銳基電腦顧問有限公司

Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

June 2006

Contents

Why Phishing Works

An academic study has revealed alarming insights into how people are deceived by fraudulent websites. Almost a quarter of the participants were relying entirely on the page content to judge the legitimacy of the site. Only 9% checked the SSL certificate. Some users showed erroneous security knowledge and were swayed by professional–looking animations and favicons. The most successful phishing site in the study fooled over 90% of the participants.

More information:

http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

http://www.securityfocus.com/brief/176

http://www.theregister.co.uk/2006/06/07/why_phishing_works/

Patch Tuesday, Virus Wednesday, Whose Advantage?

Microsoft's "Patch Tuesday" this month released twelve security updates, eight of them critical. Exploits for the vulnerabilities appeared the very next day. However, this was not the end of the bad news for Microsoft this month – it was also revealed that "Windows Genuine Advantage" (WGA)reports back to Microsoft daily, raising security and privacy issues. Observers made comparisons between the definition of spyware and the actions of WGA, and found no difference. A new version of Windows Genuine Advantage incorrectly labeled legal software as pirated in some cases.

More information:

http://www.theregister.co.uk/2006/06/09/patches_for_june/

http://www.us-cert.gov/cas/techalerts/TA06-164A.html

http://www.microsoft.com/technet/security/bulletin/ms06-jun.mspx

http://www.theregister.co.uk/2006/06/14/ms_june_patch_tuesday/

http://www.theregister.com/2006/06/15/patch_tuesday_virus_wednesday/

http://www.theregister.co.uk/2006/06/30/microsoft_wga_snafu/

http://www.theregister.co.uk/2006/06/08/ms_wga_phones_home/

http://www.theregister.co.uk/2006/06/28/microsoft_wga_patched/

http://www.theregister.co.uk/2006/06/22/wga_remove/

http://www.theregister.co.uk/2006/06/16/spyware_lesson/

http://www.theregister.co.uk/2006/06/12/letters_wga_row/

http://support.microsoft.com/?kbid=905474

http://www.eweek.com/article2/0,1895,1979756,00.asp

http://arstechnica.com/journals/microsoft.ars/2005/7/26/814

http://www.microsoftmonitor.com/archives/003782.html

http://www.betanews.com/article/The_Truth_About_Windows_Genuine_Advantage/1116005058

http://en.wikipedia.org/wiki/Windows_Genuine_Advantage

http://www.microsoft.com/genuine/downloads/whyValidate.aspx

OFTA Tackles Automated Junk Calls?

The Office of the Telecommunications Authority (OFTA) has announced a voluntary Code of Practice on Handling Complaints about Inter-operator Unsolicited Promotional Calls Generated by Machines. Under the Code, recipient of junk calls are required to provide their service provider with:

1. their full name;
2. the affected telephone number(s);
3. the date and time at which the junk call was received;
4. the content of the junk call, such as the product that the junk call advertised and the characteristics of the product;
5. the telephone number of the junk call sender as displayed on the phone (if any);
6. the consent to disclose the recipient's full name for the follow-up action on the complaint.

If two or more complaints are received within 5 days, and they are substantiated, the junk caller's phone service may be suspended or terminated.

Unlike the sender's caller ID, the details of the content of the junk call are not described as an optional requirement, and the Code makes clear that an investigation will only occur if the information is complete. This causes difficulties for people who receive junk calls in a language they do not understand. When asked, "most of the junk calls I receive are in a language I do not understand and cannot speak. How can I report the content of a recorded message that I did not understand?", OFTA's Webmaster responded in email:

> "We understand that some customers may have problem in providing some information to operators such as the content because of the language problem or the caller's number because the number is hidden etc. However, it is still possible for operators to conduct the required investigation based on the other available information from customers such as the time/date of receiving the calls. We would alert operators about your concerns and request them to accommodate customers' complaints as far as they can."

OFTA did not say that it would amend the Code. An earlier voluntary code in a related area, the "Anti-SPAM - Code of Practice" that OFTA produced with the HKISPA has been ineffective.

More information:

http://www.ofta.gov.hk/en/press_rel/2006/Jun_2006_r1.html

http://www.ofta.gov.hk/en/consumer_interest/Unsolicited/unsolicited_2006060501.pdf

http://www.hkispa.org.hk/antispam/cop.html

http://www.hkispa.org.hk/antispam/

Trojan Gang Arrests

UK and Finnish Police have arrested three alleged members of a group called "m00p" that is suspected to have sent Trojans via spam email. Computers and servers were also seized at residential addresses in Finland, Suffolk in England, and Scotland. The Metropolitan Police stated, "They have been primarily targeting UK businesses since at least 2005, and during this time thousands of computers are known to have been infected across the globe."

"Today's arrests will send a clear worldwide signal to the authors of malicious software that national borders will not limit the ability and commitment of law enforcement authorities to clamp down on this criminal activity", said Detective Constable Bob Burls, of the Metropolitan Police Computer Crime Unit, triumphantly. However, Graham Cluley of Sophos took a more measured view, "It's great to see one less virus writing gang, but the sad fact is, however, that this is probably just the tip of the iceberg."

The m00p gang have been linked with many viruses and Trojans. One of them, the Stinx trojan (also known as Breplibot.C) utilised the Dony DRM vulnerability to hide its processes. There has been no news of Sony executives being arrested for their part in enabling this gang's activities.

More Information:

http://www.theregister.com/2006/06/27/spam_trojan_arrests/

http://www.sophos.com/pressoffice/news/articles/2006/06/m00p.html

http://www.f-secure.com/v-descs/breplibot.shtml

http://www.f-secure.com/v-descs/breplibot_c.shtml

http://www.f-secure.com/news/items/news_2006020101.shtml

http://www.f-secure.com/weblog/archives/archive-062006.html#00000902

http://www.sophos.com/virusinfo/analyses/w32dogbota.html

http://www.sophos.com/virusinfo/analyses/trojhackarmyc.html

http://www.sophos.com/virusinfo/analyses/trojsantabota.html

http://www.sophos.com/virusinfo/analyses/trojshuckbota.html

http://www.sophos.com/virusinfo/analyses/w32rbotbf.html

http://www.sophos.com/virusinfo/analyses/w32tibicka.html

F-Secure Data Security Wrap–Up

The F-Secure research lab have released their summary of the significant information security events in the first half of this year. In the video, Mikko Hypponen's final assessment is, "Things seem to be getting better, but, in fact, they're getting worse."

Full summary:

http://www.f-secure.com/2006/1/

http://www.f-secure.com/2006/1/f-secure_2006_1st_half.wmv

Hong Kong Monetary Authority Fights Fraud

In June 2006, HKMA has warned the public about three allegedly fraudulent websites. They are:

- www*[dot]*icbcasiachina*[dot]*cn

  Fraudulent. Looks similar to the official website of Industrial and Commercial Bank of China (Asia) Limited (“ICBC (Asia)”). ICBC (Asia) has clarified that it has no connection with this website.

- www*[dot]*hkcb*[dot]*net

  Suspected fraudulent. Claims to represent the “Hong Kong City Bank”, and offers various banking services to members of the public in Hong Kong. The public should be aware that the alleged “Hong Kong City Bank” is not authorised under the Banking Ordinance to operate a banking business or the business of taking deposits in Hong Kong, nor does it have the approval to establish a local representative office.

- www*[dot]*stbhk*[dot]*com

  Fraudulent. Looks similar to the official website of Standard Chartered Bank (Hong Kong) Limited. Standard Chartered Bank (Hong Kong) Limited has clarified that it has no connection with the fraudulent website.

All three cases have been referred or reported to the Hong Kong Police Force for further investigation.

Given the global nature of the Internet, members of the public are reminded to verify the status of any organisation making use of the Internet to solicit deposits from the public. A list of authorised institutions is available on the HKMA's website (www.hkma.gov.hk). Members of the public may also check the status of any entity in Hong Kong which solicits deposits from the public with the HKMA by calling its public enquiry hotline 2878 8222.

References:

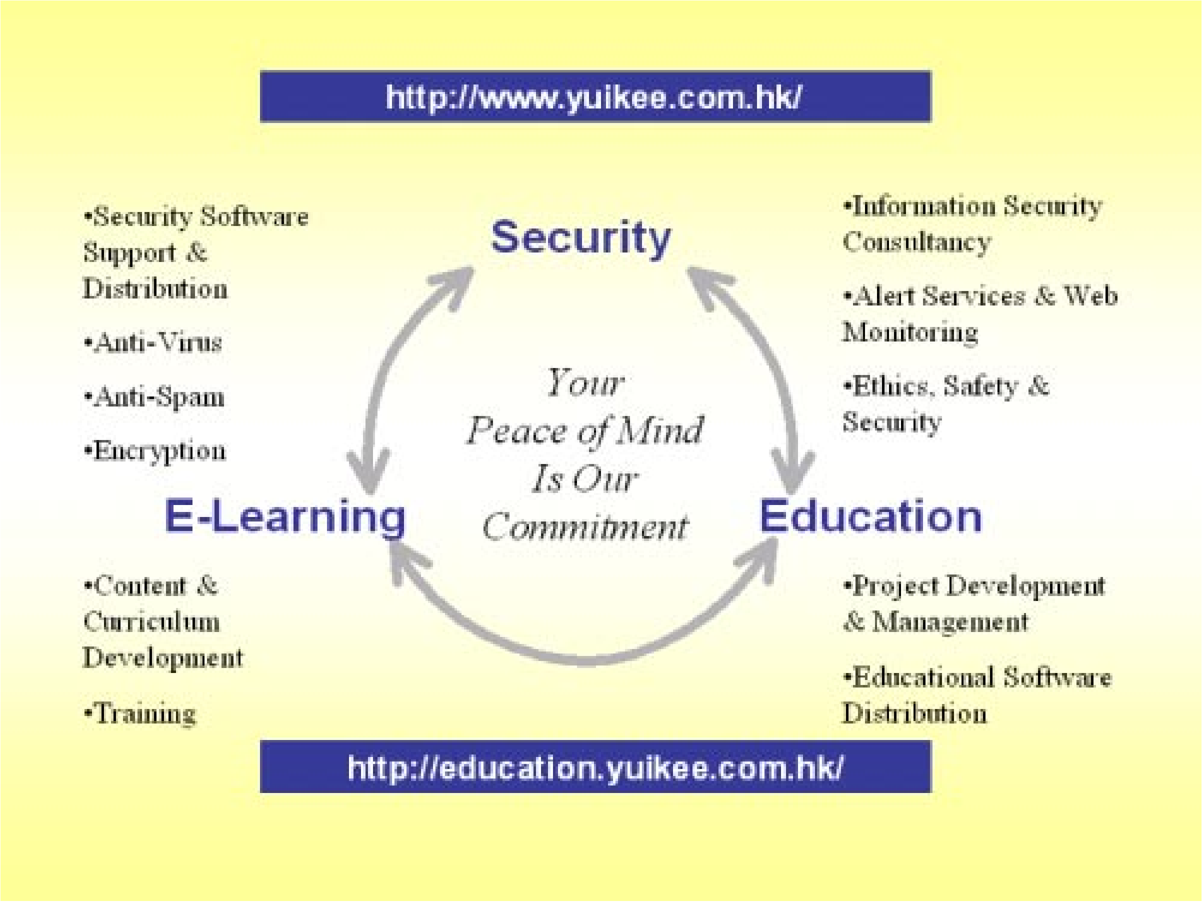
http://www.info.gov.hk/hkma/eng/press/2006/20060606e6.htm

http://www.info.gov.hk/hkma/eng/press/2006/20060616e3.htm

http://www.info.gov.hk/hkma/eng/press/2006/20060619e4.htm

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

Security

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

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

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