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

Yui Kee Computing Ltd.

Newsletter

October 2003

Contents

Incident Update

W32/Sober.A@mm appeared 24 October, 2003. It arrives in a fake warning message about a new worm. One interesting feature is that if the domain of the recipient's email address is '.de' (Germany), '.li' (Liechtenstein), '.at' (Austria) or '.ch' (Switzerland), the message is in German, otherwise, it uses English.

W32/Mimail.C@mm first appeared on 31st of October, 2003. The worm spreads in e-mails as an attachment called PHOTOS.JPG.EXE, which is actually a ZIP archive that contains the worm's executable. The worm will try to perform a DoS (Denial of Service) attack against certain sites and to steal information from the infected computer.

Security Risks of Monoculture

Seven respected information security experts have released a paper pointing out that the ubiquity of the Microsoft operating system is a security risk. Worth reading.

Full paper:

http://www.ccianet.org/papers/cyberinsecurity.pdf

Opposing Comment:

http://www.ranum.com/security/computer_security/index.html

Sophos Anti-Virus receives Virus Bulletin 100% award on Windows 2003 Server

Sophos Anti-Virus (3.74) has been awarded the VB 100% award in the November 2003 edition of Virus Bulletin. This is the 22nd time Sophos Anti-Virus has won a VB 100% award, confirming its position as one of the most powerful virus protection products available.

Virus Bulletin tested 21 different anti-virus products for their detection rates, lack of false alarms, and speed of scanning. Sophos outperformed a number of competing products, which missed some of the commonly encountered in-the-wild viruses.

All Sophos products use the same virus-finding engine, ensuring consistently high detection rates across all platforms.

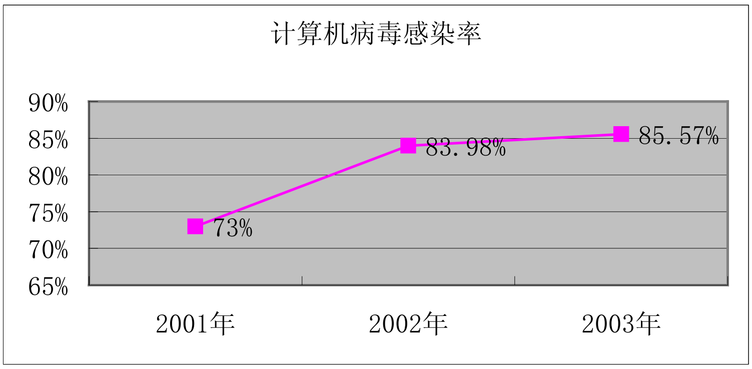
China (Tianjin) 2003 Information Security Executive Forum & China Computer Virus Incident Survey Press Conference

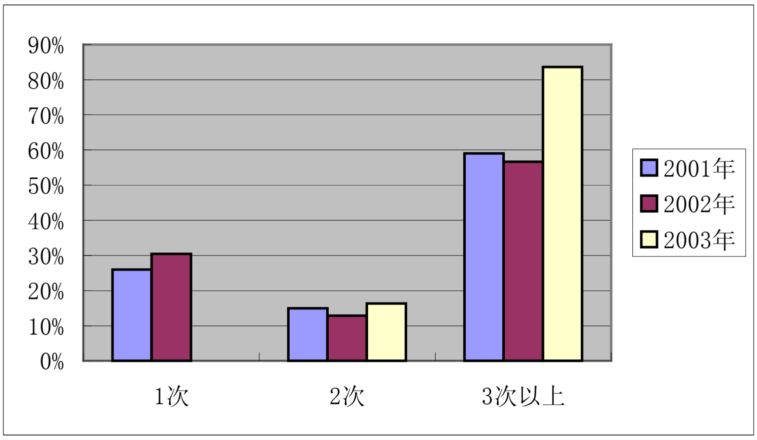
The National Computer Virus Emergency Response Centre, based in Tianjin, held a press conference on 20 October 2003 to announce the results of their third annual computer virus survey.

The results showed that the prevalence of computer viruses in China continues to rise. Also, many users are being hit three or more times.

A lucky draw was held for the survey respondants.

Immediately following the press conference, the Information Security Executive Forum was held. It featured many international speakers. Our Chief Consultant and AVAR President, Allan Dyer, spoke on "What is so Bad About Teaching Virus Writing".





Allan was not the only speaker from AVAR, Seiji Murakami, the Chairman from Japan; Charles Ahn from Korea and Randy Abrams from USA, Vice Presidents.

Chinese speakers included Shen Chang Xiang of the Engineering Academy of China, speaking on Active Defence; Du Yuejin of the National Computer Network and Security Management Centre, speaking about responding to Internet Worms; and Yang Yi Xian of the Beijing University of Posts and Telecommunications speaking about cryptographic techniques.

There were over 100 attendees, and the forum ended on 21 October with a visit to the National Computer Virus Emergency Response Centre itself.

Spyware Goes Commercial

Recent Spam with the subject, "What does your Lover do on the Internet?" has been offering an $89 program called LoverSpy. It claims, "Spy on Anyone by sending them an E-Greeting Card!", and, unlike the claims in most other Spam, it works.

However, nosey users should beware, "Sending this to someone with the intention of tricking them into running it is almost certainly a crime under the Computer Crimes Ordinance in Hong Kong" said Allan Dyer, Chief Consultant of Yui Kee Computing. Also, the fine print of the program's legal agreement allows LoverSpy's producers to look through the files!

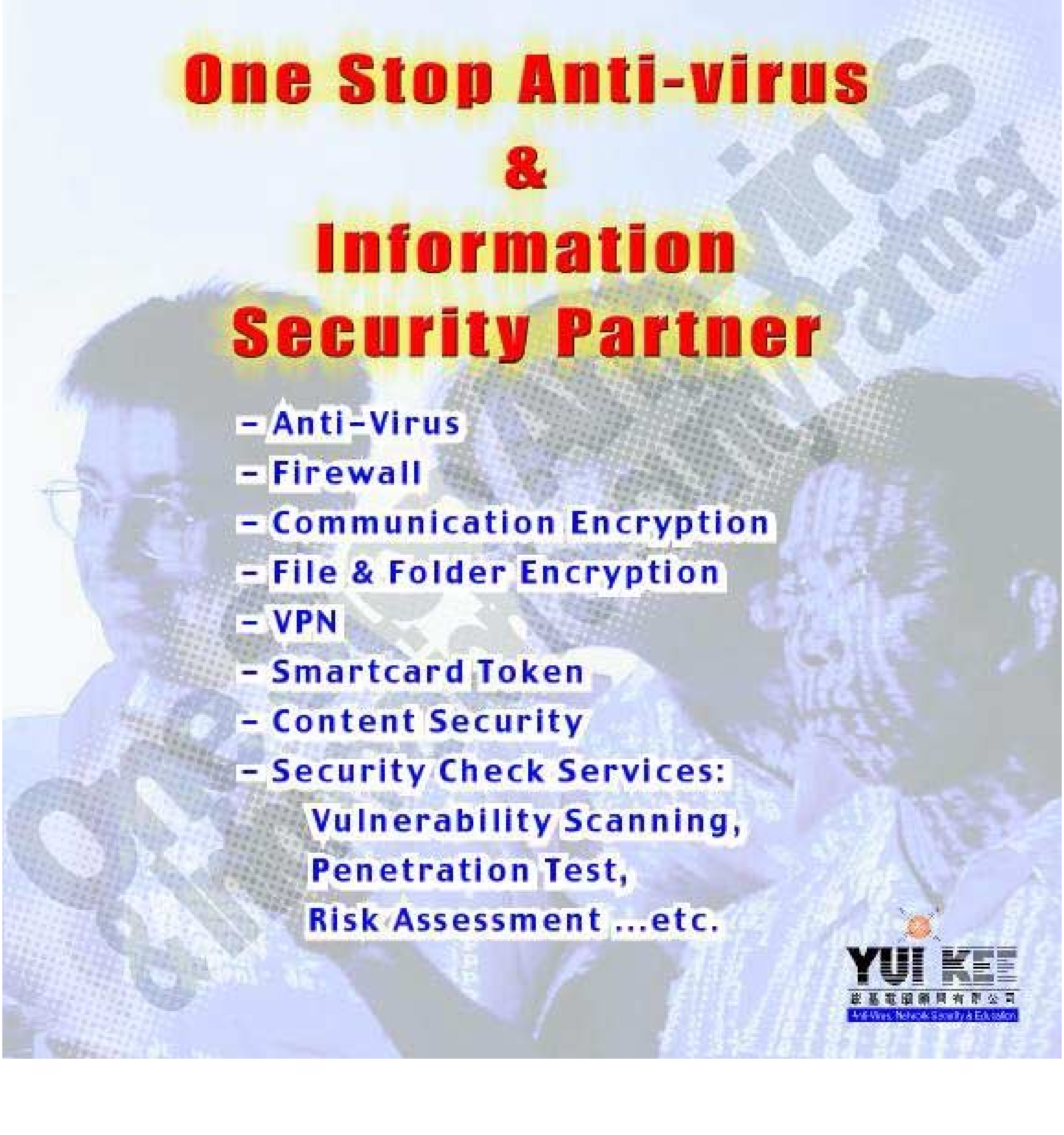
"For just $89 you can disclose your lover's secrets, perhaps including their online banking password, to an unknown company, **and** get yourself thrown into jail, what a bargain!", said Allan Dyer.

More information:

http://www.cnsnews.com/ViewCulture.asp?Page=/Culture/archive/200309/CUL20030929a.html

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