Yui Kee Computing Ltd.

Newsletter

January 2005

Contents

Incident Update

- Tue Jan 11 20:16:36 2005 FSC: Bagle variant spreading again 2
- Tue Jan 11 20:16:36 2005 FSC: Worm defacing phpBB forum sites 2
- Wed Jan 12 10:31:32 2005 TREND: MS05-003_INDEXING_SERVICE High
- Wed Jan 12 10:31:32 2005 TREND: MS05-002_CURSOR_ICON_FORMAT High
- Wed Jan 12 10:31:32 2005 TREND: MS05-001_HTML High
- Wed Jan 12 15:46:40 2005 TREND: MS05-001_HTML_HELP_ACTIVEX High
- Thu Jan 13 18:16:39 2005 SARC: W32.Erkez.D@mm L3
- Sun Jan 16 06:46:39 2005 FSC: Mydoom sending porn mails 2
- Thu Jan 27 17:01:56 2005 NAI: W32/Bagle.bj@MM Medium
- Thu Jan 27 18:46:48 2005 FSC: Bagle.AY uses different icons 2
- Fri Jan 28 01:02:05 2005 SARC: W32.Beagle.AZ@mm L3
- Mon Jan 31 22:31:59 2005 NAI: W32/Sober.k@MM Medium

Microsoft Releases Anti-Spyware Tool Beta

Windows AntiSpyware is based on technology acquired from GIANT Company Software Inc. in December 2004 and is available for Microsoft Windows 2000 and later. It is claimed to help reduce negative effects caused by spyware, including slow PC performance, annoying pop-up ads, unwanted changes to Internet settings and unauthorized use of private information.

More information:

http://www.microsoft.com/presspass/press/2005/jan05/01-06NewSolutionsPR.asp

David Perry Denies CNN Accusation of Hacking Airport Check-in System

A CNN reporter dashes off a hot story, "airport … in chaos, … stranding, … fable for the information age, … foremost computer security experts flipped open their laptops and reopened the terminal…". Unfortunately, the reporter seems intent on creating not just a fable,

but a myth. Respected experts do not usually risk arrest and prosecution for unauthorised access, however keen they are to catch their flights.

Fortunately, VMyths gets to the truth: one of the suspects named in the article, David Perry clarified the incident: the experts only told Luxembourg airline employees to reboot the network.

More information:

http://www.cnn.com/2005/TECH/internet/01/18/cyber.security/index.html

Stupid ISP

On the Internet, your physical location becomes irrelevant… unless your ISP is Verizon. The American ISP has decided to blanket-blacklist email from Europe and Asia, only unblocking domains after receiving complaints. However, affected Verizon customers are organising a class-action suit over the disruption caused.

More information:

http://www.theregister.co.uk/2005/01/14/verizon_email_block/

http://www.theregister.com/2005/01/21/verizon_class_action/

French Trial Threatens Full Disclosure

The trial of Guillaume Tena in France is highlighting the question of whether it is a good thing to publically announce security flaws. Tena posted proof-of-concept code that revealed vulnerabilities in Viguard, an anti-virus product known only in France, to a French newsgroup in 2001. He later published his research on a website. Tegam, the company that produces Viguard, reacted by initiating a prosecution under French copyright law.

Tegam claimed that Viguard would stop, "100 per cent of known and unknown viruses", however, any student of computer viruses knows that perfect anti-virus software is a mathematical impossibility. Perhaps Tegam should be prosecuted under consumer protection or false advertising laws?

Tena actually used to be a virus writer and wrote the first e-mail virus ever, Happy99, according to Mikko Hyppönen at F-Secure. "He appears to be a good citizen now, but there might be some animosity still felt against him at anti-virus companies."

Tena said the case could have a big impact on the French computer security community. "This case is not about violating intellectual property, it's about Tegam trying to shut me up. If security research is stifled, companies could produce a flawed product and no-one would know any better."

More information:

http://www.theregister.com/2005/01/12/full_disclosure_french_trial/

http://www.zdnet.com.au/news/security/0,2000061744,39176657,00.htm

http://www.newsfactor.com/story.xhtml?story_title=Security_Researcher_Sued_for_Reporting_Flaws&story_id=29660

http://p2pnet.net/story/3519

In French: http://www.elastico.net/archives/002439.html

http://www.thecrimson.com/article.aspx?ref=505398

Jeffrey Lee Parson Jailed for 18 Months

A US District Court sentenced the author of a minor variant of the Blaster worm, Jeffrey Lee Parson, to 18 months in prison and 10 months community service. The sentence could have been harsher, the maximum sentence possible was 37 months. In a statement, Parson said: "I am grateful the judge gave a very fair sentence. I feel that the judge understood me. I hope young people can learn from my mistakes, and I am sorry to anyone who got hurt in any way by what I did."

Although the little fish has been caught and punished, the big fish - the person, or people, who wrote the far more successful first version of Blaster - is still free.

More information:

http://seattletimes.nwsource.com/html/nationworld/2002163455_webblasterworm28.html

http://www.sophos.com/virusinfo/articles/parsonsentence.html

http://www.theregister.com/2005/01/26/blaster_presentencing/

http://www.theregister.com/2005/01/31/blaster_kiddo_sentencing/

"Tasin" Worm Suspect Arrested

A 20-year-old man has been arrested in Ejica, near Seville, in connection with creating and spreading W32/Anzae, also known as "Tasin". The worm spread in Spanish language emails in November 2004, and it infected and caused damage to system files in thousands of computers in Spain and South America.

More information:

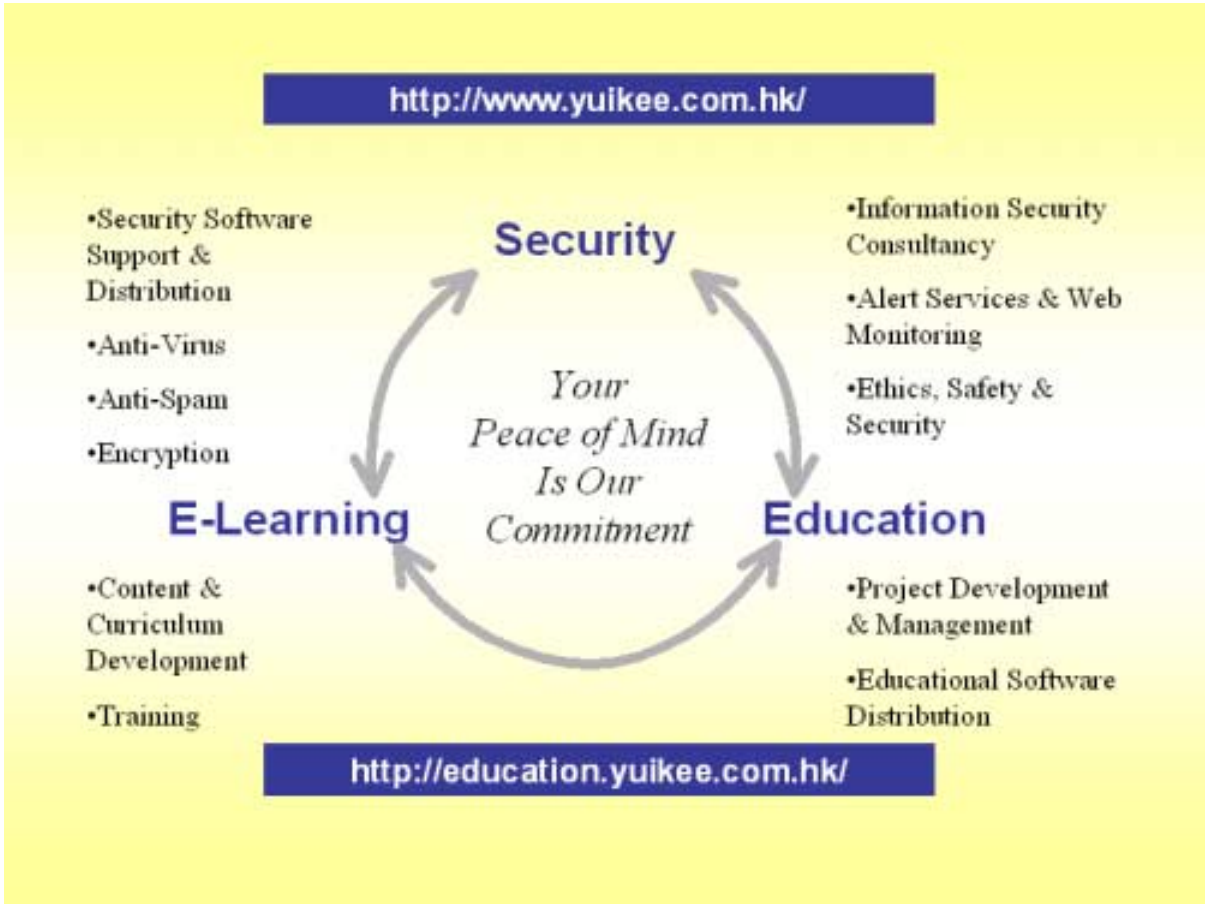
http://www.sophos.com/virusinfo/articles/spainarrest2.html

http://www.theregister.com/2005/01/27/tasin_arrest/

In Spanish: http://www.elmundo.es/navegante/2005/01/27/esociedad/1106832016.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/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/