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

Yui Kee Computing Ltd.

Newsletter

October 2013

Contents

Fraudulent Hong Leong Bank Website Suspended

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued an alert about a fraudulent website with the domain name "http://www.hk.honglb.com". They reported that the website looks similar to the official website of Hong Leong Bank Berhad. The site has been suspended by the Lithuanian hosting company that was hosting it.

The Hong Kong Police are investigating. Anyone who has used the website should contact HLB at 22838930 and the Hong Kong Police Force at 28605012.

More Information

Fraudulent website: http://www.hk.honglb.com
Alert issued on bogus website

Hong Kong Tax Department Warns of Fake Tax Emails

<web-link for this article>

The Hong Kong Inland Revenue Department (IRD) has issued an alert about fraudulent emails with the sender's address domain of @ird.gov.hk. Files with names like "Form_ird.gov.hk.zip", "File_2183065.zip", or "File_4730881.zip" are attached to the messages. The attachments are infected with computer viruses. The IRD has no connection with the messages, and the Police are investigating.

Allan Dyer, Yui Kee's Chief Consultant, commented, "At one time, malicious software was most often found in emails promising celebrity photos. Nowadays, criminals have broadened their scope; many messages target business users by mentioning quotations, purchase orders or, as in this case, government departments. Defence in depth is your friend here. Your email gateway can recognise many of these as suspicious, your endpoint anti-virus might detect the infection, but ultimately, the last line of defence is you, the user, recognising the message is not what it seems. Think before clicking."

More Information

IRD issues alert on fraudulent emails

HKMA Warns of fake Hang Seng Bank website

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about a fraudulent website with the domain name "http://ebank-hangseng.com" that looks similar to the official website of Hang Seng Bank, Limited (HSB).

Hang Send Bank has no connection with the website, and the Police are investigating. Anyone who has used the website, entering personal information or conducting financial transactions, should contact the bank at 2822 0228 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent website: http://ebank-hangseng.com
Alert issued on fake website

October Honeypot Report

<web-link for this article>

This is the twenty-first monthly report from West Coast Labs's honeypot in Hong Kong, providing some indication of the type and level of malware threat in Hong Kong, but it is only based on a single honeypot, so the conclusions should be treated with caution. The number of attacks has dropped.

Average Time To Infect: 45 hours

The average time to infect is an indication of how long it would be before a vulnerable computer connected to the internet in Hong Kong became infected.

Summary

- □ Total number of attacks : 16
- □ 11 are brand new to this honeypot.

Source of Attacks

The following breaks down where these attacks have come from by use of IP geolocation.

5	United States
3	Pakistan
2	South Korea
1	Brazil
1	China
1	Denmark
1	India
1	Japan
1	Switzerland

Malware

Checksum (md5)	This month	Previous count	Detection*
3875b6257d4d21d51ec13247ee4c1cdb	2	53	Y W32Rbot!I2663.exe, Backdoor.Win32.Rbot.bni, W32/Malware!44f4 W32/Sdbot.AEFV,
0f51974913a4f5be110ab1069c93e13f	2	0 *** NEW	Y Backdoor.Win32.Rbot.adqd ,w32/virut.ag ,
d41d8cd98f00b204e9800998ecf8427e	1	14	N ,,, invalid file download interrupted.
0e2f2731b85c5371466ed04aba18127b	1	0 *** NEW	Y UDS:DangerousObject.Multi.Generic, w32/ceg.a ,
b0ad1e3989d4b080d79014789809e97f	1	0 *** NEW	Y net-worm.win32.allaple.e, w32/rahack.a.gen!eldorado ,
c8a08205dacb271dddebf9ed0e9f775a	1	0 *** NEW	Y net-worm.win32.allaple.b, w32/rahack.a.gen!eldorado ,
eb5acf217ed919dfcd7bb5a8d90fe280	1	0 *** NEW	Y net-worm.win32.allaple.e, w32/emailworm.hqk ,
50631acf7cd8f79cd8f9b62feb5ea7c5	1	0 *** NEW	Y Backdoor.Win32.Rbot.adqd , w32/virut.7116 ,
57e6d8bed32bfa4a775045fe8363ddec	1	0 *** NEW	Y net-worm.win32.allaple.b, w32/allaple.c ,
74473505ef968e2f8cd764d9af12adb2	1	X	Y Net-Worm.Win32.Allaple.e ,W32/Allaple.H ,
a650c67e14cfb27879999036741478d5	1	0 *** NEW	Y backdoor.win32.ircbot.jwy , w32/backdoor2.dstk ,
094e157abbf4858fa343a41021c2de1d	1	0 *** NEW	Y Net-Worm.Win32.Allaple.e , w32/emailworm.hqk ,
117b19c5fc5fc6fcee86d0d9901aa5c9	1	0 *** NEW	N ,,, new file, no details available
37e6f78986dd46c92d06195334c32b24	1	0 *** NEW	Y Backdoor.Win32.Rbot.adqd ,w32/virut.ag ,

Notes:

The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

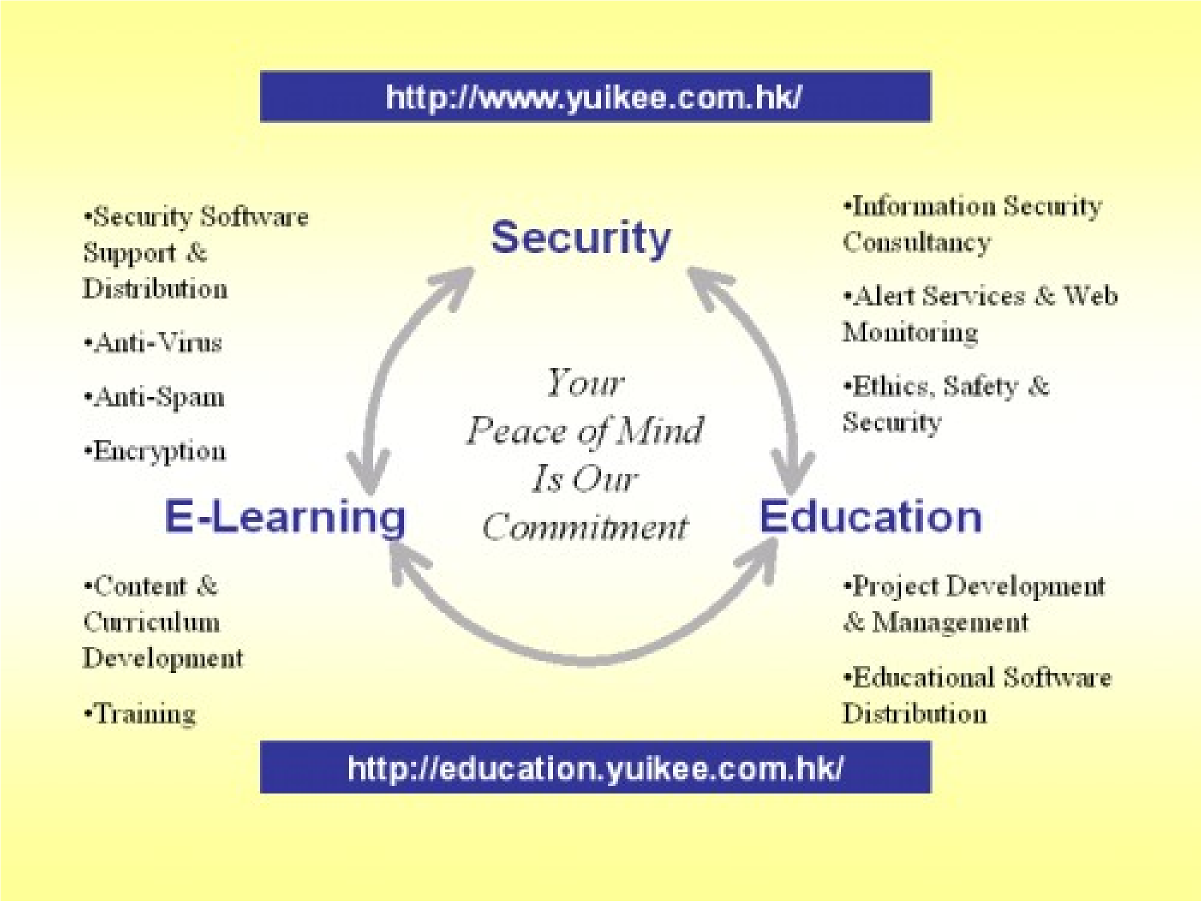
Where an X is shown under Previous, the file has been seen before in this honeypot but the relevant logs are not available

More Information

West Coast Labs
January Hong Kong Honeypot Report

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

- 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

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

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