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

Yui Kee Computing Ltd.

Newsletter

March 2003

Contents

Incident Update

Two worms appeared near the beginning of the month. W32.Deloder.A targets Windows shares, on TCP port 445, it features a list of simple passwords that are used to attempt to gain access to the target machine. This emphasises the need for defence in depth - it can be blocked by: always setting strong passwords; or by disabling unnecessary shares; or by blocking port 445 at the firewall or personal firewall. It was first seen spreading on 9th March.

CodeRed.F, a trivial variant of earlier the Code Red worm, hit just two days later, on 11th March. The fact that it was able to spread at all suggests that many IIS servers have been installed without the preventive patches since the last outbreak.

Unusually, two buffer overflow vulnerabilities were announced in Sendmail, on 4th and 31st March. Either could allow the affected host to be compromised. Upgrade to Sendmail 8.12.9 is strongly recommended.

A critical vulnerability in the WebDAV component of Microsoft Internet Information Services (IIS) was announced in MS03-007. Microsoft has issued a patch.

W32/Klez.H-mm is still the most prevalent virus in email, MessageLabs is stopping about 11 thousand messages infected with it per day.

HKCERT Seminar

Future: Nightmare Scenario
• Speed
– Anything < 1 hour is faster than our reactions

Our Chief Consultant, Allan Dyer, spoke on "The Slammer Worm and the Trend of Massive Attacks" at the Hongkong CERT seminar titled, "Incident Response on the Hostile Network", on 18 March 2003. Mr Dyer noted that even a site not vulnerable to a particular attack can be adversely affected if other sites sharing the same ISP flood the connection, and emphasised the need to treat computer viruses and worms like a public health problem.

Other speakers included Roy Ko, Centre Manager of HKCERT/CC, York Mok, Chairman of HKISPA, and Wilson Leung, Premier Support Manager of Microsoft Hong Kong.

Materials from the seminar are available from the HKCERT website:

http://www.hkcert.org/event/event078.htm

Swedish Police Question Iraqi War Virus Suspect

According to reports in the Swedish press, police in Sweden have identified and questioned the author of the W32/Ganda.A virus, which spreads in email claiming to be spy satellite photos of Iraq. The virus is capable of creating English and Swedish messages, and it spread quite well in Sweden starting on 17th March.

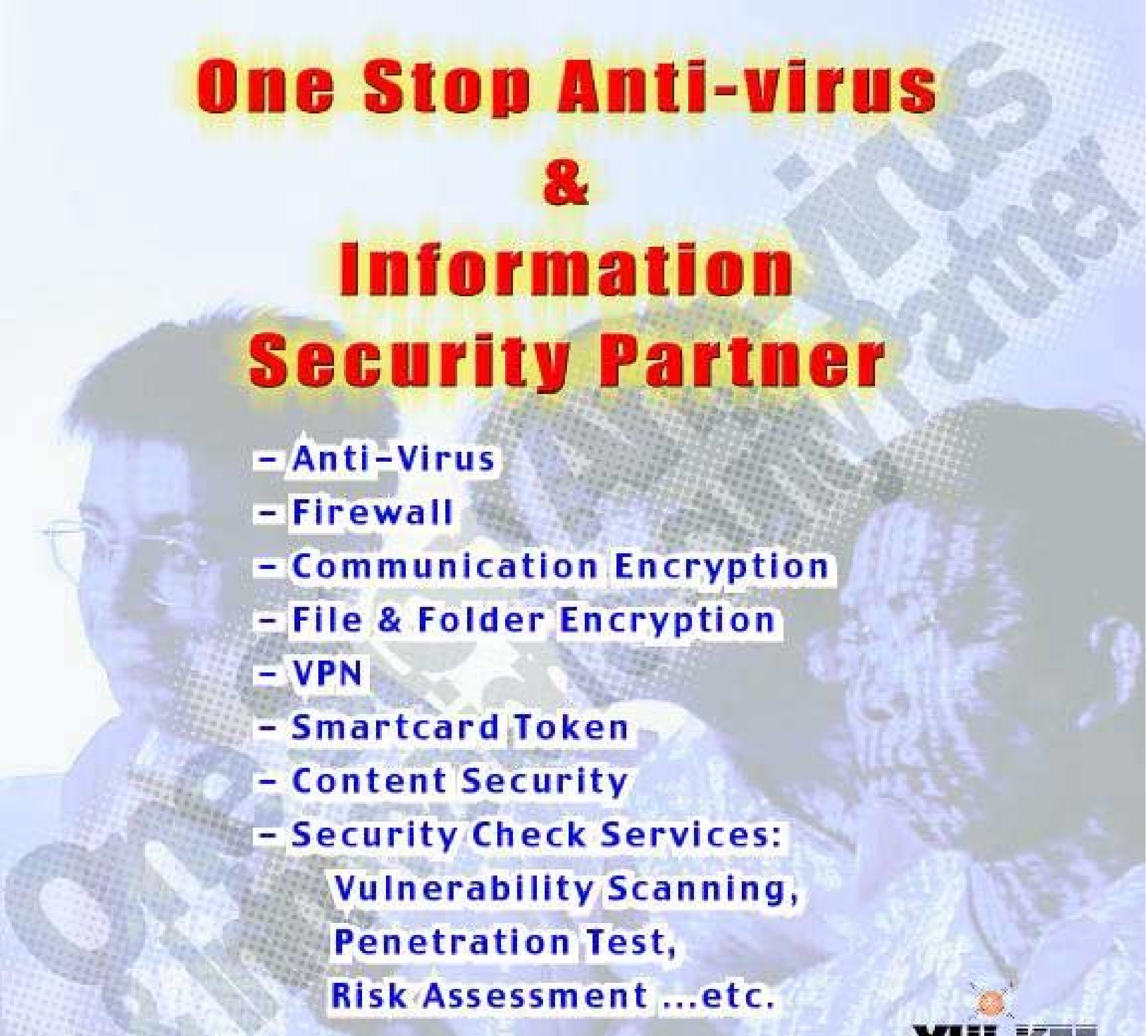
"The authorities appear to have moved quickly in locating this virus author," said Carole Theriault, anti-virus consultant at Sophos. "It is good to see computer crime authorities around the world taking the virus threat more seriously. The worm author was particularly insidious in using current events to spur the general public into double-clicking on the infected attachment."

Malaysian Security Conference

YB. Mr. Chia Kwang Chye, Parliamentary Secretary of the Ministry of Energy, Communication and Multimedia of Malaysia gave the special Key Note Address at SecurITy, a two-day conference held in Kuala Lumpur. He emphasised the information security as a prerequisite for global competitiveness, and reported on the development of MS ISO 17799, the Malaysian information security management standard derived from ISO17799.

Allan Dyer spoke on, "Developing and Implementing Effective Policies and Strategies" at the same conference.

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