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

Yui Kee Computing Ltd.

Newsletter

April 2004

Contents

Incident Update

The parade of worm variants continues, highlights include:

5 April	W32/Sober.F
7 April	W32/Netsky.S
21 April	W32/Netsky.X, W32/Netsky.Y
27 April	W32/Bagle.Z@MM
28 April	W32/Netsky.AB

On the 13th, Microsoft announced three critical updates: MS04-011, MS04-012, and MS04-013. Details and downloads are at the Microsoft website. Administrators of vulnerable systems should, of course, patch them as soon as possible. On 30 April, Hongkong CERT published a warning about worms exploiting the LSASS vulnerability described in MS04-011:

http://www.hkcert.org/valert/vinfo/lsass_worm.html

Hidden Messages

Patrick Lee

Over the years, virus authors have sought to convey messages in their creations. Quite frequently, these are not normally displayed, the virus code must be examined to find them. This year, the authors of Bagle, Mydoom and Netsky have traded insulting comments in this way. In April, although both the author(s) of Bagle and Mydoom viruses have stopped appending text strings inside their executables in April, the author(s) of the Netsky variants still have something to say. Here is a chronological list of the nature of the messages:

31st March 2004: W32/Netsky.R thanks "Mr. Bruce Schneider" *(sic)*; we have no idea why.

6th April 2004: W32/Netsky.T said it has backdoors but not for spam relaying. This time it thanks Russia and CCC.

17th April 2004: It seems that W32/Netsky.W is not created by the original writer(s), as it thanks Skynet or Netsky or whatever crew for the source code.

20th April 2004 W32/Netsky.Y greets the Bagle worm.

28th April 2004 The 27th variant of Netsky, W32/Netsky.AA "avenges" Bagle.

The Bagle and Mydoom authors have ignored Netsky’s threat and continue their mischief. These are intriguing glimpses into the mind of the authors, but are they just put there to mislead us?

The Long Arm of the (Hi-Tech) Law

British police have arrested a 21-year-old man for "phishing" in what is said to be the first case of if its kind in the UK and US authorities in Detroit have charged four men in connection with emailing fraudulent sales pitches for weight-loss products.

Sophos reports the details:

http://www.sophos.com/spaminfo/articles/phishingbust.html

http://www.sophos.com/spaminfo/articles/weightspam.html

9th Annual ICSA Labs Virus Prevalence Survey

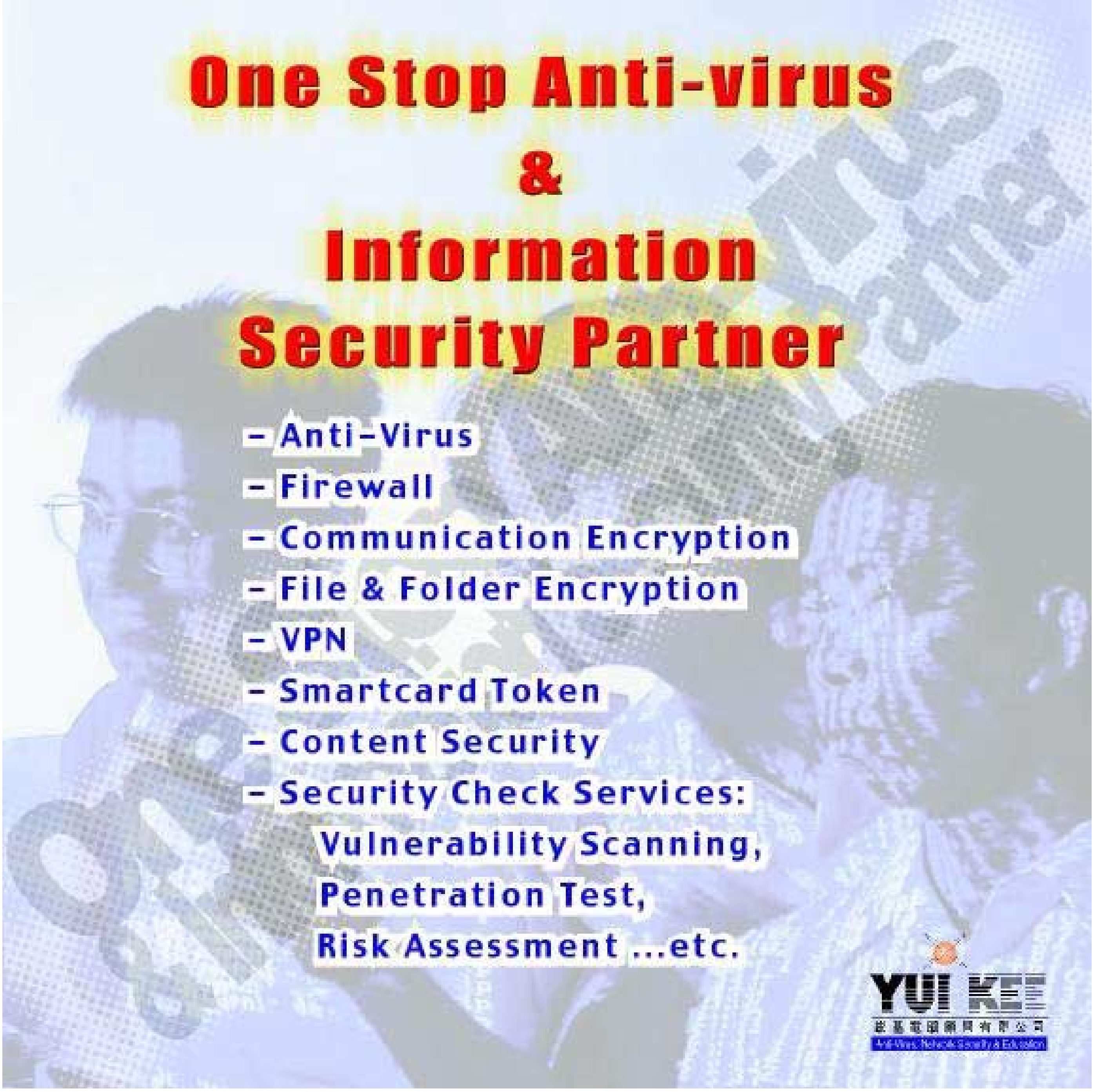
Each year, the ICSA Labs (an independent division of TruSecure) surveys around 300 large organisations to understand the malicious code situation and perceptions about it. Unsurprisingly, this year's results show the problem is getting worse, despite increased spending.

Dr. Peter Tippett, chief technologist at TruSecure Corporation commented, "These organizations are too often surprised by new malcode vectors and methods and then spend even more money and resources recovering from virus and worm disasters" and he advocates intelligent risk management.

More information at TruSecure's site:

http://www.trusecure.com/company/press/pr_20040322.shtml

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