Yui Kee Computing Ltd.

# Newsletter

April 2003

## Contents

## Editors Notes

W32/Klez.H@mm is still, by far the most common computer virus, but this month all eyes are on a new biological virus. What are the relationships between SARS and Information Security? Several perspectives are given below.

## A Big Joke on April Fools Day

The first of April is traditionally a day for practical jokes and this year a 14-year-old boy played his idea of a big joke on Hong Kong people. The boy set up a web page very similar to that of the Ming Pao newspaper, with the top story being that Hong Kong was about to be declared an infected port. He registered a domain name (www.mingpaonews.com.ultra4vx.com) that, at a quick glance, looks similar to the real domain name for Ming Pao (www.mingpaonews.com). He then started rumours, including a link to his false site. The rumour spread rapidly through telephones, email and ICQ. As a result, some people panicked: supermarket shelves were emptied and the Hang Seng Index plunging about 100 points.

This is not a new technique, another well-publicised case occurred in May 2002 when a fake BBC World website announced the death of Microsoft's CEO, Bill Gates. It is difficult for site owners to defend against such hoaxes, because any website can be copied. Detection relies on users being observant and knowing about host names and directory paths. However, in most cases just trying a few links on the page reveals the hoax because hoaxers rarely clone more than the first page.

The fake site probably infringed trademark rights, although "fair use" might be invoked to defend a parody, this was a clear attempt to deceive. There are no easy solutions to this type of hoax, users need to be educated, and at least one person needs their sense of humour checked.

# Hong Kong Government Plans Change to Cybercrime Laws

The Government has issued a Legislative Council Brief (File Ref: SBCR 11/14/3231/88) about its proposals to change the Criminal Justice Ordinance. If passed, the changes will allow Hong Kong courts to exercise jurisdiction over computer offences (including unauthorised access, criminal damage relating to misuse of a computer and access with criminal or dishonest intent) when the crimes are committed or planned outside Hong Kong.

These are the long-awaited changes that will make dealing with cybercrime a little easier. The Internet makes it easy for criminals to work Internationally, people in jurisdictions A and B can conspire together to use computers in jurisdiction C to attack computers in jurisdiction D, the changes will allow Hong Kong courts to take action, whether Hong Kong is A, B, C or D.

# SARS and Information Security

Biology and information technology do not usually come together, but SARS is affecting all human endeavours. The challenges for IT might not be as critical as those for the medical sector (where "life or death decision" means exactly that), but they have a dollar value. These three articles explore some of the implications, including hoaxes, computer viruses and encryption.

## New Coronex computer worm exploits SARS worries

April 24, 2003 - Sophos has issued a warning of a new computer worm that takes advantage of growing concern over the biological SARS virus.

Known as W32/Coronex-A, the mass-mailer worm forwards itself to all contacts in Outlook address books and attempts to dupe innocent computer users into opening an attachment offering details on the current SARS epidemic.  The Coronex worm uses a variety of subject lines, message bodies and attachment names to entice users into double-clicking including: "Severe Acute Respiratory Syndrome", "SARS Virus" and Hongkong.exe

"The worm has been deliberately coded to exploit the public's genuine concern about SARS, and is just a further demonstration of the ways that virus writers attempt to use psychological trickery to spread their creations," said Charles Cousins, managing director of Sophos Anti-Virus Asia.  "It is important that people call this virus by its proper name, Coronex, rather than 'the SARS virus'. If they don't it will only add to the confusion and panic.  In particular, anti-virus firms should act responsibly in the way they communicate news of this virus to the public by ensuring their products, alerts and press releases do not refer to this computer virus as 'SARS'".

"As ever the advice to users is simple: practice safe computing, keep anti-virus software up to date and patch against operating system vulnerabilities.  This will dramatically reduce the risk of becoming infected by a new virus," continued Cousins.

Sophos recommends companies consider using products such as Sophos MailMonitor to block all Windows programs at their email gateway.  It is rarely necessary to allow users to receive programs via email from the outside world.  There is so little to lose, and so much to gain, simply by blocking all emailed programs, regardless of whether they contain viruses or not.

More details of the Coronex worm are available at

http://www.sophos.com/virusinfo/analyses/w32coronexa.html

## Watch Out for the Other Viruses

Allan Dyer

The outbreak of SARS is a serious concern, and many people are doing excellent work in fighting its spread. However, some of the measures might lead to an outbreak of a rather different kind: computer viruses. Fortunately, no one is going to die from a computer virus, but they can have an impact on our work and economically. In the current economic climate we should try to prevent the avoidable damage caused by computer viruses.

So how will measures to control SARS affect computer viruses? The impact is via the increased interest in teleworking. Staff may need to be quarantined, or a company might seek to minimise risky human contact in general. What better way to minimise human contact than by keeping staff in their homes, linked to the outside world electronically? Obviously, there are security concerns when staff utilise office resources from their home computers, and the first thought is to install a VPN or other encrypted link (see the article below about the Need for Encryption). However, this only solves one part of the security problem - the channel is secure, but are the endpoints secure? Hopefully the office already has adequate security in place, but the average home PC is vulnerable - personal firewalls are not very common, and the only anti-virus software used might be the free version, bundled with the new PC and now hopelessly out of date. A hacker or virus that takes over the home PC can then make use of the secure connection to access corporate information.

Companies, particularly SME's, might dismiss the hacker threat - there are only a limited number of hackers, and why would they be interested in attacking one particular SME among thousands? There are some good answers to that, but the more likely threat is viruses. Viruses are generally indiscriminate, and, because they replicate, there is no limit to the number of simultaneous attacks they can make. Many home PCs are probably already harbouring a variety of viruses, using those machines all day is giving the viruses more time to act, staying online is giving them more time to spread and connecting those machines to corporate networks is giving them access to new address books to contact and new data to damage. The result of large numbers of people teleworking could be a sudden jump in computer virus incidents.

One virus that could benefit from teleworking is W32/Klez.H@mm, which is currently at the top of various incident lists. In fact, W32/Klez.H@mm has been at the top of incident lists for most of the past year. Occasionally, another virus has spread quickly and temporarily eclipsed it, but soon the usurper fades away leaving Klez triumphant. Why is Klez so persistent? Klez, like many other successful viruses, sends itself in email to as many addresses as it can find. Klez not only looks for addresses in address books, but also in text files, web pages, word documents and many other file types. However, Klez also uses one of these addresses in the From: field of the email, so the email appears to have originated from a different location. I think that this is the key reason why Klez has persisted so long. When an "ordinary" mass-mailing email virus infects a machine, it sends out many messages and users or mail gateways with up-to-date anti-virus software detect it and send back a complaint or warning, "you're sending viruses". The user of the infected machine (who may not care about viruses) is pressured to do something about it. In the case of Klez, the complaint/warning either gets sent to the wrong address, or, if the receiver understands Klez's nature, never gets sent. The user of the infected machine is never warned, and never cleans their machine or updates their anti-virus software. As Klez is currently the most prevalent virus, it is in a good position to benefit from a jump in virus incidents due to increased teleworking.

So, companies considering implementing teleworking should remember to secure the endpoints as well as the communications channel. The home PC should be protected to the same level as the corporate network, which probably includes updating with the latest security patches, installing up-to-date anti-virus software (and keeping it up-to-date) and installing a personal or distributed firewall (such as F-Secure Distributed Firewall). The advantage of a distributed firewall is the centralised management, so the policy protecting all the home workers can be easily standardised, and the technical staff are not burdened with helping each user set up the software. The good news is that companies using F-Secure and Sophos already have the licenses - the standard license terms permit the installation and use of the software on the users home machines if their office machine is licensed. The updating of the home users is also not a problem, as both F-Secure and Sophos provide mechanisms for this.

Educating the teleworkers about their essential role in corporate security is also essential. A computer virus is not going to kill you, but it might be the last straw that breaks a company facing a difficult economic environment.

Further Information:
"Remote User Security: Your IT's Achilles Heel?" http://www.sophos.com/wp/arcati_ru.html
"Remote Update FAQ" http://www.sophos.com/support/faqs/ru.html

## Telecommuting - The Need for Encryption

Telecommuting, by definition, puts corporate data onto external networks, and, unless your company has limitless money to install leased lines to every employee's home, that means public networks: the Internet.

How much protection does the data need? It depends, of course, on the company and the value of the data. Some companies might need to transfer valuable trade secrets, or highly confidential personal information. However, without exception, the most valuable data being transferred is the authentication information. In reality, listening to one interesting session in the sea of the Internet is technically difficult, and waiting for the victim to transfer the desired information could be frustrating. If the attacker can capture the victim's user id and password, then far more possibilities open up. The attacker can login and request the desired data directly, or modify it, or delete it, at will. Therefore, the authentication information must be encrypted in transit.

Conceptually, the simplest method of providing the encrypted connection is a VPN, it works at the network layer, all communications between the endpoints is automatically encrypted and theoretically the home workers have the same access as from their office desktops. This is theoretical because the office probably has a 100Mbit or faster LAN, but the external link is much slower and easily overwhelmed by a few telecommuting broadband users. It may therefore be appropriate to force the users to think a bit more, transfer files only when needed and save work in progress on the local disc.

Encryption at the application layer, such as SSL and SSH, is easy to set up and can provide encrypted connections for selected services. SSL, of course, is well known for access to secure websites. Most browsers and web servers include support for it, and it would be the obvious choice for making an Intranet server accessible to teleworkers. SSH, short for Secure SHell, is usually thought of as a secure replacement for insecure Unix services like rlogin, rsh, and rcp but any TCP connection can be tunnelled through it and sftp provides easy file transfer. There are also clients and servers available for Windows. So SSH can provide flexible encrypted connections for many purposes. Need to access the corporate email? Then tunnel POP or IMAP through SSH. Features like public key authentication and the ability to specify an application to launch when the connection is established can make the process of connecting as simple as clicking on an icon for the user. File transfers are simple with a drag-and-drop user interface.

For stronger authentication, SSH can be used with smartcards including Aladdin's eToken.

Evaluate your requirements and choose the encryption option for your teleworkers that meets your needs and budget.

Contact us for more information on security and teleworking: cdsales@yuikee.com.hk

# Computer Virus Prevalence Survey

ICSA Labs have published their 8thComputer Virus Prevalence Survey. The survey found that the growth rate of malicious code infection has slowed. There also appeared to be a move from "Bug Bang" (for example, Code Red) events to persistent threats (such as Klez).

Full Survey:

http://www.icsalabs.com/2002avpsurvey/index.shtml

# Stupid Security "Winners"

Privacy International has announced the results of the Stupid Security Competition, mentioned in the February newsletter. The competition, launched in February, attracted almost 5,000 nominations from 35 countries. While the air security sector dominated the competition, nominations arose from almost all areas of private and public sector activity. The runner-up in the category "Most Inexplicable Security Measure", where Heathrow Airport confiscated the *packaging* of some Gunpowder Tea, but **not** the tea itself, is particularly interesting.

Full details:

http://www.privacyinternational.org/activities/stupidsecurity/

# Sophos's MailMonitor improves protection against mass-mailing viruses

Sophos, a world leader in anti-virus protection for businesses, has released new versions of its MailMonitor products for Microsoft Exchange 2000 and Lotus Notes/Domino servers. These two products add significantly to the virus protection, message handling and integration features of the solutions.

Sophos MailMonitor for Exchange 2000 v1.5 scans for viruses in all incoming emails, enabling network administrators to either disinfect, delete or quarantine infected messages. MailMonitor for Exchange 2000's new features include support for the Microsoft virus-scanning Application Programming Interface (VSAPI) 2.0, allowing full scanning of the Exchange information store in both active and background scan modes.

Furthermore, the new version of MailMonitor for Exchange 2000 can scan newsgroups, both internal and internet Usenet discussion boards, intercepting known viruses, Trojans and worms in real-time. A selective "strip all" facility can also allow system administrators to prevent unknown viruses from being distributed via Exchange newsgroups by blocking all attachments.

"Companies are more likely to be attacked by a virus via email than any other route," said David Mitchell, MailMonitor product manager at Sophos. "These new versions of our MailMonitor product suite ensure that firms can focus on their core business without disruption."

Black Box, a leading worldwide network services company providing computer communications, networking services and related products to businesses of all sizes, is already benefiting from the high levels of virus protection offered by MailMonitor.

"With offices spread around the world, email is a very important communication tool for us," said Doug Boast, Group MIS Manager UK & Ireland of Black Box. "With an ever-increasing number of viruses travelling via email, it is vital for us to have first-class virus protection running at our email gateway. The latest MailMonitor offering from Sophos means we are even better protected against the latest virus threats."

Sophos MailMonitor for Notes/Domino is now available for the R6 environment, as well as the already supported R4 and R5. It detects and disinfects viruses in Lotus Notes databases and email. Installed on a Lotus Domino server, it intercepts and scans email attachments as they are sent and received providing round-the-clock protection.

Both MailMonitor for Exchange 2000 and MailMonitor Notes/Domino detect viruses, Trojan horses and worms in compressed and archived file attachments, providing automatic centralised reporting of virus incidents and outbreaks. Administrators are automatically alerted on receipt of virus-infected emails. The products come complete with continual updates to protect against the latest viruses, deliverable 24x365 via secure download using Sophos's Enterprise Manager suite.

Contact us for more information about Sophos MailMonitor: cdsales@yuikee.com.hk

## Australia Launches Cybercrime Inquiry

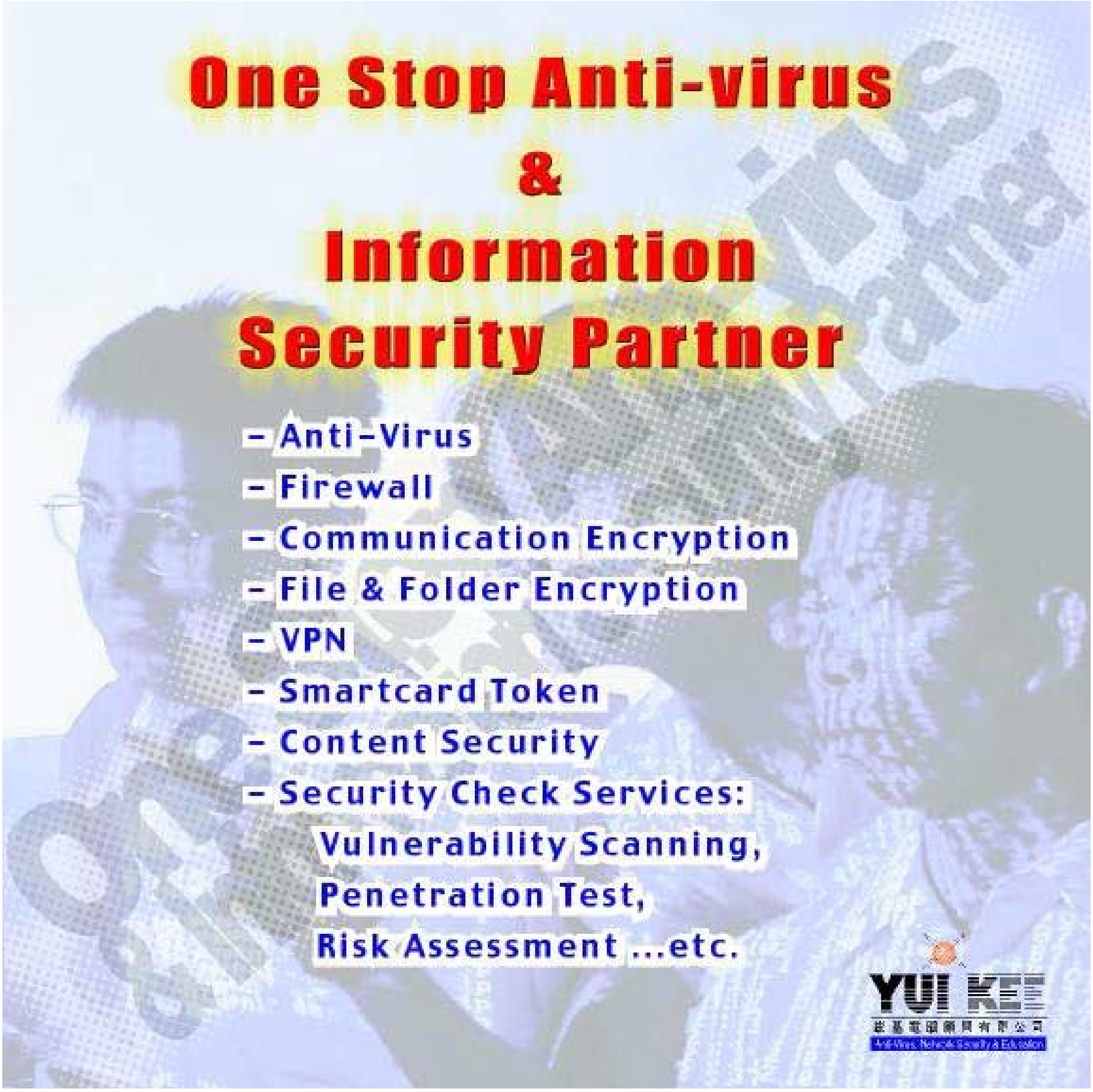
The Parliamentary Committee on the Australian Crime Commission inviting submissions for their inquiry into recent trends in cybercrime. Topping their list of concerns is child pornography and associated paedophile activity, followed by banking and threats to Australia's critical infrastructure.  Public hearings are planned for later this year.

Terms of Reference:

http://www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

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
銳基電腦網絡有限公司
Anti-Virus, Network Security & Education