Yui Kee Computing Ltd.

Newsletter

March 2007

Contents

First Bogus Website Conviction in HK

Chen Li-mee, 25 was given a six-month suspended jail sentence for five counts of obtaining access to a computer with dishonest intent and three of theft. She used forged emails to attempt to trick fifteen users of Netvigator (Hong Kong’s larges ISP) to visit a bogus website and reveal their account details, but none of the intended victims fell for the scheme. She sent the emails from her home, a coffee shop, the Hong Kong Polytechnic University, where she was a student, and the Office of the Telecommunications Authority, where she was a summer intern.

She also stole letters containing Netvigator account details from the home of a student she tutored, and used the account for multimedia entertainment services.

The Commercial Crime Bureau confirmed this is the first conviction for running a bogus website for a fraudulent scheme in Hong Kong.

EICAR Conference Cancelled

The European Institute of Computer Anti–Virus Research (EICAR) has announced that its 16th Conference, which was to be held from 5th to 8th May 2007 at the Radisson SAS Béke Hotel in Budapest, has been cancelled.

Rainer Fahs, Chairman of the EICAR board, has apologised, “EICAR deeply regrets this situation and apologises to the Conference Hotel, the EICAR members, our conference team, our sponsors and those who have submitted papers for presentation at the conference as well as to those who had planned to attend the conference.”

It is understood that the conference has fallen victim to a crime, and a police investigation is underway.

More information:

http://www.eicar.org/conference/

Malware Enters Dictionary

The word “malware” has entered the Oxford English Dictionary in the latest update on 15th March 2007. OED chief editor John Simpson commented, “Words are included in the dictionary on the basis of the documentary evidence that we have collected about them.”

Other words recognized include “undelete”, “wiki”, “Infobahn”, “Shaolin” and “Cantopop”.

More information:

http://www.theregister.com/2007/03/16/wiki_oed/

http://www.oed.com/help/updates/Prakrit-prim.html - oos

F-Secure calls on ICANN to enable safer online banking

ICANN (Internet Corporation for Assigned Names and Numbers), the organization responsible for the global coordination of the Internet's system of unique identifiers, should introduce a .safe domain name to be used by registered banks and other financial organizations, according to F-Secure.

According to APACS, the UK payments association, 17 million people now bank via the Internet in the UK and that figure is set to rise in the next few years (APACS - The way we pay bills report, February 2007). The trend is similar in other countries. But as the number of Internet bankers rise, so too does the amount of people committing fraud. Compared to the first six months of 2005, online banking fraud rose by 55 per cent in 2006 (APACS - Press Release - Latest figures show UK card fraud losses continue to decline in first six months of 2006, November 2006).

If ICANN introduced a .safe domain (or .sure or .bank), which could only be used by registered financial institutions, it would allow security providers to create better software to protect the public, according to F-Secure. It would be similar to other top level domain names such as .uk and .gov.

"While a .safe domain name won't prevent phishing attacks, it will help banks and security providers to keep their customers safe, said Mikko Hyppönen, Chief Research Officer at F-Secure. "Banks need to take on some of the responsibility for protecting their customers and using a secure domain name such as .safe will give customers the reassurance they need when banking online."

"It's true this will mean banks have to pay a premium to be able to use the domain name, but it will reduce the number of successful phishing sites that have been tricking many customers out of their hard earned cash," Hyppönen continued.

"Right now, customers have no good way of automatically being able to tell whether or not a bank website belongs to the bank. So a small bank or credit union phishing site is something that has to be researched. If .safe or .sure is locked down, then security companies would have a much better set of assumptions to start with when filtering email and web traffic. Security providers would then be able to build a better security product and users would feel safe online," said Hyppönen.

"ICANN has the power to create a safer online banking world, by introducing a top level domain name for banks and other reliable financial institutions. The idea was mooted some time ago, but with levels of online fraud as high as they are, now is the time to take action. .safe would give the millions of online customers the reassurance they need that banking via the Internet is safe," concluded Hyppönen.

More information:

http://www.f-secure.com/f-secure/pressroom/news/fs_news_20070329_1_eng.html

http://www.apacs.org.uk/media_centre/documents/TheWayWePayBills-26.02.07.pdf

http://www.apacs.org.uk/media_centre/press/06_07_11.html

OpenSSL is FIPS 140-2 Validated

The Open Source Software Institute (OSSI) has announced that OpenSSL has regained its FIPS 140-2 validation and is now available for download. The by the Computer Module Validation Program (CMVP), which normally lasts a few months, took an astounding five years to complete. The CMVP is a joint venture between the US National Institute of Standards and Technology (NIST) and the Canadian agency Communications Security Establishment (CSE).

OSSI technical project manager Steve Marquess commented, “With other software [tested by CMVP], all the proprietary information is treated as trade secrets and we can't comment on it. On the one hand, that gives someone an advantage to disparage our work. On the other hand, we've been scrutinized and tested in the open, so we have a much more solid validation than the others.”

More information:

http://www.linux.com/article.pl?sid=07/02/08/1935232

http://csrc.nist.gov/cryptval/

Security Professionals Ranked in “Most Influential” List

PC World has made its choices for the 50 “Most Influential” people on the Web. Bruce Schneier, the well–known cryptographer and commentator on security issues, is number 31 in the list. Mikko Hyppönen, F-Secure’s Director of antivirus research, is the highest anti–virus researcher at number 43.

But both these are beaten by Jon Lech Johansen at number 18, the Norwegian hacker who broke the encryption system used on DVD movies. Johansen went on to crack Apple's iTunes DRM (repeatedly).

Full Article:

http://www.pcworld.com/printable/article/id,129301/printable.html

Vista Keeps Ancient Security Flaw

Windows Vista, like earlier versions of Windows, has the “Hide extensions for known file types” option on by default. This “feature” has been widely exploited by malware authors who use double–extensions to trick incautious users into executing suspicious files.

The flaw originated when DOS was first designed, and eight–letter filenames were given a three–letter “extension” that could indicate what type of executable they were. Applications began defining their own extensions for their data files, and Windows used these to decide what action to take when the file was double–clicked. This oddity became dangerous when Windows 95 allowed long filenames (with more than one “.”), and also hid the extensions for known filetypes, to be “user friendly”. Apparently, Microsoft still has not noticed the contradiction of intentionally putting information about the file type into a file’s name, but then intentionally hiding that part of the name.

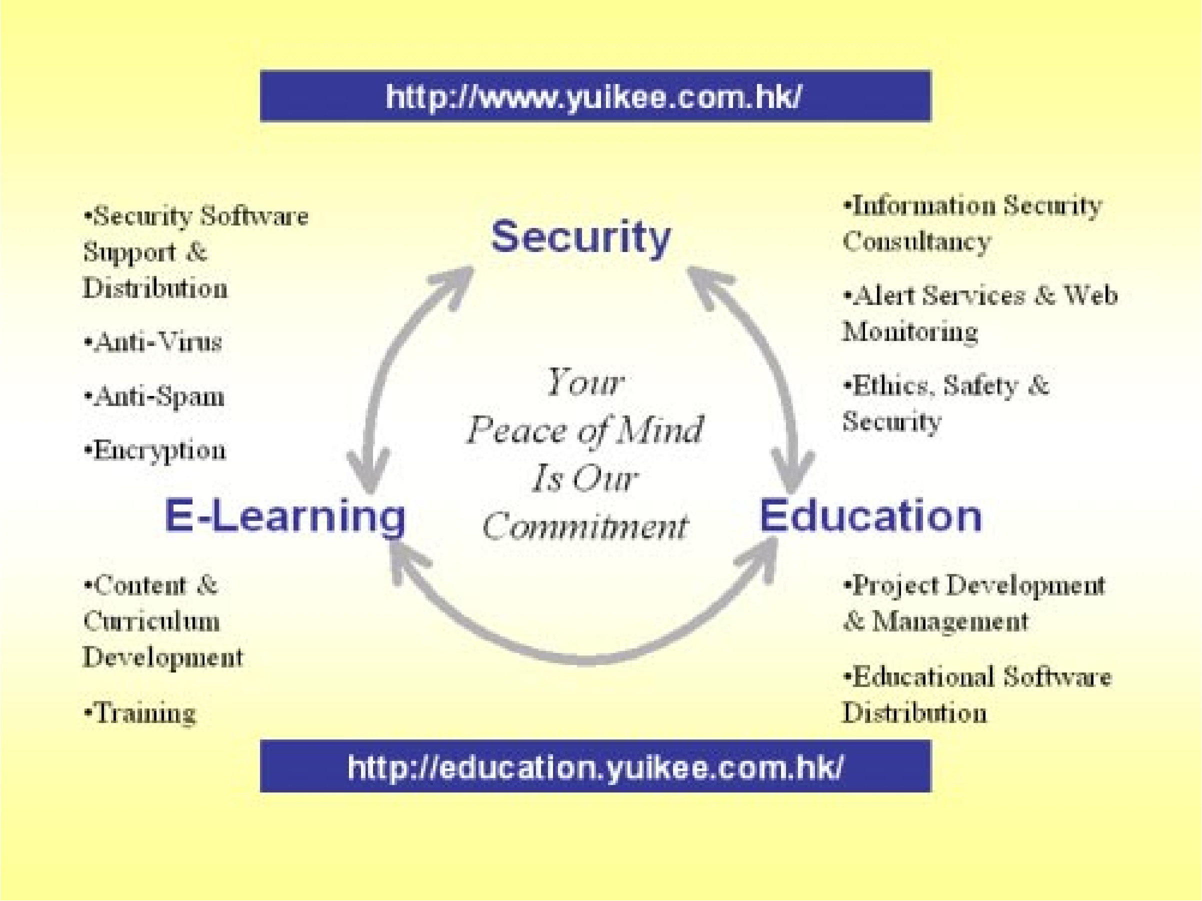
So, your new operating system contains a design “feature” from a quarter of a century ago, which became a dangerous flaw twelve years ago.

More:

http://www.f-secure.com/weblog/archives/archive-032007.html#00001148

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: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

E-Learning

Education

Your Peace of Mind Is Our Commitment

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

- Content & Curriculum Development
- Training

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/