Yui Kee Computing Ltd.

Newsletter

January 2010

Contents

Cybercrime Doubles in Hong Kong

<web-link for this article>

Statistics published by the South China Morning Post show technology-related crime is set to double in 2009. The Hong Kong Police had 1,378 cases for the first 11 months of 2009, compared with 791 for the whole of 2008. The head of the Commercial Crime Bureau's technology crime division, Superintendent Terence Yeung Chi-man, blamed a lack of public awareness of internet security, saying, "in many cases the victims' computers were compromised after they visited phishing websites, which then stole their e-mail accounts".

Illegal access to computers showed the biggest rise, from 46 to 410 cases in 2008 and 2009, respectively.

Roy Ko Wai-tak of HKCERT warned that criminals were now exploiting loopholes in social networking sites such as Facebook and MSN Messenger. He said, "It is not about anti-virus software or other protection, but the awareness of internet security. People should be very careful before clicking on any hyperlinks, even when they are sent by friends."

381 cases were related to online games, with theft of virtual possessions, such as in-game items and points, being common.

More Information

Technology Crime Statistics in Hong Kong

Gathering Confidential Data

<web-link for this article>

Vendors of hardware-encrypted USB memory sticks, including SanDisk, Kingston and Verbatim, have issued security advisories about the security of their devices. Apparently, although the drives are NIST-certified, and the data is encrypted with 256-bit AES, security researchers at SySS discovered the same character string was always sent to the drive after performing various crypto operations. By writing a tool for the active password entry program's RAM which sent the appropriate string to the drive the researchers gained immediate access to all the data on the drive without using the password.

Juergen Schmidt writing at The H criticised the different reactions of the vendors involved, Kingston recalling the devices, the others merely providing a software update. He also asked two very relevant questions, "how could USB Flash drives that exhibit such a serious security

hole be given one of the highest certificates for crypto devices?" and "Even more importantly, perhaps – what is the value of a certification that fails to detect such holes?"

Another question to consider is whether an unscrupulous vendor could use such a flaw for massive collection of confidential data. A possible scenario would be:

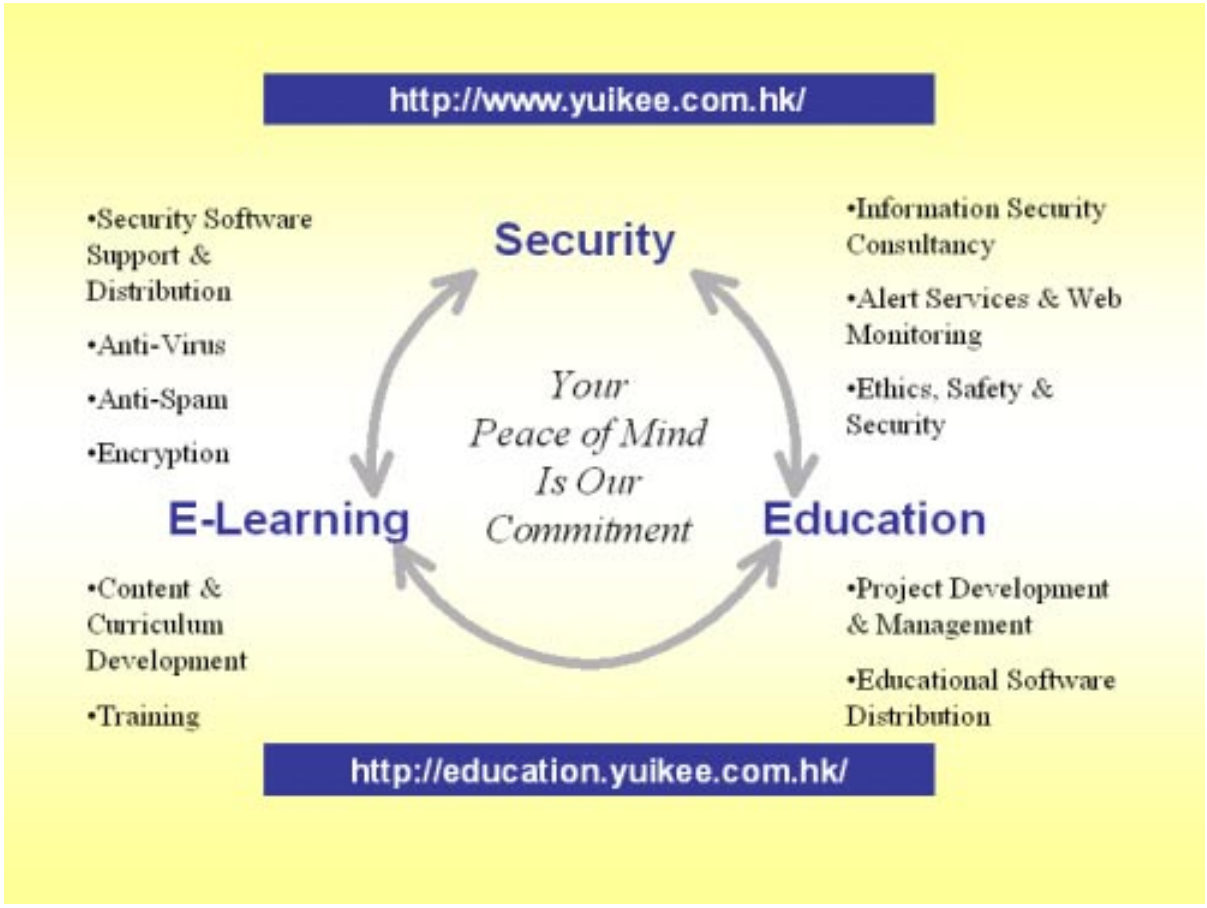
1. Design encrypted memory device with a security flaw
2. Sell device in large quantities
3. Wait for discovery of the security flaw, or "discover" it yourself
4. Issue a product recall
5. Enjoy reading confidential information on returned devices

After all, how many users of memory sticks know how to securely delete data on them?

More Information

Secure USB drives not so secure
Flash drive manufacturers warn: Hackers can decrypt 'secure' USB sticks
SanDisk Security Bulletin December 2009
Kingston's Secure USB Drive Information Page
Verbatim Important Security Update December 2009
NIST-certified USB Flash drives with hardware encryption cracked
SySS
the H: Security news and Open source developments

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
•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/