Yui Kee Computing Ltd.

Newsletter

February 2002

Contents

Contents 1
Editors Notes 1
Incident Update 1
Hong Kong Information Infrastructure Expo 1
Ten Rules of Common Sense Anti-Virus 2
Anti-Virus Technology Update 3
Microsoft's New Direction? 4
Sophos Anti-Virus MailMonitor for Exchange 2000 4

Editors Notes

This month, Kenneth Bechtel reminds us of the basics that can keep our computers safe. Also look out for us at the Hong Kong Information Infrastructure Expo.

Allan Dyer

Incident Update

CERT/CC announced many vulnerabilities in SNMPv1 on 12th February. SMNP is used in many systems for management and control, and a large number of implementations, from many vendors, have similar flaws. Currently, there do not seem to be attackers exploiting these, but that is just a matter of time. Sites that use SNMP should check http://www.cert.org/advisories/CA-2002-03.html

W32/Yarner started spreading rapidly on 19th February, but it was quickly apparent that it would have minimum effect outside Germany. The virus arrives in an email that appears to be from a Trojan information website. The German message explains that it is a new version of a utility that provides warnings if a premium-rate phone number is dialled. Of course, if it is run, it provides no benefit, but emails itself to many addresses, and it may also delete files from the hard disk. No incidents have been reported in Hong Kong.

Hong Kong Information Infrastructure Expo

Visit us at **Booth G27** and **SME IT Clinic** at the mega HKII Expo (Mar 7-10).

Thanks for the HKITF's facilitation, we have been invited by Hewlett-Packard Hong Kong Limited as their "Business Partner" to present Anti-Virus and Information Security Solutions at their Pavilion. We will have exclusive **Special Offers** of premier Anti-Virus and Content Security software bundled with HP's high performance servers.

You can also meet our consultants / "doctors" in the SME IT Clinic Room C at the following times under the speciality on "IT Security & Risk Management":

Mar 7th: 3.30-4.00pm & 4.30-5.00pm

Ten Rules of Common Sense Anti-Virus

Kenneth L, Bechtel, II
Team Anti-Virus

1. Buy and keep up-to-date, Anti-Virus Software. If you fail to keep it up-to-date, you might as well not have anything at all.
2. Just because you trust a person with your house key, doesn't mean they practice safe computing. If you don't know why they are sending you a file don't double click on the attachment, ask why it was sent. A healthy dose of paranoia will save you time, energy and frustration.
3. Recordable CDs are cheep, your data's not. With a CD Burner costing below $150 and the CDs less than $.25 each, There's no reason not to make regular back ups of your information. This goes easier if you store your documents in the "My documents" folder. If you say, "my data's not important", then why are you wasting space and saving it in the first place? If it's important enough to save, it's important enough to back up.
4. You don't trust your family doctor to treat cancer, why do you trust a general practitioner to destroy your data to cure a virus? Most Computer shops will use Anti-Virus Software to cure your PC of any infection. Unfortunately, Viruses have become the fall guy for any and all PC Problems Technicians can't explain. Be very cautious when you are told you'll have to reformat your computer to remove the virus. THERE has NEVER been a case where the virus was so unrecoverable that the drive needs to be reformatted. In some cases this will NOT remove the virus. Now there may be times when you will have to reinstall a program or the operating system (Windows, Linux, MAC OS) because of corrupt files, but this does not require a reformat. Of course this applies only to the statement of "You have a virus we have to wipe the entire system", if a virus has already "wiped the system" you can't boot into your OS, and that is a different story.
5. Learn the basics of the computer. You already know (if you drive), that you have to put petrol (gas), change the oil, check the tires and have the vehicle serviced periodically, or it stops running. You don't have to be an expert on the internal combustion engine; you can do the simpler tasks yourself and let a mechanic take care of the more complex items. The same applies to your computer. Understand things like directories (folders) and how to tell where you're saving your files, learn how to "change the oil" by updating your anti-virus and installing the service packs and patches for the OS and other software, and put gas in it by defraging and running scandisk. By having a basic understanding of your computer, you will also better know when something is wrong, and can call the "auto Club" when the "tire goes flat".
6. Install and use a "Personal Firewall" Granted they are not perfect, granted they're easy to defeat for a determined attacker, but, when used in conjunction with current anti-virus, they will increase your protection immensely. If you are on broadband, either DSL, or cable, consider investing in a "router" with built in firewalling. There are several, and run less than $200. Even if your provider doesn't permit sharing of the connection, you don't have to violate your agreement, you can put the router between your cable/DSL Modem and your PC, and still be in agreement, but be a LOT more secure. Just remember to keep your eye on the manufacture's site to apply any updates, and not allow insecure remote "updates" you may be shooting yourself in the foot if you do.
7. If someone tells you they think you have a virus, don't ignore them. You owe it to yourself and your friends to at least update your Anti-Virus Software and do a system scan. As hard as we try, sometimes things do get past, and it's always better to check and be clean than to remain infected.

8. Don't believe everything you hear. While it's nice to warn your friends and family about the latest threat, first make sure that you're not sending them a hoax. Spending a few minutes checking out sites like http://www.vmyths.com/ can quickly save you some embarrassment and make you look like a guru when you tell someone else they are sending along a hoax.

   Second, before you mass mail out the alert, be sure your "audience" wants to hear it from you. Many people already subscribe to a vendor's alert list and may not want the extra mail, be polite and ask (you only have to ask once), before putting someone on a mailing list.

9. Not all cute things are safe. While Flash movies, games, and other little "Nifty" programs are often enjoyed by everyone, it is not the best or safest to send it in email. This can cause aggravation for people that are on slow dial up connections, and helps viruses spread. If you have something you feel your friends will enjoy, or find useful, provide a weblink to the original source. This gives your friends the option to download it, or not, and also is safer as the originator, if they are reputable, is less likely to have an infected or corrupted version on their site. Likewise, if some one sends you a file, politely tell them you'd prefer a link to the original, if they can provide it. Of course if someone ASKS you to send them the file, this is a different matter.

10. Don't share your hard drive. If you do need to provide some file and print sharing, don't give the keys to the kingdom, use a password where you can, and ONLY give the minimum that you have to a directory (folder) is much better than giving all of C$. If you have to give a C$ administrative share (like in companies that use SMS) limit the number of people who can use it.

Anti-Virus Technology Update

On 20 February our Chief Consultant Mr. Allan Dyer presented a technology update on "Anti-Virus Past, Present and Future" to government department representatives at the invitation of the HKSAR ITSD.

Tailor made IT security Awareness Promotion & Training in English or Cantonese can be arranged via our Business Development Manager Ms. Karen Cheung, please call 28708552 to discuss or send your requirements to karen@yuikee.com.hk

Some example topics include:

- Anti-Virus Technology update
- User Awareness Training
- Security Incident Handling & Response
- Intrusion Detection & Monitoring
- IT Security Policies & Management

Microsoft's New Direction?

Last month we discussed Microsoft's "Trustworthy Computing" initiative. Some people do not seem impressed by it, see http://www.bbspot.com/News/2002/01/security.html if you have a sense of humour.

Sophos Anti-Virus MailMonitor for Exchange 2000

Sophos has released an Anti-Virus solution for Exchange 2000. MailMonitor for Exchange 2000 detects, reports and disinfects viruses in Exchange 2000 mailboxes. It is installed on Exchange 2000 servers and operates in immediate, scheduled and real-time modes. Infected body text or attachments are deleted, quarantined or automatically disinfected. Comprehensive messaging allows MailMonitor to notify administrators, senders and recipients of any viruses found. MailMonitor for Exchange 2000 can find viruses in attachments compressed with ZIP and other popular compression utilities.

Virus detection and disinfection is performed by the high-speed Sophos virus detection engine, which allows easy, central and transparent updating of virus definitions.

How it works

Sophos MailMonitor for Exchange 2000 uses the SAVI (Sophos Anti-Virus Interface), which is included on the CD as part of the MailMonitor installation.

Once installed, MailMonitor operates in three modes:

- Immediate: scans Exchange 2000 mailboxes immediately for infected attachments.
- Scheduled: scans Exchange 2000 mailboxes on scheduled days and at
- specified times.
- Real-time: intercepts and scans email attachments as they are received.

Infected body text or attachments are disinfected, deleted or quarantined. The administrator has full control over quarantined messages.

Features

- Detects and disinfects viruses in incoming and outgoing email.
- Allows multiple scheduled jobs to be configured for automatic scanning of mailboxes at predetermined times.
- Scans Exchange 2000 mailboxes on demand.
- Provides automatic centralised reporting of virus incidents.
- Allows remote administration.
- Protects WANs and LANs from viruses before they enter the organisation.
- Is transparent to end users.

- Detects viruses in compressed attachments including recursive ZIP, LZH,
- ARJ, RAR, GZIP, TAR and CMZ archives.
- Detects Macintosh viruses.
- Is updated constantly.
- Easily detects polymorphic viruses using Sophos's advanced Virus Description Language (VDL) and a built-in code emulator.

System requirements

Microsoft Exchange Server 2000 with Windows 2000 (Service Pack 1)

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE