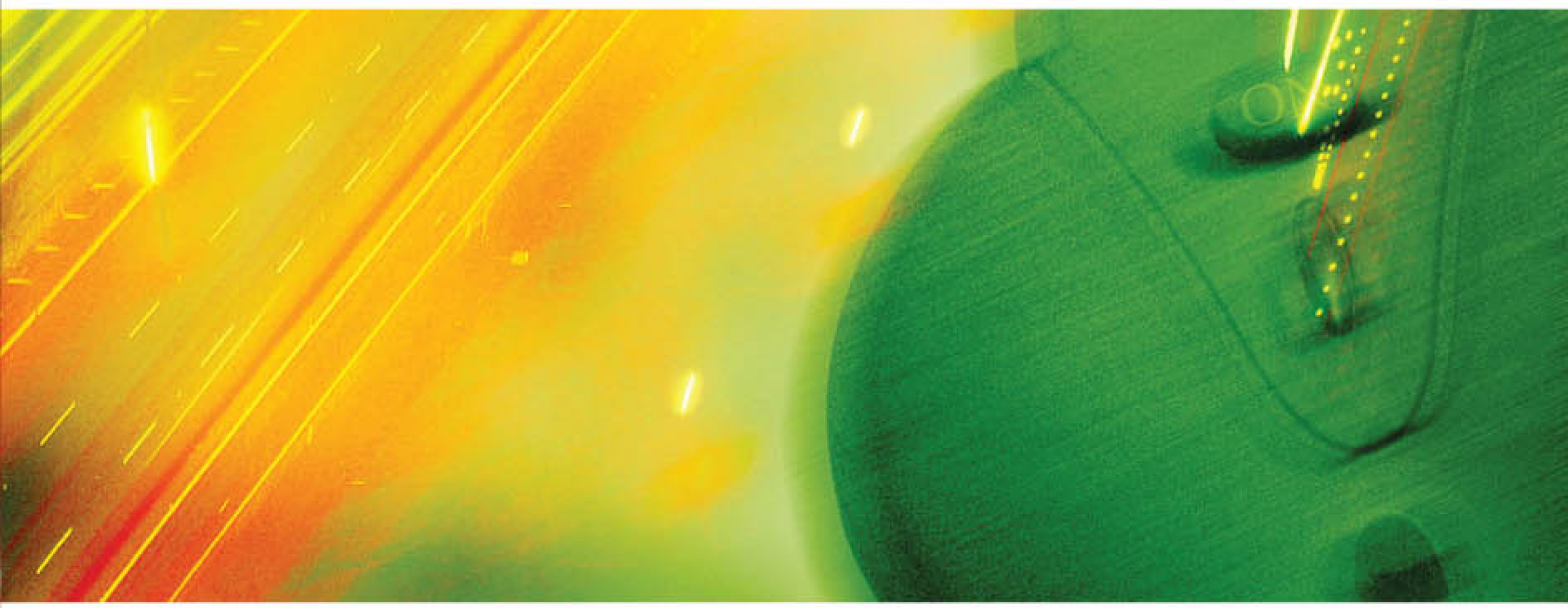


Figure 8: The changes in a thumbcache file after adding more JPEG images into the directory

Still, this result did not indicate anything so I ran a keyword search (using EnCase Forensics) for all the thumbcache_xxx.db files for the keyword "JFIF" (JFIF is the file header / signature for JPEG image files). It produced a very interesting result, whereby only the thumbcache_256.db file returned hits; a total of 140 hits. Figure 9 depicts the keyword search result.





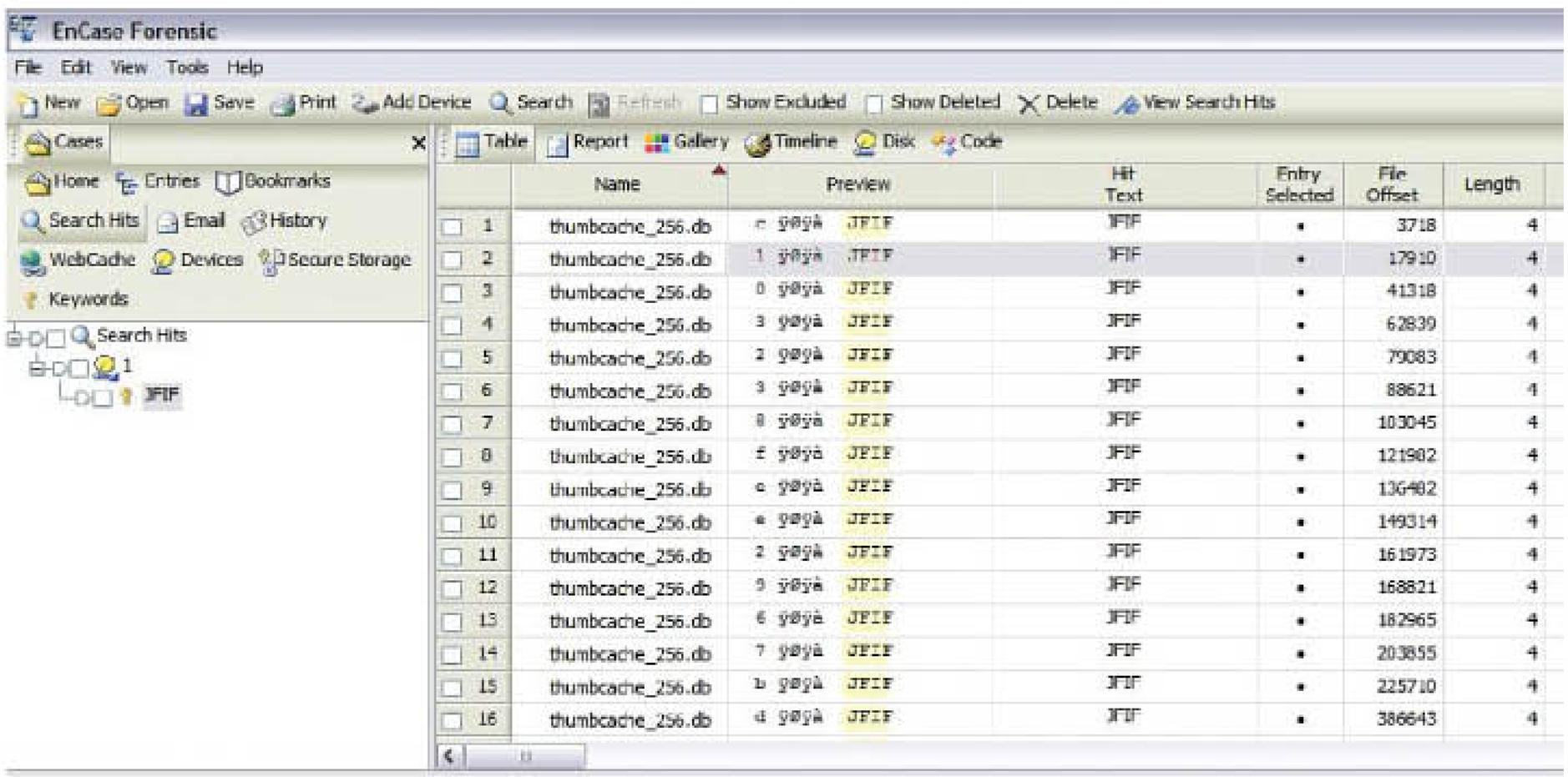


Figure 9: JFIF keyword search result for thumbcache files

CONCLUSION

It is clear that Microsoft has significantly changed the Thumbs.db database files in Vista. I presume that these changes are introduced to increase the performance of the OS. However, there are plenty other unanswered questions due to the lack of information of Vista's file system structure. I will cover the analysis and discussion on thumbcache_xxx.db in the next publication of this newsletter.

FORTINET®

PRESS RELEASE

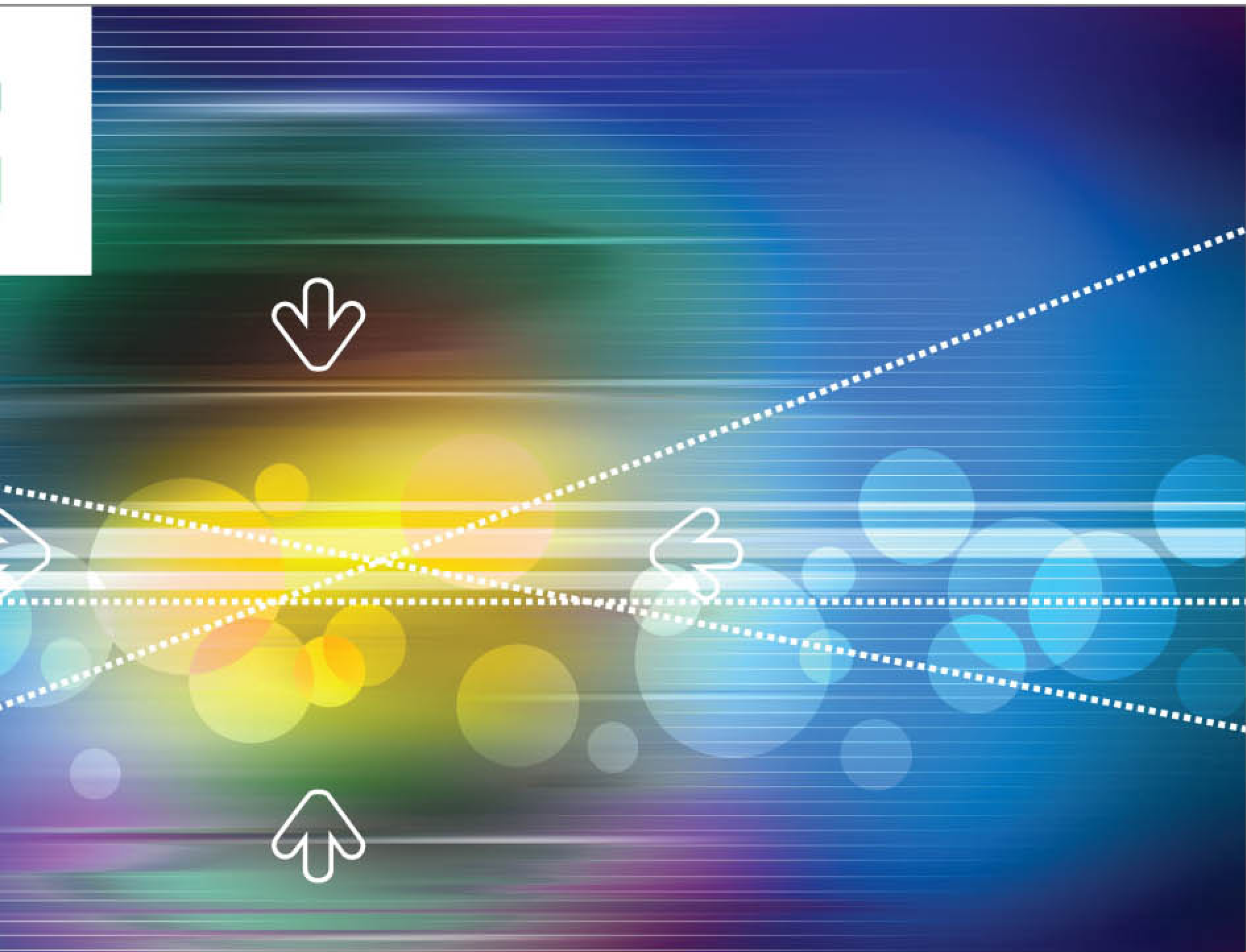
Media Contact:
Goh I-Vee or Cordelia Lee
AccentEdge Communications
+603 7728 0184
i-vee.goh@accent-edge.com

Fortinet Announces Top Reported Threats for November 2007

KUALA LUMPUR, Malaysia, 4 December 2007 – Fortinet – the pioneer and leading provider of unified threat management (UTM) solutions – today announced the top 10 most reported high-risk threats for November 2007. The report, compiled from all FortiGate™ multi-threat security systems in production worldwide, is a service of Fortinet's FortiGuard Global Security Research Team.

November 2007's top 10 threats, as determined by the degree of prevalence are:

Rank	Threat Name	Threat Type	% of Detections
1	W32/Netsky!similar	Mass mailer	10.87
2	HTML/Iframe_CID!exploit	Exploit	8.21
3	HTML/Clicker.AC!tr	Trojan	6.60
4	W32/ANI07.A!exploit	Exploit	5.14
5	W32/Stration.JQ@mm	Mass mailer	3.11
6	W32/MyTob.CJ@mm	Mass mailer	2.42
7	W32/Bagle.DY@mm	Mass mailer	2.25
8	W32/Grew.A!worm	Worm	2.09
9	Adware/TCent	Adware	1.86
10	Adware/Bdsearch	Adware	1.71



The November top 10 highlights the following:

The beginning of the holiday season led to the arrival of two new adware, TCent and Bdsearch, which reached the top ten for the first time this month. Meanwhile, Clicker.AC, which bypasses code to prevent browser pop-ups, claimed a solid third place.

Mass mailers dominated the top ten in November, remaining a strong threat. Netsky!similar represents the highest volume detected this month with 10.87 percent of the overall reported activity, whereas mass mailer MyTob.CJ, which first reached the top ten in October, and Bagle.DY maintained their level of activity and respectively reached the sixth and seventh positions.

Stration.JQ, absent from the monthly top ten since June, was back in force as November came to a close, jumping into fifth place from last month's 57th position.

For this holiday season, Fortinet security researchers not only reported a general increase in malicious online advertising – with the emergence of new adware such as TCent and Bdsearch – but also an increase in the sophistication of Internet threats in general. Clicker.AC, for instance, has code that is specifically designed to bypass browsers' pop-up blocking technology, which is supposed to block pop-up advertisements. Users who have pop-up blocking enabled should be suspicious if their browsers still display pop-ups. Clicker.AC "anti-anti-popup" technology is a good example of how pop-up generators and pop-up blockers are engaged in an arms race, much like spam filters and spam generators.

Such malware can however be stopped by advanced antivirus solutions, such as the features found in Fortinet's UTM appliances, which will detect and block Clicker.AC before it attempts to circumvent the computer's pop-up blocking features.

Another example of the increasing sophistication of malware is Stration.JQ, which relies on an advanced social engineering strategy based on dual attachments. While the email received by end users aims at misleading them by providing instructions for personal account access, the innovation lays in the attachments: an "authorization module", which is in fact Stration.JQ, coupled with a PDF attachment containing financial information such as an invoice, a fee analysis, etc. The content of the email and PDF are both intended to stir the user's curiosity and make the request sound legitimate, therefore tremendously increasing the click-through rate of the mass mailer. Unfortunately, any user opening the "authorization module" will turn her/his computer into a bot.

"Hacking legitimate site content to host malicious code has become very common. This month, many trusted Internet sites were unwittingly 'hosting' flash advertisements injected with encrypted redirects, forcing users to visit other sites once the ad was displayed. More determined efforts to conceal malware using trusted sources are likely to be made as we enter into the busy holiday season of December," said Derek Manky, security research engineer at Fortinet. "Examples of adware such as Clicker.AC illustrate the trend in what is becoming the blend between malware and grayware and further emphasizes the need for threat awareness, not only from the end user's perspective, but also for corporations and their affiliates."

To read the full November report, please visit
http://www.fortiguardcenter.com/reports/roundup_nov_2007.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.

About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS, and Anti-Spyware). Fortinet is privately held and based in Sunnyvale, California.

Fortinet is a registered trademark of Fortinet, Inc. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are trademarks of the Fortinet, Inc. in the United States and/or other countries. All other trademarks referred to herein are the property of their respective owners.

Implementing Security Awarene

This is the final part of the Security Awareness series. The first part describes the importance of having a security awareness programme for organisations and the benefits to be derived from having such programmes. The second part describes the processes involved in planning and assessing the need for such a programme. The third part focuses on designing an effective awareness programme. The fourth part focuses on the methods and the techniques for developing an effective programme that meets the need of the employee and the organisation's security objective. This part will conclude the series by addressing the some of the techniques for implementing the security awareness and also some of the constraints to be considered.

The security awareness programme should be developed with the users in mind in order to successfully meet the security needs of the organisation. Once the development is completed, the implementation of the programme need to be carefully planned and resources required for the rollout need to be identified.

The awareness programme implementation should be communicated to all those are involved to ensure the programme objectives are met and support is gained, especially from department heads or managers. Without the support of the staff, the programme can be difficult implement as they will not be ready to accommodate the security awareness resources, especially if a formal training is to be conducted. Therefore it is crucial that the most suitable communication channel must be determined in order to effectively reach as many staff as possible.

A security awareness programme should only be implemented when the programme delivery plan and awareness materials have been completely developed and agreed by the top management. The focus should be more on how to strategically inform the target audience the security messages to be delivered, and also to consider the possible obstacles to the programme implementation. This can be the most challenging part as you need to understand the needs of the target audience and this is where the needs assessment of current awareness level is to be conducted at the earlier stage of the awareness programme. There is no definitive method to a successful implementation but a careful study on effectiveness of using various communication channels based on your environment should be conducted, e.g., those staff working away from office, they may not be able to attend an instructor-led session. For this group, the most suitable communication channel could be the web or via e-learning.

ss Programme for Organisations

The following are some of the communication channels that can be used for implementation, but not limited to:

- Trinkets or stationeries with short security messages
- Posters describing various security issues with safety tips and best practices
- Computer screensavers with security messages
- Regular Awareness newsletter
- Emails with security messages as part of the signature
- E-learning or Web-based learning
- Instructor-led sessions
- Awareness activities, e.g. Crossword puzzles, Games
- Best practice guides/Brochures
- PC Security Checklist
- Teleconferencing sessions

As mentioned there are many communication channels or techniques that can be used for implementing the awareness programme. Some requires more resources to develop such as awareness newsletters, e-learning or instructor-led, whereas trinkets with security messages and screensavers are easier to develop and disseminate. Also some of the resources developed may be more appropriate for one environment or group, but may not be suitable for another, e.g. Teleconferencing sessions may not be suitable if your organisation does not have the necessary equipment or slow internet connection, or emails with brief security messages may be suitable for computer literate users but may not be suitable for novices users where more elaborate information would be helpful for them.

Formal instructor-led awareness programmes are usually conducted in a classroom mode, the messages can be complimented with awareness trinkets, posters or reference to awareness websites, to further enforce and to be continuously updated with new information. This would enable increased retention rate of the target audience. The

awareness program should not be delivered once to the said target audience. They must be nurture over a period of time to achieve full understanding of the concepts and issues to be covered in the awareness programme. It must be noted that when a staff is said to be fully "aware" or have achieved that, it means that their behaviour or their approach has changed in order to secure systems, application and themselves. The current security culture must be considered and the awareness drivers must accept the fact that it takes time to for the staff to change, especially those who lack IT or computer knowledge. A formal evaluation and feedback mechanism must be put in place.This assessment of current situation and post-awareness would enable you to assess and understand the effectiveness of the programme to date. Improvements cannot be made if the current progress or state of the programme is unknown. It is important that the programme should be continuously reviewed and amended especially if right messages are not reaching the target audience. Some of the feedback mechanisms that can be utilized are evaluation form with questionnaires, having discussion groups, conducting interviews and observation.

Expected outcomes of the programme can only be realized if the implementation is well delivered and expected results are communicated to all concerning staff. It is easy to develop an awareness programme but to reach the target audience can be a challenge task for all parties concerned. The developed awareness resources and programme must be continuously updated taking into account the current information system technology advancement, IT infrastructure and organizational changes. The awareness programme must be relevant and continuous improvements must be made to keep the awareness programme going and those involved must ensure that this is done.

REFERENCES:

European Network and Information Security Agency (ENISA), June 2006,
A User Guide: How to Raise Information Security Awareness: ENISA publication

Rasmussen, Gideon T, 2005.
Building a Security Awareness Programme-Addressing The Threat From Within.
Published by CyberGuard Corporation.
Available from:
http://www.gideonrasmussen.com/article-01.html
[Cited 26 November 2007]

Wilson, M., Hash, J., October 2003.
Building an Information Technology Security Awareness Program
Available from:
http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
[Cited 26 November 2007]

Risky Business: Consumers in the Workplace

In the not-too-distant past, stealing time for a personal call or quietly extending a lunchtime trip to the mall were the riskiest private behaviors in the workplace. In just a few years, the ubiquity of Internet commerce, the rise of telecommuting, and the arrival of online communities in the social mainstream have blurred the lines between home and work. Despite corporate efforts to limit personal Internet access, online banking, commerce, and Web surfing during the workday are now the norm. Many employers even encourage consumer behavior in the office, through Intranet-based shopping, healthcare, and financial services portals, or through employee-only deals with external retailers.

Broadband Internet connections at work may increase employee morale, but the risks they bring can be devastating. Business networks provide a "perfect storm" for cyber criminals capable of breaching their defenses. Large numbers of computers with high speed access make networks lucrative targets for botnet farmers recruiting "zombies." Sensitive information such as customer data, intellectual property, and email archives can be sold on the black market or used for extortion. Any PC is valuable to a cyber criminal. Networked PCs are orders of magnitude more so.

For less than $1000, cyber criminals can purchase the toolkits necessary to inject malware through an infected Web page. Time spent crafting that page into a convincing, compelling forgery targeted at a specific company or type of user ("spear phishing") is well worth the effort. Further complicating matters, users report that they feel more comfortable opening email attachments and performing other risky behaviors at work, because they feel protected by corporate IT and antivirus tools.[1] In August, 2007, using a single compromised account, criminals stole names, email addresses, and other private personal information on nearly 1.6 million jobseekers from monster.com.[2] In late 2005, spear phishers targeted CEOs and other executives at credit unions.[3] As cyber crime becomes better organized, corporate attacks will continue to grow. Today's cyber criminals are profit driven, and corporate networks are a jackpot.

Internet crime may be less public than other data theft (for example, the theft of a laptop and hard drive from the Veteran's Administration in 2006[4]), but it is no less damaging. A successful Web attack can lead to millions of dollars in customer notification and compensation costs, legal fees and judgements, and regulatory fines. It can also compromize brand loyalty, diminish employee productivity, and jeapordize critical intellectual property and competetive advantage. Safeguarding the network against malware is essential, and doing so requires reining in risky user behavior in the office.

References:

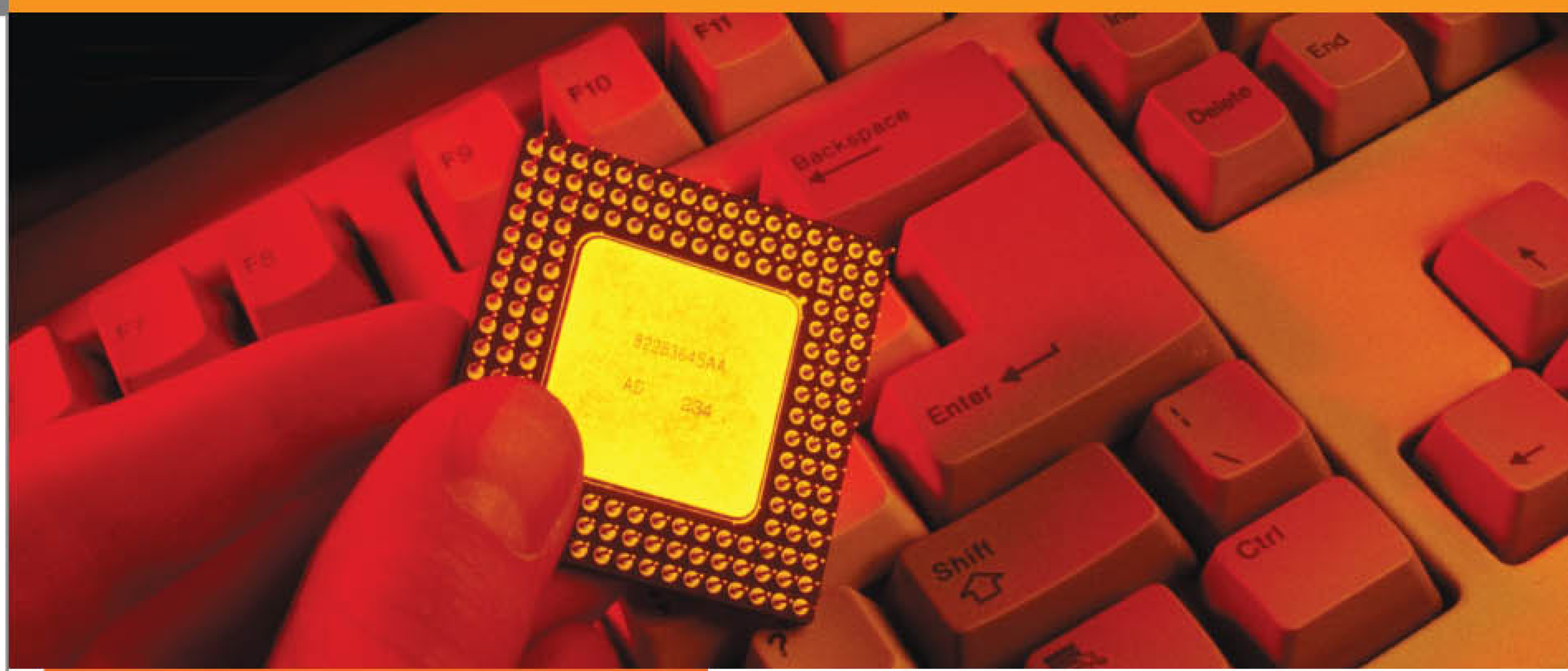
TrendLabs 1H07 Threat Report

"Here There Be (Monsters) Trojans,"
Jasper Pimentel, TrendLabs Malware Blog,
http://blog.trendmicro.com/here-there-be-28monsters29-trojans , August 22, 2007,

"Spear Phishing Attack Targets Credit Unions,"
Paul F. Roberts, eWeek.com,
http://www.eweek.com/article2/0,1895,1902896,00.asp
[December 16, 2005]

"Stolen VA Laptop and Hard Drive Recovered,"
Christopher Lee and Zachary A. Goldfarb,
The Washington Post,
http://www.washingtonpost.com/wpdyn/content/article/2006/06/29/AR2006062900352.html
[June 30, 2006]

STRATEGIC INITIATIVES TO PROTECT CONTROL SYSTEMS (SCADA/DCS)



Abstract

In the previous bulletin (E-Security, Volume 11-Q2/2007), we have explained the importance of securing the control systems (SCADA/DCS) as based on the facts that these systems are widely converging towards Internet Protocol (IP) based systems. The practice that SCADA/DCS systems are interconnected with the corporate network has also increased, thus open to common vulnerabilities and attacks, including internet attacks.

We have reviewed a few countries that have embarked on the SCADA/DCS systems protection programs for their critical infrastructures. We have decided to provide our review of United State of America (USA) strategic initiatives and programs that could provide valuable inputs in developing our SCADA/DCS Security Program for our Critical Infrastructures. The review is compiled according to National and Industry Initiatives, and National and International Standards and Guidelines.

NATIONAL AND IND

Strategy

In 2003, the President's National Strategy to Secure Cyberspace (NSSC) established a role for the Department of Homeland Security (DHS) to coordinate with the private sectors and other government to improve the cybersecurity of control systems.1 Under Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program, the document cites,

"Securing DCS/SCADA is a national priority. Disruption of these systems can have significant consequences for public health and safety. However, securing these systems is complicated by various factors. First, adding security requires investment in systems and in research and development that companies cannot afford or justify on their own. Such research may require the involvement of multiple infrastructure operators or industries. Second, current technological limitations could impede the implementation of security measures." (Page 32)

The strategy document has also emphasized public and private sectors roles to work in partnership to ensure broad awareness among industry vendors and users, both regulated and unregulated. And the development of adequate test bed environments and the development of technology will aid in the effort to secure SCADA/DCS.

The strategy has summarized the Action and Recommendation for SCADA/DCS security as cited in :

"A/R 2-5: DHS, in coordination with DOE (Department of Energy) and other concerned agencies and in partnership with industry, will develop best practices and new technology to increase security of DCS/SCADA, to determine the most critical DCS/SCADA-related sites, and to develop a prioritized plan for short-term cybersecurity improvements in those sites." (Page 56)

The result from the strategy has derived DHS to provide the implementation plan under its "National Infrastructure Implementation Plan" (NIPP)2 document. The NIPP provides the coordinated approach that will be used to establish national priorities, goals, and requirements for Critical Infrastructure and Key Resources (CI/KR) protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents.

USTRY INITIATIVES

Amongst the stakeholders are Government, National Labs and Research Institutes and Industry. The following lists are currently addressing the SCADA/DCS cyber security programs:

GOVERNMENT

DHS Control Systems Security Program (CSSP)

DHS National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP). The CSSP coordinates efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk.

US-CERT Control Systems Security Center (CSSC)

The Control Systems Security Center (CSSC) is a state-of-the-art analysis and testing facility that works to provide proactive means for securing the control systems that operate many of the nation's critical infrastructures.

CSSC is tasked to identify technology gaps and operational security needs related to control system security and report these to DHS Science & Technology on areas of consideration for developmental efforts.

DHS Process Control Systems Forum (PCSF)

The purpose of the PCSF is to accelerate the design, development, and deployment of more secure new and legacy control systems. PCSF participants include international stakeholders from government; academia; industry users, owner/operators, and systems integrators; and the vendor community. The PCSF is an open, collaborative, voluntary forum that will leverage and unify the experience,capabilities, and contributions of these stakeholders through meetings, interest groups, and working groups, to develop and adopt common architectures, protocols, and practices.

Dept of Energy, USA - "Roadmap to Secure Control System in the Energy Sector"

The Roadmap is designed to address the full range of needs for protecting the cyber security of legacy and advanced control systems across the electric, oil, and natural gas sectors (including the supporting telecommunications infrastructure). It aims to define a consensus-based strategy that articulates the cyber security needs of owners and operators in the energy sector; Produce a comprehensive plan for improving the security, reliability, and functionality of advanced energy control systems over the next 10 years; and Guide efforts by industry, academia, and government and help clarify how each key stakeholder group can contribute to planning, developing, and disseminating security solutions.

NATIONAL LABORATORIES

Idaho National Laboratories - National SCADA Test Bed

Department of Energy (DOE) established the National SCADA Test Bed (NSTB) to help the energy sector and equipment vendors assess control system vulnerabilities and test the security of control systems hardware and software. NSTB was developed back in 2004 with the DOE's fund of USD2 Million and the funds were increased to USD5 Million in 2005 and USD10 Million in 2006. At least, there are four (4) SCADA test beds that was sponsored and equipped by SCADA vendors, i.e. ABB, GE, Siemens and OSI. The SCADA systems were fully sponsored including the redundancy (backup) hardware and software. There are two (2) assessment approaches used in this lab. First, Test Bed Assessment: To perform cyber vulnerability assessments with the primary SCADA vendor in the test lab environment. Second, On-site Assessment: To perform cyber vulnerability assessments at operational sites to validate test bed results and confirm applicability of recommended solutions.

Sandia National Laboratories - Center for Control System Security

The Center for Control System Security is composed of several test bed facilities, which allow real-world critical infrastructure problems to be modeled, designed, simulated, verified, and validated. These labs are integrated into a research effort focusing on solving current control system security problems and developing next generation control systems.

SCADA RESEARCH & INDUSTRY PROJECTS

Institute for Information Infrastructure Protection (I3P) : Process Control Systems Project

The I3P is a consortium of leading national cyber security institutions, including academic research centers, government laboratories, and non-profit organizations. I3P has embarked on the "Process Control Systems Security Research" project. The project is focusing cyber security related research at some of the country's top institutions on improving the robustness of the information infrastructure in the oil and gas sector. Eleven institutions from across the country have joined forces to develop new solutions and demonstrate their effectiveness to the oil and gas sector owners, operators, and vendors.

Digital Bond Inc. : SCADA Security Research projects and SCADA Security Scientific Symposium (S4)

A research and consulting practice, Digital Bond Inc., founded by Dale Peterson has recent SCADA security research projects include:

- SCADA Network IDS Signatures - Modbus, DNP3 and ICCP signatures were developed for the Snort IDS and have been ported to most major IDS including ISS, Cisco, and McAfee.

- SCADA Nessus Plugins - Tenable Security funded the development of SCADA plugins for the extremely popular Nessus Vulnerability Scanner. These feeds are already available in the Nessus Direct Feed.

- SCADA Honeynet - Developed a PLC honeypot and integrated this with technology from the Honeynet Project to create a SCADA Honeynet. The solution is easily deployable as VM server images and requires little knowledge of honeynets or PLC's. The project is also to monitor SCADA Honeynets in detecting and analyzing attack data.

- SCADA Vulnerability Disclosure – Identified much vulnerability in the research and consulting engagements. After multiple vendors were not responding with timely patches or customer notification, Digital Bond decided to exercise the US-CERT/CERT organizations for vulnerability disclosure. This has resulted in patches and the first control system vulnerabilities published by US-CERT/CERT.

- SCADA Security Event Monitoring - Developed a Data Dictionary that normalizes these events and provides the pattern a SEM or MSSP can use to detect the events in a variety of SCADA systems.

Digital Bond has conducted the SCADA Security Scientific Symposium (S4) which is a unique event for the presentation of highly technical research papers on SCADA and control system security. The next coming event will be on January 23-24, 2008 in Miami Beach, Florida.

SCADA SECURITY STANDARDS & GUIDELINES

- **The Instrumentation, Systems and Automation Society : ISA99 Manufacturing and Control Systems Security Standards**

The ISA99 Committee will establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance. Guidance is directed towards those responsible for designing, implementing, or managing manufacturing and control systems and shall also apply to users, system integrators, security practitioners, and control systems manufacturers and vendors.

ISA99 has completed work on its Part 1 standard, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models. In addition, ISA99 has recently completed an update of a Part 2 standard, Security Technologies for Manufacturing and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.

There are four (4) Working Groups involved in the development of this standard, namely: WG1 - Security Technologies for Manufacturing & Control Systems (Technical Report 1); WG2 - Integrating Security into the Manufacturing & Control Systems Environment (Part 2 Standard); WG3 - ISA-99 Part 1 Standard; WG4 - Specific Requirements for Industrial Automation and Control Systems (Part 4 Standard).

- **National Institute of Standard and Technology : NIST SP800-82 "Guide to Industrial Control Systems (ICS) Security, 2nd Public Draft**

NIST SP800-82, second public draft document was released in September 2007. The document provides guidance for establishing secure industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. The document also provides an overview of ICSs and typical system topologies, identifies typical threats and vulnerabilities to these systems and provides recommended security countermeasures to mitigate the associated risks.

NIST has initiated the Industrial Control System Security project in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

- **North American Electric Reliability Council (NERC) - NERC Cyber Security Standards, (CIP 002-009)**

NERC plays a major role in protecting the electric system by serving as the focal point for coordinating information exchange on critical infrastructure issues between the electricity industry and the federal government. Through NERC, government and industry work together to protect the electricity infrastructure from physical and cyber attacks. NERC adopted Cyber Security Standards CIP-002-009 in 2006. The standards establish the minimum requirements needed to ensure the security of electronic exchange of information needed to support the reliability and the bulk power system. The multi-year implementation schedule establishes the milestones for compliance by the electric sector's owners and operators.

Through NERC, Electricity Sector Information Sharing and Analysis Center (ESISAC), who provides Security Guidelines for Electricity Sector addresses topics including vulnerability and risk assessment, business continuity, physical and cyber security, and protecting sensitive information. This center is also function to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions.

American Petroleum Institute (API) Standard – SCADA Security Standard and Guidelines

The SCADA Security standard, API 1164, first edition was released in September 2004. This standard provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. Although the standard does address physical security, the primary thrust of this document is cyber security and access control.

There are a few of security guidelines released by API that can be used by Oil and Gas industry such as:

- Security Guidelines for the Petroleum Industry, (April 2003) – Part VII : Security Guidelines for Cyber/Information Technology (IT) in the Petroleum Industry (Page 123)
- Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition (October 2004), by API and National Petro chemical & Refiners Association (NPRA) – the document describes an approach for assessing security vulnerabilities that is widely applicable to the types of facilities operated by the industry and the security issues
- Security Guidelines for the Petroleum Industry, (April 2005) – Chapter 7 : Information (Cyber) Security (Page 30)

American Gas Association (AGA) Standard 12, "Cryptographic Protection of SCADA Communications"

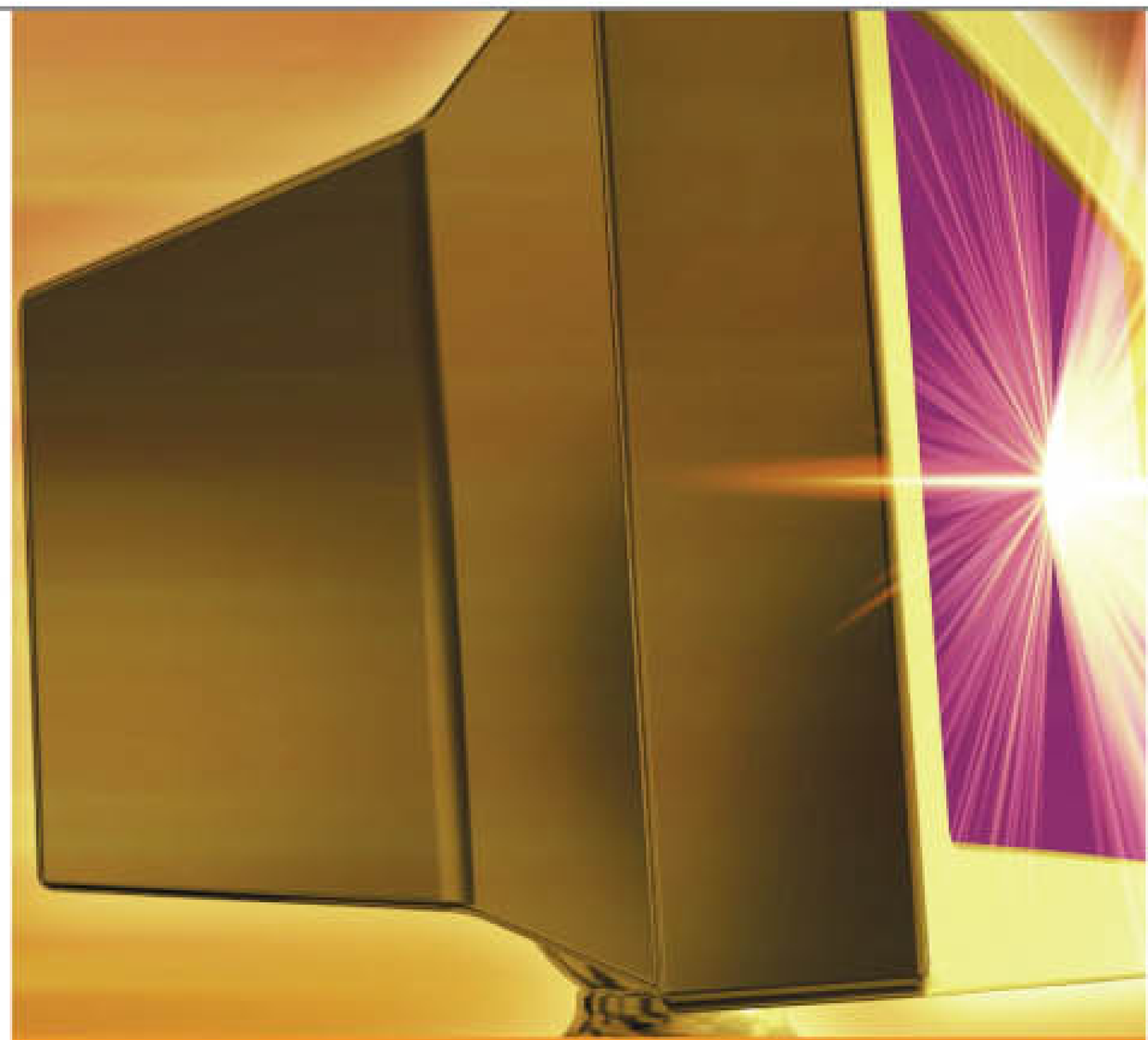
The AGA 12 series of documents recommends practices designed to protect SCADA communications against cyber attacks. The recommended practices focus on ensuring the confidentiality of SCADA communications by using cryptography. Note that AGA 12 is a voluntary standard and does not mandate any companies to install encryption technology as recommended by the standard.

Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0 – by American Chemistry Council's Chemical Information Technology Council (ChemITC)™,

This document was released in May 2006. The document was the enhancement of guideline documents developed by Chemical Industry Data Exchange (CIDX). Under Chemical Sector Cyber Security Program, all documents are consolidated under ChemITC.

This document defines the elements of a cyber security management system (CSMS) that address manufacturing control systems, information technology systems and the chemical sector value chain. The document is designed to provide general information and guidance to assist companies conducting business within the chemical sector supply chain in implementing cyber security management system practices and controls.

There were other guideline documents released by CIDX prior to this document.



CONCLUSION

Numerous SCADA/DCS security initiatives have been undertaken to address the vulnerable nature of these systems. Obviously, in USA, valuable contributions have been made by all of the stakeholders in improving SCADA/DCS systems security for their country including the government, National Labs, system owners, vendors, consultants, academic institutions, independent associations and bodies. The contributions are widely established from the moment the Presidential Decision Directive 63 (PDD63) was essentially released for Critical Infrastructure Protection in 1998. This was followed by comprehensive DHS's NSSC document in 2003 and the NIPP document in 2006.

USA has become the dominant player in protecting the SCADA/DCS systems. They have developed programs in developing the assessment lab, research, training and education and conferences in promoting the security of these critical systems. They have well-consolidated the international standards, such as ISA99 and ISO/IEC 17799 and other guidelines in NIST and UK Guidelines to their respective "Cyber Security Guidelines" of the critical sectors such as electricity, oil & gas, and chemical.

As for Malaysia, the strategic initiative was developed under the National Cyber Security Policy (NCSP) project of Ministry of Science, Technology and Innovation (MOSTI) in the year of 2006. Under the NCSP implementation plan, protection for the critical systems such as SCADA/DCS systems will be the focus area that CyberSecurity Malaysia has planned. The work has begun and the momentum must be continued towards successful implementation of this plan. CyberSecurity Malaysia is moving forward to develop the SCADA/DCS Security Program within its capability.

REFERENCES

"National Strategy to Secure Cyberspace", by Department of Homeland Security, February 2003,
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

"National Infrastructure Protection Plan (NIPP)", by Department of Homeland Security (DHS),
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

The Center for SCADA Security, Sandia National Laboratory,
http://www.sandia.gov/scada/home.htm

Institute for Information Infrastructure Protection (I3P) : Process Control Systems Project,
http://www.thei3p.org/projects/pcs.html

The Instrumentation, System and Automation society, ISA99 - Manufacturing and Control Systems Security,
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

NIST SP800-82 – Guide to Industrial Control Systems (ICS) Security, 2nd public draft edition,
http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf

Industrial Control Systems (ICS) Security project,
http://csrc.nist.gov/sec-cert/ics/index.html

North American Electric Reliability Council (NERC) - Cyber Security Standards, (CIP 002-009),
http://www.nerc.com/cip.html

American Petroleum Industry - Security Guidelines,
http://new.api.org/policy/otherissues/index.cfm

Chemical Sector Cyber Security Program,
http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm

A Summary of Control System Security Standards Activities in the Energy Sector, by Sandia National Laboratories, Pacific Northwest National Laboratory, Argonne National Laboratory, and Idaho National Laboratory, October 2005,
http://www.oe.energy.gov/DocumentsandMedia/Control_System_Security_Standards_Activities.pdf

MENACING THREATS IN CY

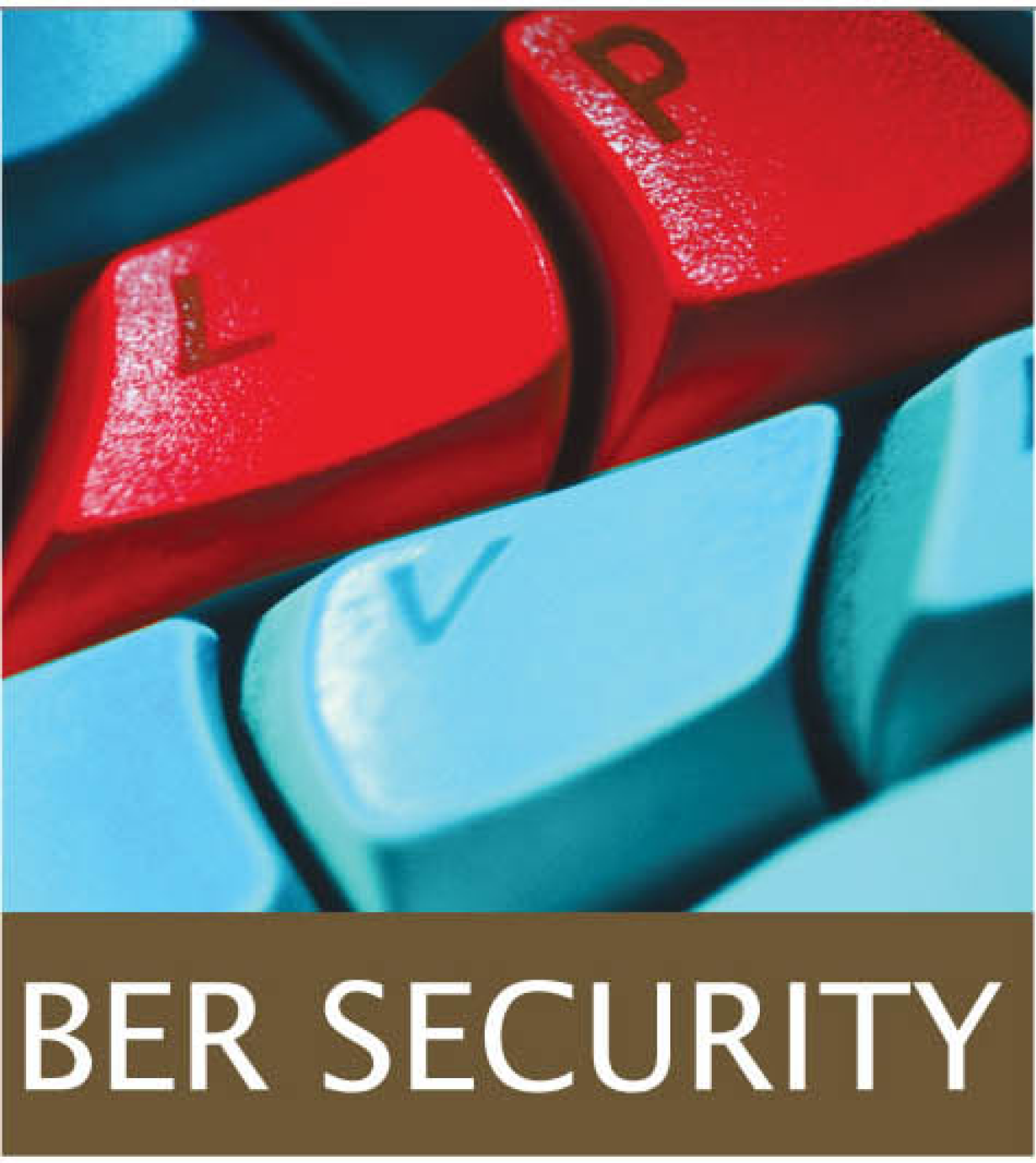
Certainly, It is not an over statement if we were to say that the internet or going online has become part of our daily lives. In the past people basically used the internet for sending e-mails, but now, going online means a whole lot of things. It is where people interact, pay their bills, read the news and even do shopping. Given that people are so dependant on the internet, it is important for internet users to be aware of a number of threats that can happen online. Some of the popular threats today are Denial of Services (DOS), phishing, intrusion and hack threat, virus or worm dissemination, and spams.

The very first well known internet threat occurred in 1988, coined as the Morris Worm. It caused 10 percent of the internet systems to a halt. In order to avoid such incidents from recurring, the United States Defense Advanced Research Projects Agency (DARPA) instructed the Software Engineering Institute (SEI) to set up a centre to coordinate communication among experts during cyber security emergencies and help to prevent these malicious activities. Global monetary and other losses due to this cyber threats were unbelievable, for instance, the Code Red virus saw to a lost of more than USD$2.6 billion. Nimda, on the other hand, paralyzed many organizations within an hour between 8.30 am to 9.30 am of its first public report on the 18th of September 2001. At the end of the day, more than 100,000 computers were affected and tampered with.

In 1990s, threats such as phishing were already starting to take shape. Phishing is an activity whereby attackers or phishers act as trustworthy agents, attempting to acquire private and confidential information i.e. involving passwords or financial details and exploiting such information for unlawful activities. These unlawful activities could certainly lead to financial losses and furthermore could also be used as a spamming tool. In spamming, attackers or spammers will send unsolicited bulk messages to e-mails or in various other forms of messaging which will then affect and slows the capacity in messaging. Threats do not just stop here; today we are further exposed to intrusion and hack threats. Intrusion or hack threat is when someone successfully exploits a system by illegal access through skills, tactics and detailed knowledge. The threats are indicative when your root has been compromised, website defacements, and installation of malicious programs such as Trojan and Bots are present.

The worst case of hacking occurred in 2006, involving Citibank. The Citibank hack forced the bank to reissue debit cards and even block PIN-based transactions. This incident not only affected Citibank but also affected many US national banks. These threats made financial institutions to realise that debit cards, Automated Teller Machines, and Personal Identification Numbers were not secured and were vulnerable to attacks. Today, the information security experts agree that getting hacked seems inevitable.

The threats and intrusions further continued, in 2007. Estonia, a country situated in Eastern Europe, was hacked and infected with the Denial of Service or (DOS). Since nearly 100% of Estonia's operations are dependant on the internet, it was oblivious to them that their critical infrastructures were unquestionably vulnerable to the threats. The Denial of Service (DOS) commands other computers to attack a certain website by requesting for



data, subsequently paralysing the website. As such, most of the Estonians were denied entry to certain websites and infected computers with malicious software i.e. Botnets to launch an attack.

In Malaysia, the total security incidents reported to CyberSecurity Malaysia saw a significant rise from the year 1997 to 2007. In 1997, a total number of 115 cases were reported however the figure rose to an approximate 30,038 cases in September 2007. Normally, hacking doesn't involve a big expenditure, but the financial gain obtained can be huge. The effects of these cyber threats can be unbearable and every person should be aware of its impact either personally or commercially.

If you feel that you have been a victim of a cyber threat or threats, who do you turn to?

In Malaysia, such threats are managed by Cyber Security Malaysia (http://www.cybersecurity.org.my). Established in 1998, the organization comes under the aegis of The Ministry of Science and Technology. Prior to this, the Malaysian Computer Emergency Response Team or MyCERT was responsible to eliminate such malicious activities.

Today, CyberSecurity Malaysia provides incident response services; publish alerts, and offer other related services to improve computer and network security for the nation.

Due to the nature of the internet, cyber threat is a global issue, and cannot be dealt solely by a single organisation. Furthermore by realising the borderless nature of the attacks, the information security workforce is expanding rapidly around the world. Governments worldwide are beginning to form a team and actively participate in joint action to control these problems.

CyberSecurity Malaysia is collaborating with other Computer Emergency Response Team or CERTs around the world such as Forum of Incident Response Security Team popular known as FIRST and Asia Pacific Computer Emergency Response Team (APCERT).

FIRST consists of CERTs from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. FIRST is based in Carnegie Mellon University, USA and currently has more than 170 members worldwide. CyberSecurity Malaysia is an active member of FIRST since 2003. APCERT on the other hand was established in 2002 to address the cyber security issues in the Asia Pacific region. Currently it has 20 teams from 14 Economies in the Asia Pacific region with an operational focus. At the moment, CyberSecurity Malaysia is holding the Chairmanship of APCERT until 2009.

With Computer attackers constantly looking for new targets, cyber threats is ever evolving rapidly. As such, Internet users are prone to cyber attacks. Therefore, it is imperative that the general public should not only have the knowledge on cyber threats, but also must be alert concerning recent development of new threats in the cyber world. Therefore, CyberSecurity Malaysia is continuously striving to serve the community in order to face new challenges of this borderless world.

REFERENCES

http://ftp.fas.org/irp/congress/1996_hr/s960605m.htm

http://world.std.com/~franl/worm.html

Don't be hooked by phishers, JO TIMBUONG, Sunday Star – Focus (pg.27) 26 November 2006.

http://www.infoworld.com/article/07/05/17/estonia-denial-of-service-attack_1.html

http://www.infoworld.com/article/07/02/23/09OPsecadvise_1.html

http://www.itnews.com.au/News/NewsStory.aspx?story=30785

http://www.news.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html

http://www.viruslist.com/en/index.html

Winning the War Against Spyware – We All Have A Part to Play, – Victor Lo is principal Consultant Technology at Trend Micro Malaysia, PC PRO November 2006.

http://www.cybersecurity.org.my/en/about_us/brief_detail/main/detail/729/index.html

Threat Chaos Predictions for 2008

While online theft is nothing new, cyber-criminals are figuring out ways to generate massive, multi-million dollar payoffs through sophisticated Internet exploits. With financial gain on the table, attack methods are improving and the number of people involved is escalating. Now more than ever, organizations need extreme preventive measures in place to protect themselves from the next wave of increasingly covert and targeted attacks.

From my observation, 2008 could very well be the year that attackers launch smarter attacks on social networking sites (e.g. Alicia Keys' MySpace page), On-Demand software applications, E-Commerce and SMB's in a fashion that could double their cyber crime revenue – moving their market to between USD 5 billion and USD 10 billion.

That said, here are my top ten threat predictions for 2008:

Facebook widgets will be used to distribute malware. Facebook, the hugely popular social networking site with over X million users, has recently introduced the ability for users to create and publish small applications and widgets. These applications could cater to just about anything. I have seen one that asks you to compare your friends in a "hot or not" like manner. Another, a simple game, is a blatant rip-off of Scrabble. Facebook hosts these applications and makes it possible for users to share and interact with them. In 2008, we will see attempts to exploit Facebook through these widgets. It could happen through vulnerability in an existing application that could for instance allow the download of a malicious Trojan. Or, it could be a new application deployed to steal information or infect visitors' computers.

Google's latest OpenSocial is an attempt to break the strangle hold that MySpace, Facebook, and LinkedIn are attempting to establish with their user base. OpenSocial is a set of tools that allow developers to create social network applications that can cross the boundaries of proprietary systems. Imagine a mash-up between your LinkedIn network and your Salesforce.com database. While OpenSocial promises great rewards in increased networking functionality, it also opens up risks for exploitation. In 2008, we will see the first attempts to exploit OpenSocial tools to hack social networks.

Salesforce.com AppStore will be involved in a data loss incident. In 2007, we saw the first targeting Salesforce.com (SFDC) through phishing attacks. Once a user's credentials are stolen, the information can be used to gain access to their database of contacts, who are then subsequently spammed. Imagine the power of a SFDC application that is maliciously used to steal information from those who use it. I predict that 2008 will be the year that SFDC applications will be exploited for nefarious purposes.

China will continue to have its way with other nations' critical information. In 2007, we learned that attacks emanating from the Chinese military had penetrated the German Chancellery, England's Whitehall and the Pentagon. 2008 will see a continuance of China's attacks on Western governments and the industry. More penetrations of government agencies will be uncovered and publicized.

Ex-Soviet states will continue to snipe at each other using the weapons of cyber-extortionists: Distributed Denial of Service Attacks, the tactical nukes of the digital era. In May of 2007, a political dispute over a war memorial in Estonia escalated to a full fledged cyber attack against Estonia encouraged by the Putin regime. I believe that Russia will continue to use their newfound ability to use cyber extortionists' tools to impose their political will on break away states.

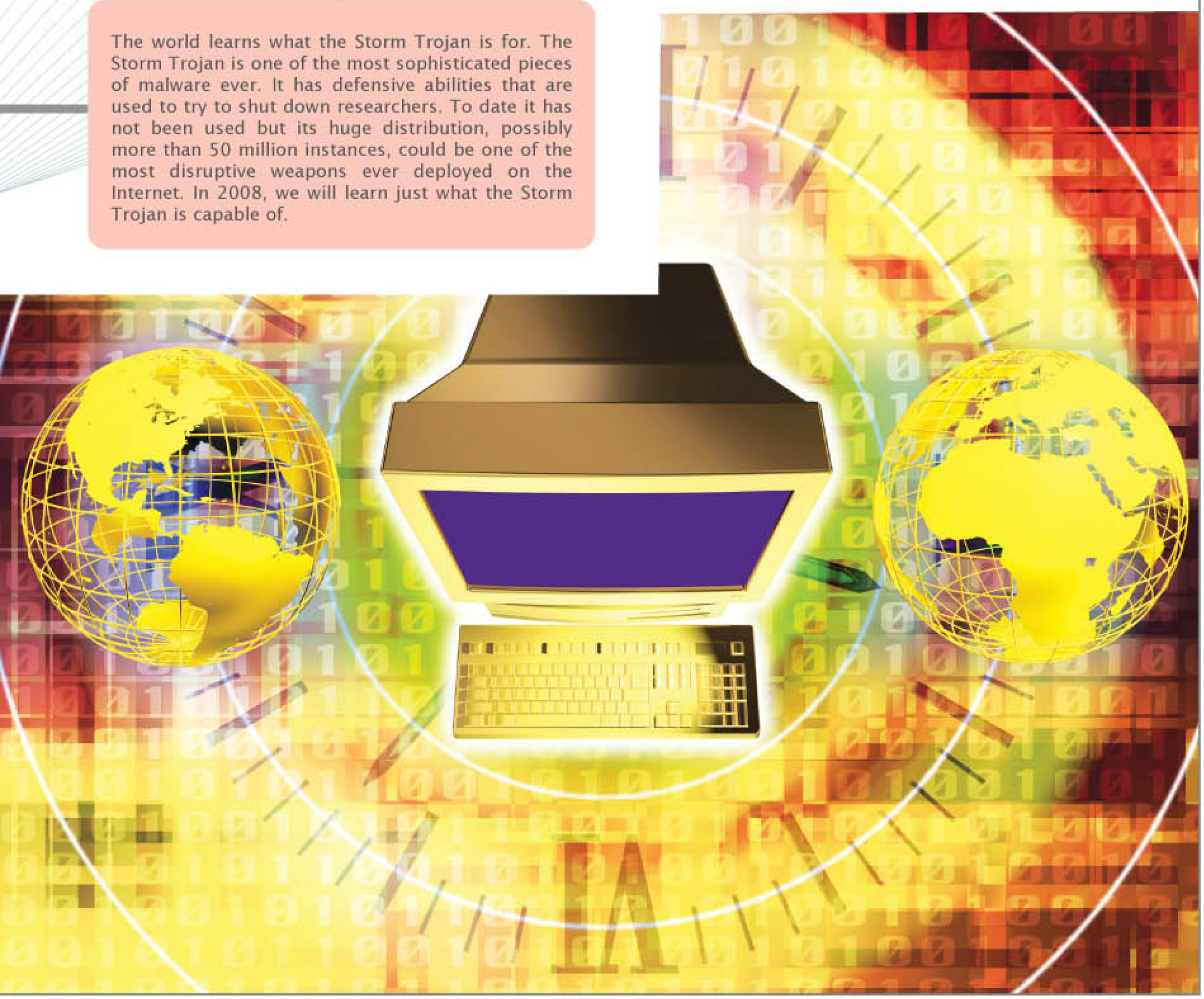
Cyber crime will get up-close and personal. Targeting will become the most profitable means of attack for the cyber criminal. In 2007 Igor Klopov, a 24 year-old Russian, used the Forbes list of wealthiest Americans to choose a target billionaire in Texas. More companies and individuals will find themselves the targets of hackers in 2008.

Terrorist organizations bring out DDoS as a weapon against e-commerce and media sites that choose to display images of Mohamed. This first occurred in December 2006 but the site involved chose not to publicize the incident then. Imagine what would happen if a site started selling plush toys bearing the names of various prophets? Watch out for it in 2008.

Financial markets will be disrupted by increasingly elaborate schemes. For instance, pump and dump combined with DDoS. One scenario that could play out: Hackers use phishing attacks to gain access to online brokerage accounts. They liquidate the victim's stock portfolio and buy short positions in some other stock. They then execute a massive denial of service attack against the company behind that stock and redeem their positions when the stock tumbles.

Game console exploits will be transmitted over the Internet, especially through Wii where vulnerabilities in the system will spread malware. The game console industry is tremendously competitive. One of their biggest opportunities is in networking games between consoles. Network access means exposure to network attacks. That, coupled with the wide ownership of game consoles by hackers, and you have an easy prediction for 2008.

The world learns what the Storm Trojan is for. The Storm Trojan is one of the most sophisticated pieces of malware ever. It has defensive abilities that are used to try to shut down researchers. To date it has not been used but its huge distribution, possibly more than 50 million instances, could be one of the most disruptive weapons ever deployed on the Internet. In 2008, we will learn just what the Storm Trojan is capable of.



Preventing LEAKS of Confidential Information in Email

Introduction

These days, email is used frequently by just about everyone, from the President & CEO to executives and clerks. It is considered that the cheapest and fastest method to send information is through email. We depend a lot on computers and emails to connect to others, from official matter i.e. sending resumes to daily activities pleasure i.e. bertanya khabar and sending birthday cards to the loved ones. As email has become one of the most important communication channels in today's corporation, the email systems have become the main repository for sensitive, confidential and private information.

Unfortunately, a lot of employees out there do not use it prudently, not thinking about security risks, using up excessive bandwidth and practicing lousy etiquettes.The widespread use of email has raised serious privacy concerns to most corporations. One of the critical issues they need to face is how to prevent email information leaks, i.e., when an email message is accidentally sent to the wrong recipients. This is an increasingly common problem that can severely harm corporations as well as the employee himself. As an example, a single email with leaked information can potentially cause expensive and messy law suits, reputation damage, negotiation setbacks and severe financial losses to the company.

Research conducted by IT security and control firm Sophos has revealed that 70 percent of businesses are concerned about sensitive and confidential document falling into the wrong hands as a result of data leakage via email. A further 50 percent of employees admit to having accidentally sent an embarrassing or sensitive email to the wrong person from the workplace, demonstrating that email leakage is a very real concern. Sophos experts note that it can potentially cause corporate embarrassment, compliance breaches and the loss of business critical information.

The good news is that you can prevent information leaks in email easily. How? Best practices need to be implemented to protect valuable corporate information from leaking outside your organization via email. Here are some basic email usage guidelines to help you in handling your email responsibly and to safeguard your organization.

Best Practice #1:

Do not send confidential information via email

Choose only to email non-sensitive information. Do not make the mistake of thinking your emails are secure and private. They are not. Think of them as postcards. You should never include any information in an email that you would not want to be published on the front page of your local newspaper. In other words, never send confidential, proprietary, sensitive, personal, or classified information through email.

Best Practice #2:

Encrypt sensitive information and/or attachment in email

If you still need to send confidential information via email, the best thing for you to do is to encrypt the email and/or attachment. Email messages are usually sent through a vast system of routers and servers. The only sure way to secure private information via email is to use encryption. Encryption is a very simple process and can be done within just 30 seconds. There are many available encryption tools that you can choose from and use everyday.

Best Practice #3:

Think twice before you click on the "send" button

Be extra careful when sending sensitive or confidential information. Never forward proprietary information to external audiences or to unauthorised recipients. Before clicking the "send" button, give it a final once-over. Reread the entire email, review whether a message's contents are appropriate for each listed recipient.

Best Practice #4:

Make sure that you have correct receiver's email address before you send

Ensure that you verify the recipient's correct email address listed in the To and Cc fields before sending the email. It is important that the correct recipients are receiving

messages from you and that you are not revealing the information to unknown people unnecessarily. You can contact the recipient to get his or her correct email address. Save or bookmark the recipient's email address so that you do not have to type the email address and make a mistake during the process of typing it in the To or Cc field.

In addition, practice to keep your friends and colleagues' email addresses private. Here are a couple of simple ways. First, use the Blind Carbon Copy (BCC) feature when you need to hide their email addresses from external audiences. Second, delete their addresses from messages you forward. It takes only a few moments that will reduce the chances of your friends and colleagues receiving junk emails from the unknown

Best Practice #5:

Delete spam email

Spam is loosely defined as unsolicited bulk emails and loosely correlates to the junk mails that turn up in your home mailbox. But spam represents more than unwanted clutter. It clogs email accounts, corporate networks and servers while trying to sell products, spread jokes or propagate internet hoaxes. If you accidentally open spam emails, do not click links offering to unsubscribe or remove you from the mailing list unless the sender is a trusted or reputable vendor. Reduce the amount of spam you receive by being cautious where you publish your email address. Avoid publishing your email address on websites or submitting it to every site or organization that requests it. Subscribe only to websites and newsletters you really need and consider creating a generic Hotmail or Yahoo email account for these subscriptions.

Best Practice #6:

Do not leave a copy of confidential information in email system, save them in your hard disk

Every time you receive sensitive email, immediately save them in your hard disk and delete the email from your email. This can prevent attackers who try to access confidential email in the email system. Furthermore, it is advisable for you to delete all unnecessary electronic mails from the email server(s).

Best Practice #7:

Use antivirus software to prevent virus outbreaks in your organization

You can greatly reduce the spread of email viruses by using antivirus software. Scan every email you received using antivirus software because email is an easy target for virus outbreak. Only open attachment from trusted sender, and scan attachments before opening them. Do not forget to update your antivirus software regularly; if possible enable it to run automatically and connect to the Internet whenever there is new update from the vendor.

In addition, it is advisable that you use only email services that offer automatic antivirus protection. Most free web based email today comes with antivirus programsuch as AOL, Google, Hotmail, and Yahoo.

Best Practice #8:

Change your email passwords regularly to deter potential intruders

You must change your password frequently. The recommended frequency is every 3 months. If you suspect that your password is known or stolen by unauthorized person, immediately report to your email system administrator or provider, and promptly change your password. You must never reveal your password to your friends or acquaintances. The best practice is for you to memorize it without having to write it down or store it in your PC. You can create and memorize a password which is a combination of an English word and your own native word (i.e. Malay, Chinese or Tamil). Examples are 'ulatbook' or 'kerusirock'.

Conclusion

There is no denying in the importance of email as means of communication. Therefore, it is equally important to implement best practice in protecting critical and private information in your email from leaking to outsiders thus causing harm to you, to your company's reputation as well as financial losses. These best practices range from simply double-checking the receiver's email address before sending email to using antivirus software to prevent virus outbreak. Having these best practices can greatly help to ease our minds while we communicate with our friends and colleagues via email.

References

http://www.sophos.com/pressoffice/news/articles/2007/11/data-leakage-poll.html

http://www.cs.cmu.edu/~vitor/papers/sdm07.pdf

http://ise.gmu.edu/techrep/2006/06_05.pdf

http://www.sfisaca.org/events/conference07/Presentations/ S12_WhitePaper.pdf

Roaming Users:

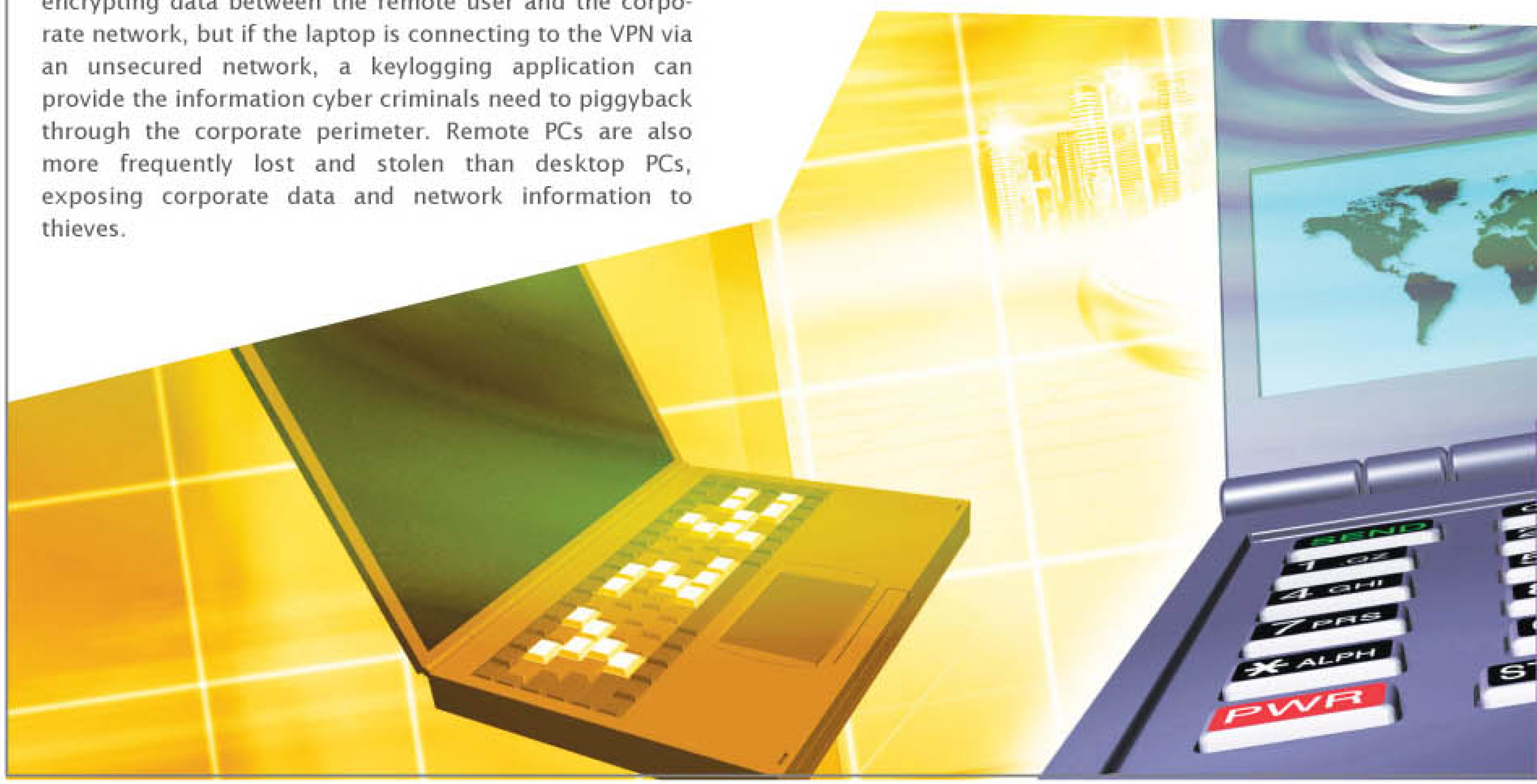
In the past, most remote workers were sales or service techs requiring access to email, CRM systems, and a small number of field service applications. Over the last decade, dropping laptop prices, vastly-improved handheld and smartphone capabilities, and the rise of telecommuting has made nearly every employee a potential remote worker. Expanded connectivity options have made the workplace far more efficient, but they also expose enterprises to additional risks.

Loss of Control

The greatest challenge remote users pose to IT is their inherently uncontrolled environment. Inside an office, IT can control hardware, software and network configurations with any necessary granularity. Remote users connect through public or personal networks of unknown security, load media from unknown sources, perform unrestricted personal browsing in off-hours on corporate hardware, and may not update local virus definitions for extended periods. Each of these factors increases risk of infection, which can then spread to the rest of the network once the user reconnects. Virtual Private Networks (VPNs) address some security issues by encrypting data between the remote user and the corporate network, but if the laptop is connecting to the VPN via an unsecured network, a keylogging application can provide the information cyber criminals need to piggyback through the corporate perimeter. Remote PCs are also more frequently lost and stolen than desktop PCs, exposing corporate data and network information to thieves.

New Technologies

Handheld devices are no longer just organizers—they are fully functioning mobile PCs. PDAs and smartphones provide full, laptop-like functionality, and IT should consider them equally dangerous. Any device with a Web browser and the ability to sync with network resources is a potential malware injection point, and the ability of newer handhelds such as the iPhone to automatically recognize local WiFi networks for personal introduces new risks even within company walls.



Safety On-The-Go

Wireless solutions

As with desktop PCs, an anti-malware solution is a critical component of a remote user protection plan. Enterprises should be sure to install anti- malware software on hand-held devices, as well as laptops. IT departments should also consider using Network Access Control (NAC) to evaluate the state of each remote PC before allowing it to connect to the network. If a PC does not have the most recent virus definitions, patches, or other updates, NAC-compliant products can redirect the computer to an isolated subnet where it can download any necessary updates.

To combat keyloggers, IT departments should look for software that encrypts transmissions from the keyboard to the OS. If the hardware vendor does not provide bundled hard drive encryption software, businesses should also purchase third-party software to secure their data from physical theft. Generally, enterprises should leverage OEM management tools wherever possible, particularly in the case of handhelds, which often provide tools to remotely administer, lock down, and erase lost or damaged devices.

CyberSecurity MALAYSIA

An agency under:

MOSTI

WORLD CYBER SECURITY SUMMIT 2008

21 – 22 MAY 2008 | JW MARRIOT, KUALA LUMPUR

In conjunction with WCIT 2008

WCIT 2008 MALAYSIA MAY 18 - 22, 2008

MSC MALAYSIA Spearheading Transformation

12 Sessions, 4 Security tracks over 2 days!

About WCSS 2008

The World Cyber Security Summit 2008 (WCSS) is held in conjunction with the 16th World Congress on Information Technology (WCIT) 2008.The World Cyber Security Summit 2008 (WCSS) aim is to address issues that are challenging the sustainability of critical information infrastructure and related organisations. The World CyberSecurity Summit 2008 will bring together case studies, best approaches and strategic views from technology implementers, law enforcement agencies and security experts in dealing with various threats that are challenging critical sector organisations in their implementation of a secured environment.

- **Are You Responsible For Securing Information For Your Company Or Your Clients?**
- **Join us at the World Cyber Security Summit 2008 to gain insight and best practices to secure your organisation from the experts.**

Programme Highlights

There will be four security tracks over the two days. Each track will comprise of two presentations and a panel discussion:

1. Anti-Phishing
- Challenges to Pay Pal Payment system, Karim Noorali, PayPal
- APWG, Collaborating To Deliver Forensic Tools & Resources for ECrime Fighters, Foy Shiver, Anti-Phishing Working Group (APWG)
- Panel discussion on "Anti-Phishing Initiatives - Good Governance"

2. Emerging Technology, Security Threats, Law and Enforcement
- ASCLD/LAB Accreditation, John Barbara, State Law Enforcement, United States
- Presenting E-Evidence in Court, Raemarie J. Schmidt, Digital Intelligence, United States
- Panel discussion on "Cyber crime in the face of Law and Enforcement"

3. Online Identity and Internet/Mobile Banking
- Challenges in Online transaction: Determining who is on the keyboard, VISA International
- Internet and Mobile banking security issues, World Bank
- Panel discussion on "The future of Online Identity"

4. Critical National Information Infrastructure Protection
- SCADA Security Threats: A Global Issue?, Jonathen Pollet, Industrial Defender
- SCADA/DCS Security Protection Framework Requirements – Keith Stouffer, National Institute of Standards & Technology (NIST), United States
- Panel Discussion on "Securing work environment within CNII organisations"

CISSP & SSCP earn 16 CPE Points

Contact information and enquiries

CyberSecurity Malaysia (formerly known as NISER),
Level 7, SAPURA @ MINES, 7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan,
Malaysia.

Phone : +603-8992 6888
Fax : +603-8945 3405
Email : training@cybersecurity.org.my