Jurnal Teknologi Maklumat & Multimedia **4**(2007): 53-72

User Awareness in Handling Computer Viruses Incident for Windows Platform

MADIHAH MOHD SAUDI

ABSTRAK

Kertas ini mengfokuskan dan mengkompilasi tanda dan simptom oleh jangkitan virus komputer, pemulihan dan pencegahan daripada virus komputer di Windows platform termasuk Windows ME, Windows 95, Windows 98,Windows NT dan Windows XP. Kertas ini turut membincangkan tentang salah anggap terhadap virus. Di samping itu, penyelidik juga menganalisis tahap pengetahuan pengguna dalam pengendalian virus komputer. Daripada 600 soal selidik yang diagihkan melalui dalam talian dan salinan keras, sejumlah 450 orang responden adalah mereka yang melibatkan komputer di dalam kerja harian mereka. Disebabkan oleh masa dan kekangan belanjawan, responden pensampelan adalah hanya dari Putrajaya, Selangor dan Kuala Lumpur. Pensampelan adalah terpilih berdasarkan jumlah pelanggan menggunakan Internet, lokasi tempat yang terletak di dalam kawasan bandar dan sebagai pentadbiran kerajaan persekutuan dan pusat perniagaan di Malaysia.

Katakunci: virus, tetingkap, pengetahuan pengguna, tanda dan simptom.

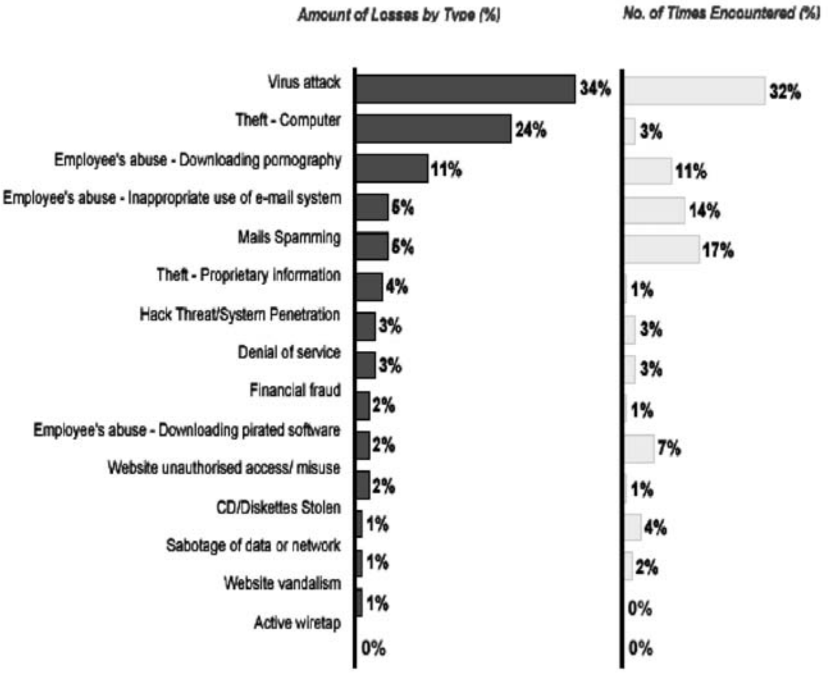
ABSTRACT

This paper focuses and compiles signs and symptoms of computer virus infections, recovering and defending from computer viruses on Windows platform including Windows ME, Windows 95, Windows 98, Windows NT and Windows XP. This paper also discusses on the mythical myth of viruses. Besides that, the researcher had analyzed the level of knowledge on user in handling computer virus. Out of 600 questionnaires distributed through online and hard copy, a total of 450 respondents who were involve with computer in their daily work had taken part in answering the questionnaires. Due to time and budget constraint, the sampling respondents are from Putrajaya, Selangor and Kuala Lumpur only. The sampling was chosen based on total subscriber on the Internet, location of the place in urban area and as the federal government administrative and business centre in Malaysia.

Keywords: virus. windows, user awareness, signs and symptom.

Malicious code is a term used to describe all sorts of destructive programs which are viruses, worms, Trojan Horse, pests and rogue Internet content (Indefense 2004). Virus is more prevalent today than ever before, and both home users and system administrators need to be on the alert to protect their network or company against attacks. It is coming out so fast these days that even the most accurate scanners cannot track all of the new ones.

By referring to MyCERT's Abuse Statistics from 1997 until October 2004, rapid increase of computer crime cases in Malaysia especially in virus cases (MyCERT 2005). For virus cases, from seven cases in 1997, it has increased to 379 cases in 2001 and until September 2004 it has touched 210 cases. From NISER ICT Security survey for Malaysia 2001/2002 (NISER 2002), based on the result shown in Figure 1, virus attacks was the most frequent security breach experienced in year 2001/2002 with a record of 1,280 times.



Base: Organisations that have experience/ unsure if experienced ICTsecurity breach in 2002

FIGURE 1. NISER ICT Security Survey for Malaysia 2001/2002
Source National ICT Security and Emergency Response
Centre (2002), page 23, Figure 23

From NISER'S ISMS Survey (NISER 2004) which is carried out in 2003 for Malaysia, virus attack is the most common types of security breaches experienced which is shown in Figure 2. A breach in information security can impact many business processes within an organisation and that impact becomes more difficult to assess. It is not simply a case of how much it costs to rectify the breach but of a range of other issues such as; delayed delivery of contracts, lost opportunities, legal and contractual liabilities incurred, loss of customer confidence and loss of trust. Furthermore, organisations do not like to publicise that they have suffered a security breach because of the adverse publicity that it brings and the damages it is likely to inflict on the company's reputation.

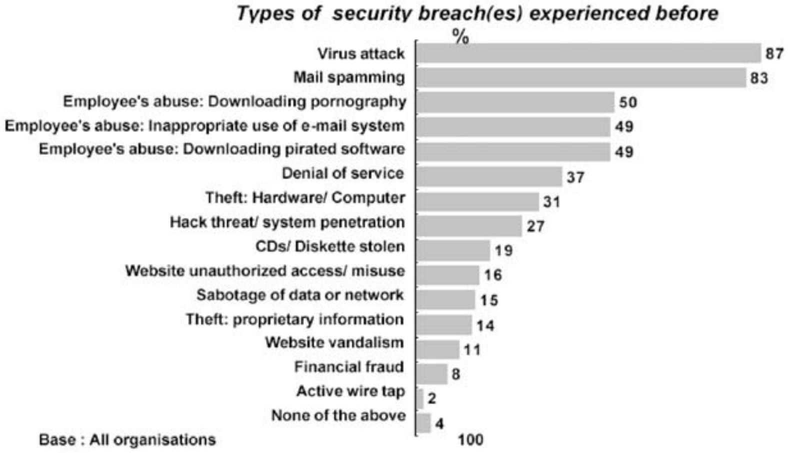


FIGURE 2. NISER ISMS Survey 2003 *Source* National ICT Security and Emergency Response Centre (2004), page 18

In terms of financial losses, virus attacks thus become one of the major contributors. It is estimated the total loss of money due to Code Red, Nimda, Nachi and Blaster worm outbreaks from 2001 to 2003 in Malaysia is RM 104 million (Indefense 2004). From CSI/FBI Computer Crime and Security Survey (Gordon et al. 2004) which is carried out at the United States, the virus category emerged for the first time as the incident type generating the largest total losses. In a survey which was carried out in year 2004, 269 respondents out of a total of 494 provided dollar loss estimates. In Figure 3, it is estimated the total loss of money due to virus outbreaks is $55,053,900. To the extent that this result can be generalised to the whole population, it may be due to last four year's rise(2003) in the degree to which virus threats were entwined with denial of service attacks (witness the numerous variants of the MyDoom worm, which carried as its payload a time-triggered denial of service attack program).

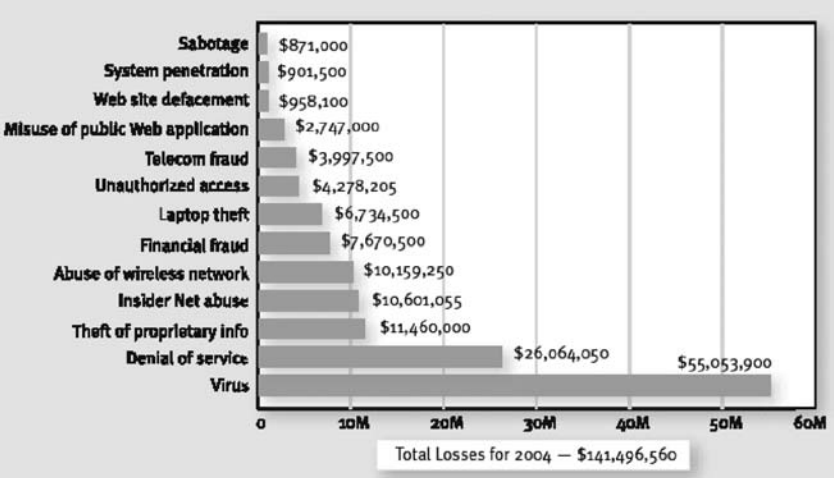


FIGURE 3. CSI/FBI Computer Crime and Security Survey,
Computer Security Institute (2004)
(*Source from:* Gordon *et al* (2004), page 10, Figure 15)

A questionnaire that was carried out for this project identified factors that contributed to fast growth of computer virus cases. Details of the result analysis are explained in section 3.

COMPUTER VIRUS DEFINITION

The Internet is constantly being flooded with information about computer virus, worm,Trojan Horse, adware and spyware. These terms have been used interchangeably, but most of the time the public do not know that they have different meanings and functions. Thus, it is critical that we understand these malicious codes or what we call computer virus, worm, Trojan Horse, adware and spyware. Malicious code can be referred as any software program that moves from one computer to another or network to network and can modify computer system without the consent of the owner or operator. There are many ways in which malicious codes spread. The common mediums are through email attachments, scripts in web pages and networks and file sharing. In this paper, we will specifically focus on virus.

Virus is defined as a program, which when executed, can add itself to other programs, without permission or right. This is done in such a way that the infected program, when executed, can add itself to other programs as well. The virus inserts itself into the chain of command and executes a legitimate program that results in the execution of the virus as well as the program. If we relate to our daily life, computer virus programming logic mimics human virus biological counterparts. First, it invades the host victims by changing the underlying structure. Once infected, host files become viruses themselves and begin to infect other files. Later, computer viruses mutate and evolve to fight antivirus ‘antibiotic’ programs, and massive infection results in the larger system malfunctioning.

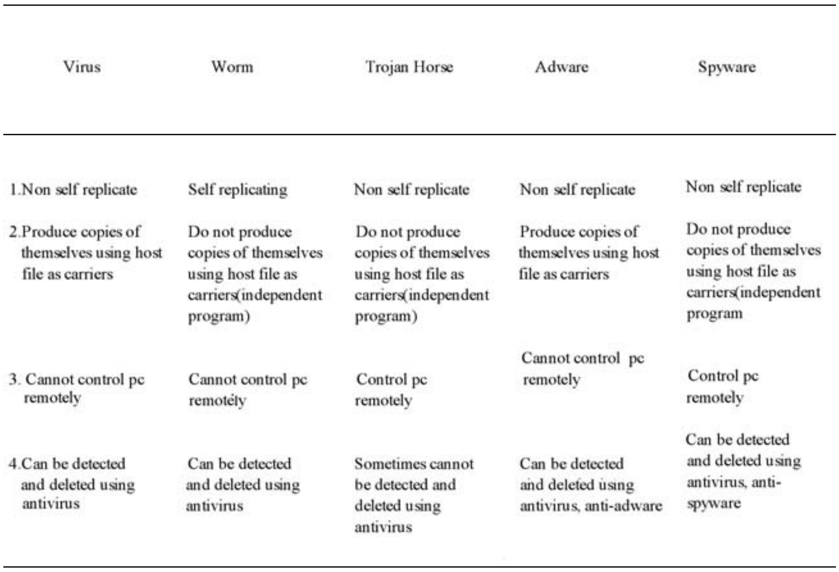
Different with worm where it is defined as a program that replicates itself from system to system without the use of a host file. As for Trojan Horse it is referred as to impostors, files that claim to be something desirable but, in fact, are malicious. Viruses are in contrast to worms, which require the spreading of an infected host file. A very important distinction between Trojan Horse programs and viruses is that they do not replicate themselves. Trojan Horse contains malicious code that when triggered can cause loss, or even theft of data. In order for a Trojan Horse to spread, it is a must for the Trojan Horse program to be executed in the victim’s host. As for adware and spyware they can easily be installed on a victim’s pc by downloading free software or by browsing the Internet. Adware usually comes together with free software or demo version of softwares. Generally, most or all features of the free softwares are enabled but users have to look at sponsored advertisements which are known as adware while using the software. ‘It is considered as malicious code because it is installed automatically together with free softwares into the user’s machine without user knowledge. Sometimes when free software is installed from untrusted source, the adware tracks user surfing habits in order to serve ads related to user. When the adware becomes intrusive like this, then it is categorised as spyware and it then becomes something user’s should avoid for privacy and security reasons.

Spyware is considered a malicious program and is similar to a Trojan Horse in that users unintentionally install the spyware when they install another program. Also spyware collects personal information without the user’s permission, monitors user activity on the Internet, gather information about e-mail addresses and even passwords and credit card numbers and transmits that information in the background to someone else.

The differences between virus, worm, Trojan Horse, adware and spyware is summarised as in Figure 1. Therefore, worm and virus are very similar to one another but are technically different in the way they replicate and spread through a system. As for Trojan Horse, its capability to control PC remotely makes it different from virus,worm and adware but similar to spyware.

Signs and Symptoms of Virus Infections

There are many ways to identify if a machine has been infected by a virus or not. Below are the signs and symptoms that can help to determine if a machine is infected with a virus (Microsoft 2004; David 2002).



Virus	Worm	Trojan Horse	Adware	Spyware
1.Non self replicate	Self replicating	Non self replicate	Non self replicate	Non self replicate
2.Produce copies of themselves using host file as carriers	Do not produce copies of themselves using host file as carriers(independent program)	Do not produce copies of themselves using host file as carriers(independent program)	Produce copies of themselves using host file as carriers	Do not produce copies of themselves using host file as carriers(independent program
3. Cannot control pc remotely	Cannot control pc remotely	Control pc remotely	Cannot control pc remotely	Control pc remotely
4.Can be detected and deleted using antivirus	Can be detected and deleted using antivirus	Sometimes cannot be detected and deleted using antivirus	Can be detected and deleted using antivirus, anti-adware	Can be detected and deleted using antivirus, anti-spyware

FIGURE 1. Differences between Virus, Worm, Trojan Horse, Adware and Spyware

- The infected file may make copies of itself. This may use all the free space in your hard disk
- A copy of the infected file may be sent to all the addresses in user e-mail address list
- The virus may reformat disk drive and delete files and programs
- The virus may install hidden programs, such as pirated software
- The virus may reduce security. This could allow intruders to remotely access your computer or network
- Computer always stops responding when try to use Microsoft Office products
- Cannot start Windows Task Manager.
- Antivirus software indicates a virus is present
- User received an e-mail message that has a strange attachment. When the attachment is opened, dialog boxes appear or a sudden degradation in system performance occurs
- There is a double extension on an attachment that recently opened, such as .jpg.vbs or .gif.exe.
- An antivirus program is disabled for no reason and it cannot be restarted
- An antivirus program cannot be installed on the computer or it will not run

- Strange dialog boxes or message boxes appear on screen
- Received complains from friends, colleagues or unknown person about receiving e-mail messages that contains attached file (especially with .exe, .bat, .scr , .vbs extensions) or pornography website URL links which the user himself did not send
- New icons appear on the Desktop that a user did not place there, or are not associated with any recently installed programs
- Strange sounds or music plays from the speakers unexpectedly
- A program disappears from the computer, and it was not intentionally uninstalled
- Recent programs file date changes
- The number of bad sector or cross linked file grows on the disk
- Inappropriate floppy disk accesses
- Sudden decrease in total conventional memory

A virus infection can also cause the following symptoms, but these symptoms can also be the result of ordinary Windows functions, or problems within Windows that is not caused by a virus.

- Windows will not start at all, even though no changes for examples uninstall or remove programs has been made by the user
- Windows will not start because certain critical system files are missing, and then receive an error message that lists those files
- There is a lot of modem activity. If the user uses an external modem, there are the lights blinking extensively when the modem is not being used
- The computer starts as expected sometimes, but at other times it stops responding before the desktop icons and taskbar appear
- The computer runs very slowly and it takes a long time to start
- Out-of-memory error messages appear, even though the computer has plenty of RAM
- New programs do not install properly
- Windows spontaneously restarts unexpectedly
- Programs that used to run now stop responding frequently. If try to remove and reinstall the software, the issue continues to occur
- A disk utility such as Scandisk reports multiple serious disk errors
- A partition completely disappears

All the signs and symptoms listed above can be use as guidelines to determine if a machine has been infected by a virus. It is not mandatory or a must that signs and symptoms will appear to indicate virus existence.

Below are the recommended steps to recover from viruses:
a. Disconnect the infected machine from the network.
b. Disable the system restore for Windows XP and Windows ME.
Windows XP

- Click Start
- Right-click My Computer, and then click Properties
- Click the System Restore tab
- Select "Turn off System Restore" or "Turn off System Restore on all drives"
- Check box

Windows Me:

- Click Start, point to Settings, and then click Control Panel
- Double-click the System icon. The System Properties dialog box appears
- Click the Performance tab, and then click File System. The File System Properties dialog box appears
- Click the Troubleshooting tab, and then check Disable System Restore
- Click OK. Click Yes, when you are prompted to restart Windows

c. Scan computer with an updated antivirus program. Reinstall the antivirus program (if it has stopped working). Get the latest "virus signature file" from antivirus vendor's Web site. If user does not have anti-virus software, it can be downloaded from any anti-virus vendor's website. Anti-virus software can be downloaded at:
http://www.mycert.org.my/anti-virus.htm
d. Install the latest security patches from the following Microsoft Web site:
http://windowsupdate.microsoft.com
e. Disable any file/directory/network sharing if exists
f. Remove the infected file of the viruses

To remove the viruses either using an automatic removal tool or with manual removal.
Generally below are the manual steps taken to remove Windows viruses.

- To remove the viruses, research the virus. Search information about the virus from the trusted website for example, the anti virus website and CERT website.
- Then stop any virus services. If the virus service's name has already been identified, go to Control Panel -> Services -> Startup -> Disable.
- Delete and replace infected files. Anti-virus software will often be able to repair files with minor damage. However, user will have to restore badly damaged or destroyed files and programs from back-up copies and

installation disks. User may also have to replace some files from original system installation disk

- Clean up startup areas. In Windows 98, use the MSCONFIG.EXE to disable any virus startup program. In other platform, have manually edited the necessary files for example, at the WIN.INI, SYSTEM.INI, AUTOEXEC.BAT or CONFIG.SYS
- Replace the infected file at the Registry

To be more specific for certain viruses, below are the steps.
Removing Boot Viruses

Each of different Windows file systems FAT, VFAT, FAT32 and NTFS have their own boot files.

1. *Boot with a clean floppy disk*. Below are the steps to create boot floppy.

Windows 98, Windows 95, Windows ME boot floppy
For system with FAT , VFAT and FAT32:

a. Type 'SYS A:' or 'FORMAT A: /S' at the command line prompt
b. Or can use click at 'My Computer' -> Right click at 'Floppy A:' -> 'Format' and choose 'Copy System files'
c. Or can use by clicking at 'Start' -> 'Settings' -> 'Control Panel' -> 'Add/ Remove Programs' -> 'Startup'

Windows NT boot floppy

a. Format a floppy disk on a Windows NT computer
b. Copy NTLDR, BOOT.INI, NTDETECT.COM and NTBOOTDD.SYS to floppy

2. *If want to remove the boot virus manually, below are the steps.*

Windows 98, Windows 95, Windows ME

a. Use FDISK /MBR to remove a hard disk virus
   Do not use FDISK / MBR if:
   - If the hard disk has more than four logical partitions
   - If the hard disk is dual-booted NT
   - If the hard disk has dual-boot partitions
b. Use SYS.COM to remove a boot sector virus from floppy disk
   Copy a new DOS boot sector using the command SYS.COM from floppy disk to the infected machine with boot virus

Windows NT

a. Put NT installation CD-ROM in the drive and boot up using the installation setup diskettes

b. Select R to repair the NT installation
c. Choose 'Inspect boot sector and restore Startup Environment'
d. Insert the ERD (Emergency Repair Disk)

3. *Removing Macro Viruses*

a. Get a clean application starts with getting a clean global template and clean startup files
b. For both Word and Excel search for infected global template (normal.dot for Word) and delete the infected files
c. Rescan the machine with the anti virus software to ensure it is virus free
d. Enable system restore for Windows XP and Windows ME
e. Reconnect the machine to the network

Defending Against Viruses

There are many ways and opinions regarding defending steps against viruses. One of the ways which is quoted from Fred Cohen, "Three basic things allow viruses to spread: sharing, programming and changes. All we have to do is eliminate those three things and we will be perfectly free of viruses" (Cohen 1990). One of the most effective protections against malicious code is based on defense-in-depth (Cohen 1991a). In this approach, many approaches are combined so that when one technique fails, redundant techniques provide added coverage. Combinations of virus monitors, integrity shells, access controls, virus traps, on-line backups, SnapShots, BootLocks, and ad-hoc techniques are applied to provide barriers against operation, infection, evasion, and damage by known and unknown viruses.

Other research said 'prevention is the better than cure' applies here too as it does everywhere else. Some of the preventive steps include by having the latest anti-virus software, sensible filtering (such as quarantining all executable content from e-mail and Web traffic), firewalls, and religiously maintaining patches (Weaver 2002). Ensure that the PC operating system is properly patched against all announced security issues. The Security Bulletin page at Microsoft will keep users informed of known issues. A good example was the "Code Red" worm that has affected almost 500,000 users. Microsoft had announced the exploit and offered a patch to prevent this worm for over a month prior to the release of "Code Red". Users simply failed to patch their servers.

The most common virus defense is the anti virus scanner, which examines computer files to detect known viruses. Scanners have several important problems that have a serious impact on their current and future viability as a defense, most probably; (Cohen 1990 & 1991b) they only detect viruses known to the author, they produce infinite numbers of false negatives, they may produce false positives as new programs enter the environment, they are ineffective against many types of evolutionary viruses, they are not cost effective relative to other available techniques, and they become less cost effective as time passes. But still enhancement has been made by the anti virus software for example, by integrating the monitor function capabilities. Until today, anti virus is seen as one of the best ways in defending machine from being infected by viruses. Nevertheless, it is a must to up-date the anti-virus signature file or the database file on a regular basis in order to make sure the anti-virus is working accurately. There are many free anti-virus software available out there and can be easily used and downloaded from the Internet.

Another way to prevent virus or worm from spreading through share file, folder or network is to use passwords to log on to the system or network. One of the virus or worm most common payload is to spread through file, folder or network sharing. Once one machine is already infected with this kind of worm, definitely by having a password to access the file, folder or network would help to prevent the worm from spreading itself either through file, folder or network sharing. Passwords consisting of letters and numbers, referred to as alphanumeric passwords, work best for security. Avoid using name, significant others name or birthday date. These are often the first passwords tried by would-be crackers. Change password often and never, ever give password to a co-worker. Be aware of attempts by miscreants to obtain passwords via email. Never, ever give anyone the passwords for any reason. Some miscreants will try to fool users into thinking that they are from user's ISP, such as AOL. They will email users with what appears to be a valid request for information. This is bogus. For example Maybank fraudulent email which request user to reactive their account by entering the id and the password. This technique is also known as phishing scam.

Use a personal firewall anytime whenever online. Dialup connections are being targeted more and more. Personal Firewalls essentially make computer "invisible" to passing scans looking for vulnerable machines. Do not download files or programs from sites users know nothing about. Warez or Kazaa sites are infamous for being a good source of infection. In theory, any program downloaded could contain a virus, Trojan Horse, or spy ware. Of course, this is not practical so it is recommended that users scan downloaded files with at least two different up to date virus scanners and a Trojan scanner. Despite this, it is still possible to become infected with a virus or Trojan, but a lot less likely.

Do not give out actual email address to people users do not know personally. This might lead to receiving email spam or worm infected email from unauthorised party. Avoid using primary email address in news groups as well. Have a web based email at Hotmail, Yahoo or any of the other free sites for these purposes. If users do not have a network, check the configuration and the bindings to ensure that it is set properly to prevent unauthorised access from outside. When in chat rooms, ensure that user IP address is not part of user profile.

The following guidelines besides what have been stated above could be used as the defending and preventive steps from virus outbreaks or infection (McDuffie 1994).

- Backup copies of all programs and data files should be made at regular intervals, such as weekly or monthly
- Public-domain software such as freeware and shareware should be tested for virus presence before use
- Users should routinely test all software for viruses, both retail- purchased and public-domain programs
- Users should always boot a system from the original write-protected disc. In the case of hard disc systems, users should avoid booting from an untested diskette
- Users should enter meaningful volume labels on all hard discs and diskettes, and routinely check volume labels when the DIR command is executed. Inspect the labels for changes
- Users should be wary of unusual system activities such as less available system memory than normal, or turned-on access lights on a system device when there should be no activity

E-mail is also known as one of the medium that is used by the viruses to spread. Below are the recommended steps that should be taken when using the email.

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source. If received email from unknown person, always make sure to scan the attachment with the antivirus first
- Do not open any files attached to an email if the subject line is questionable or unexpected
- Delete chain emails and junk email. Do not forward or reply to any of the email. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network
- Do not download any files from given URL link from strangers which contains in the e-mail
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If uncertain about the files, do not download the files at all or download the file to a floppy and test it with the anti-virus software
- When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments.

Until today there are still many people who click on email attachments from untrusted sources. Who should be blamed? There are few ways users can avoid from being infected by the virus, worm, Trojan Horse or spyware. As already explained earlier, all the recommended steps can be used as guidance.

VIRUSES MYTHS

YOUR ANTI-VIRUS TOOL AND SECURITY TOOLS PROTECT YOU FROM ALL KINDS OF VIRUSES

If you update your anti-virus signature once a month, there is no assurance you will be safe anymore. The release of the viruses variants which takes less then 1 week shows that anti-virus signature need to be updated daily and regularly. Nevertheless, if your anti-virus signature file is not up to date there is a possibility that your computer will be infected with worm that is capable to corrupt your anti-virus functionality and your anti-virus will not be able to cleanup the worm. Not only that, the virus also has the capability to end processes of security related software for example, your personal firewall and block access to several security related web sites. If your computer has been infected with this kind of worm, it is highly recommended for you to reinstall your anti-virus and your security tools.

Another thing users and organisations should be aware of is flaws or bugs released related with anti-virus software or any security tool. Make sure when vendor announce the fix solution or patch for the bug found in the software, user should immediately download and install the patch. Sometimes users claimed that even though they had cleaned up their computer with the anti-virus and other security tools, they still get reinfected by the worm or they were unable to cleanup the worm. So what when wrong? The answer is wrong procedure in cleaning the worm. Following the right standard operating procedure to cleanup the worm is a must. For example, when users do the clean up process for computer with Windows XP as the platform, the 'system restore' must be disabled first before running the security tools. For other operating system platform, users might have to startup the computer in safe mode or stop the worm or other malicious code before running in the computer memory. For different operating system platform, different procedure to cleanup the virus should be followed and considered. User needs to refer to the anti-virus website or CERT website for example MyCERT website for accurate procedure to cleanup the worm.

Another suggestion that might be useful for organisations is to have their own CERT team or operation center that can respond immediately once the worm outbreak happens. There are cases where organisations spent endless hours repeating processes that are non-effective to clean up the worm within the network due to uncoordinated effort within the organisation. MyCERT had released a computer worm incident handling standard operating procedure which can be referred at MyCERT website.

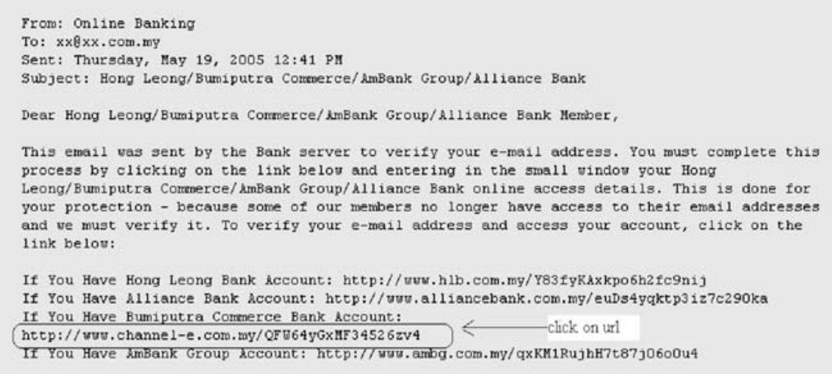
Another thing that users should be aware of is the fake result of anti-virus scan in the infected email. Nowadays it is not rare to find an email with infected attachment contaning email message stating that the file attachment is virus free. Sometimes users might be fooled by this kind of email message. It is highly recommended for users to scan all email attachments before opening them.

VIRUSES CODE CAN ONLY INFECT COMPUTER, MOBILE PHONE AND INSTANT MESSENGER ONLY

It is true that the most targeted device for viruses to infect is computer and mobile phone with Bluetooth, wireless or infrared features and instant messenger. The best way to prevent your computer, mobile phone with above features and instant messenger from being infected with virus is to install the anti-virus or security tools and never accept any suspicious file send to you. There are many reports and stories about viruses and Trojans infecting these hardware, device and software. Currently these malicious codes have already attacked handheld games. First Sony's Playstation Portable (PSP) Trojan was found infecting Nintendo DS handheld gaming console in October 2005. This simple trojan, known as 'Trojan.PSPBrick' deletes essential system files on the PSP and renders it unbootable. This can be prevented by not to modifing handheld games console to run unauthorised software. The best thing users can do is to be more aware about what software they run on their computers, mobile phone and PSP and run security tools with latest signature update or patch.

WRITING VIRUS IS FOR FUN AND FOR RECOGNITION

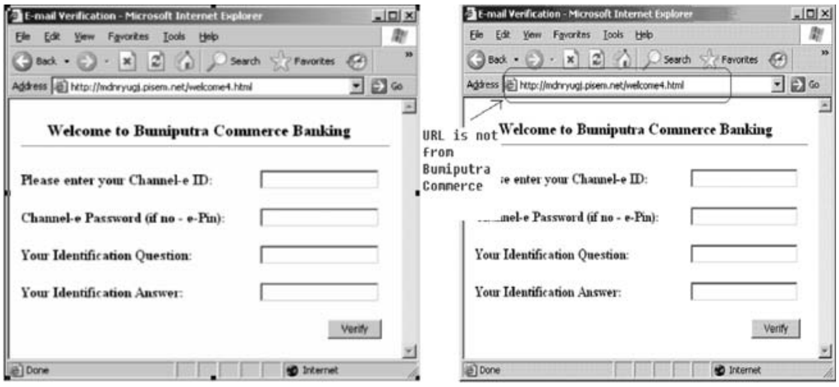
10 years ago or probably 3 years ago, one of the motive of the virus writer can be associated with fun or to gain recognition from certain organisation or groups. Unfortunately, we can see many viruses,worms or Trojans are created to make money. Phishing scam is an example where the intention is to steal username and password for money transaction purposes. In Malaysia, the phishing activities involve local and foreign financial institutions. A serious well-organized phishing attack occurred in May 2005 involving four well-known local internet banking. The phishing email requested users/recipients to login to the links attached in the email for the four targeted banks as displayed in Figure 4.Once the victim clicked on the URL, the victim will be redirected to a malicious website instead of the genuine website as displayed in Figure 5.



```
From: Online Banking
To: xx@xx.com.my
Sent: Thursday, May 19, 2005 12:41 PM
Subject: Hong Leong/Bumiputra Commerce/AmBank Group/Alliance Bank

Dear Hong Leong/Bumiputra Commerce/AmBank Group/Alliance Bank Member,

This email was sent by the Bank server to verify your e-mail address. You must complete this
process by clicking on the link below and entering in the small window your Hong
Leong/Bumiputra Commerce/AmBank Group/Alliance Bank online access details. This is done for
your protection - because some of our members no longer have access to their email addresses
and we must verify it. To verify your e-mail address and access your account, click on the
link below:

If You Have Hong Leong Bank Account: http://www.hlb.com.my/Y83fyKAxkpo6h2fc9nij
If You Have Alliance Bank Account: http://www.alliancebank.com.my/euDs4yqktp3iz7c290ka
If You Have Bumiputra Commerce Bank Account:
http://www.channel-e.com.my/QFW64yGxMF34526zv4
If You Have AmBank Group Account: http://www.ambg.com.my/qxKM1RujhH7t87j06oOu4
```

click on url

FIGURE 4. Example an Email of Phishing Scam



E-mail Verification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://mdnryugj.pisem.net/welcome4.html
Go
Verify
Done
Internet

Welcome to Bumiputra Commerce Banking

Please enter your Channel-e ID:

Channel-e Password (if no - e-Pin):

Your Identification Question:

Your Identification Answer:

URL is not from Bumiputra Commerce

FIGURE 5. Fake Website

If we have a close look at the URL, is the form in Figure 5 is a fake form. This is one of the ways how people steal other people's password. It is highly recommended for users who receive emails from a bank requesting to change their login and password to ignore or delete such emails immediately. Users are also advised to refer and verify any such emails with their ISPs, CERTs or with the Particular Financial institutions. Another way to ensure that the website they visited is not a phishing scam website is by installing anti-phishing tool such as netcraft which can be downloaded free from the internet.

YOUR BROWSER WILL NOT BE INFECTED BY SURFING TO SITES YOU TRUST

It is highly advisable to browse the web site you trust and download tool or software from trusted website. But what happen if the website is DNS poisoned? How can end users especially non technical people identify if the website is DNS poisoning or not? DNS poisoning means injecting false information into the DNS system so that future requests are diverted to another site. In simpler word, URL of the website is still the same but the IP address is different. For example the user type YPERLINK "http://www.xyz.com" www.xyz.com but it is redirected to other website www.abc.com but the URL is still displayed as www.xyz.com. If the DNS of a website has been poisoned, it is very hard for end users to differentiate between the genuine and fake website content. One of the best solutions to overcome the DNS Poisoning is by using the DNSSEC which stands for DNS Security Extensions. It adds security to the Domain Name System and a set of extensions to DNS, which provide an origin authentication of DNS data, data integrity and authenticated denial of existence. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the info on the authoritative DNS server. As another alternative end user can check the IP displayed for the given URL and compared with requested URL or end user can ask directly the owner of the website to verify the content if user feels suspicious with the website content.

Another issue related with the web browser is the patch. It is a must for end users to patch the web browser regularly. Last year there were so many issues related to web browser especially Internet Explorer. At one stage the U.S. government's Computer Emergency Readiness Team (US-CERT) warned Web surfers to stop using Microsoft's Internet Explorer (IE) browser due to so many security flaws that were found in the Internet Explorer. To protect against the flaws, IE users can download the patch from the Microsoft website and install the patch immediately and it is highly advisable to disable Active scripting and Active X controls in the Internet Zone if it is not used by the users.

USER AWARENESS ON COMPUTER VIRUS

Currently, few systems, if any, are capable to educate end user about virus and give proper procedure in handling the computer virus incident. In order to handle computer virus incident properly, one big area that needs deeper research is user awareness and education about computer viruses (David 2002; Jeffrey & Steve 2001) and a system that is capable to guide users how to handle virus incident following the incident response procedure (Madihah and Nazean 2006). In this paper details of the system was explained.

Summarised from the article (Danchov 2004), human factors contributs to the security breach and dissemination of malicious code. Virus is one of the examples of malicious code. In spite of the latest technological improvements, it is human who plays role in interacting and configuring devices or programs and contributing to the dissemination of malicious code.

One of the approaches to overcome this problem is to increase awareness level of the user, which is also as one of the strategies in combating virus.

From the researcher's observation, most of the research are on computer viruses in Malaysia and are more focused using Intrusion Detection System (IDS) techniques in solving virus problems (Alias et al. 2001; Zambri 2003; Sarim 2002; Keong 2003; Ramadass et al. 2003). Nevertheless, there is still few research papers related to user education of computer viruses produced for the past 10 years in Malaysia (Summers and Mohd Hussain 1991a; 1991b; 1991c; Summers et al. 1992; Shukor 2003). As a continuity of this research and the urgency to produce more research related to user education of computer viruses in Malaysia, a research was conducted. (Madihah et al. (2006).

QUESTIONNAIRE

Marko Helenius conducted a questionnaire survey related to computer viruses at Finland (Marko 1994). From his questionnaire survey result, the knowledge of viruses was quite poor in all sectors: government, local authorities and companies. Respondents' knowledge of viruses was best in government organisations. He did a large-scale questionnaire survey in Finland in the summer 1993. There were not macro viruses at that time yet, so today the virus situation is a bit different. How important is virus prevention? The most positive attitude to virus prevention was in government organisations. It was found that 90 percent of the government organisations used some kind of anti-virus program, the same in local authority organisations was about 55 percent and in companies, it was over 60 percent.

In Malaysia, the money estimated lost due to Code Red and Nimda outbreak was RM 21 million, and RM 31 million estimated lost due to Blaster and Nachi (Madihah 2004). In order to get information about the computer viruses awareness among users, prevention levels in organisations and the impact computer viruses have in Malaysia, a questionnaire survey research was conducted (Madihah et al. 2006).

Based on the research by (Madihah et al. (2006), which was carried out at Putrajaya, Selangor and Kuala Lumpur, the findngs can be summarised as follows:

1. Majority of the respondents which is 92 percent had been infected by computer viruses while only 8 percent had not been infected. Majority of the respondents had encountered virus and 46 percent of them do not realise it when they are faced with virus problems. The result shows lack of respondents' awareness to virus problems.
2. Most of the respondent installed anti-virus software computer into their computer and update their anti-virus signature and only 22 percent of the respondents did not update their anti-virus signature file. Nowadays, it is very

important to update the anti-virus signature file regularly which could help to reduce the possibility of being infected with new viruses. Even though the result showed that majority of the users installed and updated the signature of anti-virus regularly, users should be aware that if there was one user who did not update the anti-virus software it would affect other computers in the same network, as virus can spread throughout a computer system or network. Every program that gets infected may also act as a virus and thus the infection grows.

3. Besides the awareness on updating the virus software, another aspect that should be emphasised is the action taken by users once their computers infected by virus. The result showed 44 percent choose to solve the problem themselves, 33 percent will contact IT department or technical support team, 7 percent will contact anti-virus vendor, 6 percent just ignore and 1 percent did not know what to do.

4. The respondents were requested to rank their own level of knowledge regarding viruses. Good level of knowledge is highly ranked and followed by poor level of knowledge. These 2 groups contribute to the majorlty of the respondents' level of knowledge. The small difference between these 2 groups indicate the need to educate the respondents about viruses which is one of the objectives for this research. Only minority (6 percent) of the respondents had a very good knowledge about viruses on Windows platform.

CONCLUSIONS

All the steps and recommendations given in this paper which are based on the research and testing that was conduted. Finding of this research can be used as guidance by users and organisations in identifying, recovering and defending against viruses. As for the analysis conducted on the questionnaires, finding showed that users still lack awareness on computer viruses and it is very important to equip users with knowledge in handling computer virus. The analysis also indicates that a lot of efforts still need to be carried out in order to educate the public about viruses.

REFERENCES

Alias, A.J., Mohd Supian, M.K. & Sim K.Y. 2001. Linux Based Local Area Network Intrusion Detection System. *Proceedings of the IEEE Malaysia International Conference on Communications 2001 (MICC2001).* Kuala Lumpur, Malaysia.

Chia Keong. 2003. Analysis and Design of Intrusion Detection System Implementation. M.Sc.Comp Dissertation, Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya.

David Perry. July 2002. PC Answers Issue 108. (Online). http://www.pcanswers.co.uk/tutorials/default.asp?pagetypeid=2&articleid=7929&subsectionid=607 (1 April 2008).

Fred Cohen. 1990. *A Short Course on Computer Viruses*. ASP Press.

Fred Cohen. 1991. Trends in Computer Virus Research. (Online). http://vx.netlux.org/lib/afc06.html (1 April 2008).

Hafiz bin Mohd Sarim. 2002. The Effectiveness of Detection Methods in Intrusion Detection Systems. M.Comp.Sc. Disseratation, Fakulti Sains Komputer dan TeknologiMaklumat, Universiti Malaya.

Indefense Website. 2004. Malicious Code. (Online). http://www.indefense.com/manuals/white/malicious.htm (1 April 2008).

Jeffrey Kephart & Steve White. 2001. How Prevalent are Computer Viruses? (Online).

http://www.research.ibm.com/antivirus/SciPapers/Kephart/DPMA92/dpma92.html (1 April 2008).

Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson. 2004.

2004 CSI/FBI Computer Crime and Security Survey. Computer Security Institute

Madihah Mohd Saudi. 2004. Situational Report on Major Worms Outbreaks Up to Year

2003 in Malaysia. (Online). http://www.mycert.org.my/other_resources/NISER-MYC-PAP-7070-1.pdf (1 April 2008).

Madihah Saudi, Shaharuddin Ismail and Mohd Najib Masdan. 2006. User Knowledge and Attitude of Computer Viruses In Malaysia. *International Journal of Learning 2006* 13 (8): 112-121.

Malaysia Computer Emergency Response Team. 2005. Incident Statistics 2005. (Online). http://www.mycert.org.my/abuse-stat/index.html (1 April 2008).

Marko Helenius. 1994. Computer Viruses in Finland - A Questionnaire Survey. Master Thesis of Sciences, University of Tampere.

Mazni Zambri. 2003. Evaluating Intrusion Detection Systems in a Unix Based Environment. Master Dissertation of Software Engineering, Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya

McDuffie, R. Steve. 1994. Defending Against Computer Viruses. *The CPA Journal.* (Online).http://www.nysscpa.org/cpajournal/old/15703023.htm (1 April 2008).

Microsoft Website. 2004. What is a Virus, Worm or Trojan Horse? (Online). www.microsoft.com/security/articles/virus101.asp (1 April 2008).

CyberSecurity Malaysia. 2002. NISER ICT Security Survey for Malaysia 2001/2002. (Online). http://www.cybersecurity.org.my/ (1 April 2008).

CyberSecurity Malaysia. 2004. Malaysia ISMS Survey 2003. (Online). http://www.cybersecurity.org.my/ (1 April 2008).

Nicholas Weaver. February 2002. Future Defenses: Technologies to Stop the Unknown Attack. (Online). http://online.securityfocus.com/infocus/1547 (1 April 2008).

Roger A. Grimes. 2001. *Malicious Mobile Code : Virus Protection for Windows.* First Edition, 56. O' Reilly & Associates, Inc.

Shukor Sanim Mohd Fauzi. October 2003. A Study On Computer Viruses Attacks and The Way To Cure Them. Degree Thesis, Faculty Information System Engineering, UITM, Malaysia.

Summers, W.C. & Naimah Mohd. Hussin. November 1991. Computer Viruses and Practicing Safe Computing. *Proceedings of EDUCOMP '91, National Symposium on Educational Computing.* Kuala Lumpur, Malaysia.

Summers, W.C. and Zaidah Ibrahim. November 1991. Computer Literacy – What Should We be Teaching Our Students? *Proceedings of EDUCOMP '91, National Symposium on Educational Computing*. Kuala Lumpur, Malaysia.

Summers, W.C., Zaidah Ibrahim & Naimah Mohd Hussin. September 1992. *Computer Viruses: What They Are and How to Prevent Them.* Federal Publications, Kuala Lumpur.

Summers, W.C. & Zaidah Ibrahim. November 1991. Computer Viruses: What are They and How do We Combat Them. *Proceedings of EDUCOMP '89, National Symposium on Educational Computing*. Kuala Lumpur, Malaysia.

Sureswaran Ramadass, Azlan Bin Osman, Rahmat Budiarto, N. Sathiananthan, Ng Chin Keong and Choi Sy Jong. 2003. Real-Time Virus Detection System Using iNetmon Engine. Network Research Group, School Of Computer Science, University Science Malaysia, (Online). www.qgpop.net/2003fukuoka/papers/B6-1.doc (1 April 2008).

Madihah Mohd Saudi
Faculty of Science and Technology
Islamic University College of Malaysia (KUIM)
Bandar Baru Nilai
71800 Nilai, Negeri Sembilan.
madihahsaudi@yahoo.com