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

Yui Kee Computing Ltd.

Newsletter

February 2013

Contents

HKMA Warns of Fraudulent ANZ Bank Email

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued an alert concerning an e-mail purporting to be sent from Australia and New Zealand Banking Group Limited (ANZ). The email entices the bank's customers to follow an embedded link to a fake online banking login page. ANZ does not have the policy of sending e-mails asking its customers to provide their passwords or verify their account information online. If you have provided personal information or conducted financial transactions on the fake website contact ANZ at 2176 8888 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The fraudulent login page was set up on the domain www.vyhlidkaskalsko.cz, which appears to be the website of the Lookout Restaurant - Skalsko in the Czech Republic, north-east of Prague. The login page no longer exists.

An HKMA spokesperson advised, “Members of the public are reminded not to access their Internet banking accounts through hyperlinks embedded in e-mails, Internet search engines or suspicious pop-up windows. Instead, they should access their Internet banking accounts by typing the website addresses at the address bar of the browser, or by bookmarking the genuine website and using that for access. If in doubt, they should contact their banks.”

Yui Kee's Chief Consultant Allan Dyer commented, "Unfortunately, many innocent businesses are facilitating crime by not securing their websites. Once a criminal has access, they can use the site for fake bank login pages, as seen in this case, drive-by infection, search engine stuffing or many other nefarious activities. Businesses should make sure their hosting provider values security, is keeping their content management system up-to-date, and they are using strong passwords and access methods."

More Information

Alert issued on email scam
Fraudulent email purporting to be related to Australia and New Zealand Banking Group Limited

Insurance Commissioner Warns of Dodgy Insurance Website

<web-link for this article>

Hong Kong's Office of the Commissioner of Insurance (OCI) has alerted the public about "China Eastern Pacific Insurance Shares Limited", which is not an authorised insurance company. The company was operating a website, www.eastpc.com.hk where it claimed to be authorised under the Insurance Companies Ordinance. The case is being investigated by the Police. The website is currently unavailable, but anyone who has done business with the company or provided personal information should contact the Police on 2731 7278 or the OCI at 2867 2565.

The full list of authorised insurers in Hong Kong is available on the OCI website.

The eastpc.com.hk domain registration shows that the address of China Eastern Pacific Insurance Shares Limited is in Shanghai. The contact email address is also used for the domain wealthroll.com.hk, registered to "Zhongjin Financial the Global Fund Share Co., Ltd" that shares the same address in Shanghai. The website www.wealthroll.com.hk is currently operational, and the company appears to be providing online trading and other financial services. The site appears to be negligent about their customers' security: the login page is not protected by TLS, and it uses the customer's ID card or passport. Both eastpc.com.hk and wealthroll.com.hk were registered on 31-05-2012 for one year.

More Information

Alert issued on bogus website
Office of the Commissioner of Insurance February 2013 Press Releases
List of Authorized Insurers

February Hong Kong Honeypot Report

<web-link for this article>

This is the fourteenth 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 was quite low.

Average Time To Infect: 39 hours 9 minutes

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 : 19
- □ 4 are brand new to this honeypot.

Source of Attacks

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

8	Japan
3	United_States
3	Canada
1	Ecuador
1	Sweden

1	Germany
1	Cameroon
1	Taiwan

Malware

Checksum (md5)	This month	Previous count	Detection*
14a09a48ad23fe0ea5a180bee8cb750a	2	12	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
1d419d615dbe5a238bbaa569b3829a23	2	10	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
df51e3310ef609e908a6b487a28ac068	1	14	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.rgk , ,)
15965bb88165d1eb06851d8f076130ba	1	20	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
673fdc1e6cc862c42b82d4091249c4b9	1	0 ***NEW	Y (w32/virut.7205 , Net-Worm.Win32.Allaple.e Virus.Win32.Virut.bl , ,)
786ab616239814616642ba4438df78a9	1	0 ***NEW	N (, , ,) old file, limited detection
98eb0fdadf8a403c013a8b1882ec986d	1	1	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.kez , ,)
681295872c5ce4f25617943c4e7a83f9	1	0 ***NEW	N (, , ,) old file, limited detection
27e0cb71d5229bf0290590dc9eef70ba	1	2	Y (w32/allaple.h , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
4d56562a6019c05c592b9681e9ca2737	1	1	Y (w32/trojan-sml-sdcw!eldorado , Trojan.Win32.Genome.ahpxd Net-Worm.Win32.Kido.ih UDS:DangerousObject.Multi.Generic , ,)
b82698a30e07fc71349f06750cae2664	1	7	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
b43ad71209c5100b9ed71edb10041514	2	10	N (, , ,) old file, limited detection
1d53fb866c27a421f7557e3cda0592ac	2	22	N (, , ,) script
d8f3cc60bf226f6a5745ed9fdef2d287	1	0 ***NEW	Y (, Backdoor.Win32.Rbot.adqd , ,)
0da155b04f16dafafffbb1a485b3d0e1	1	1	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)

Note:

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

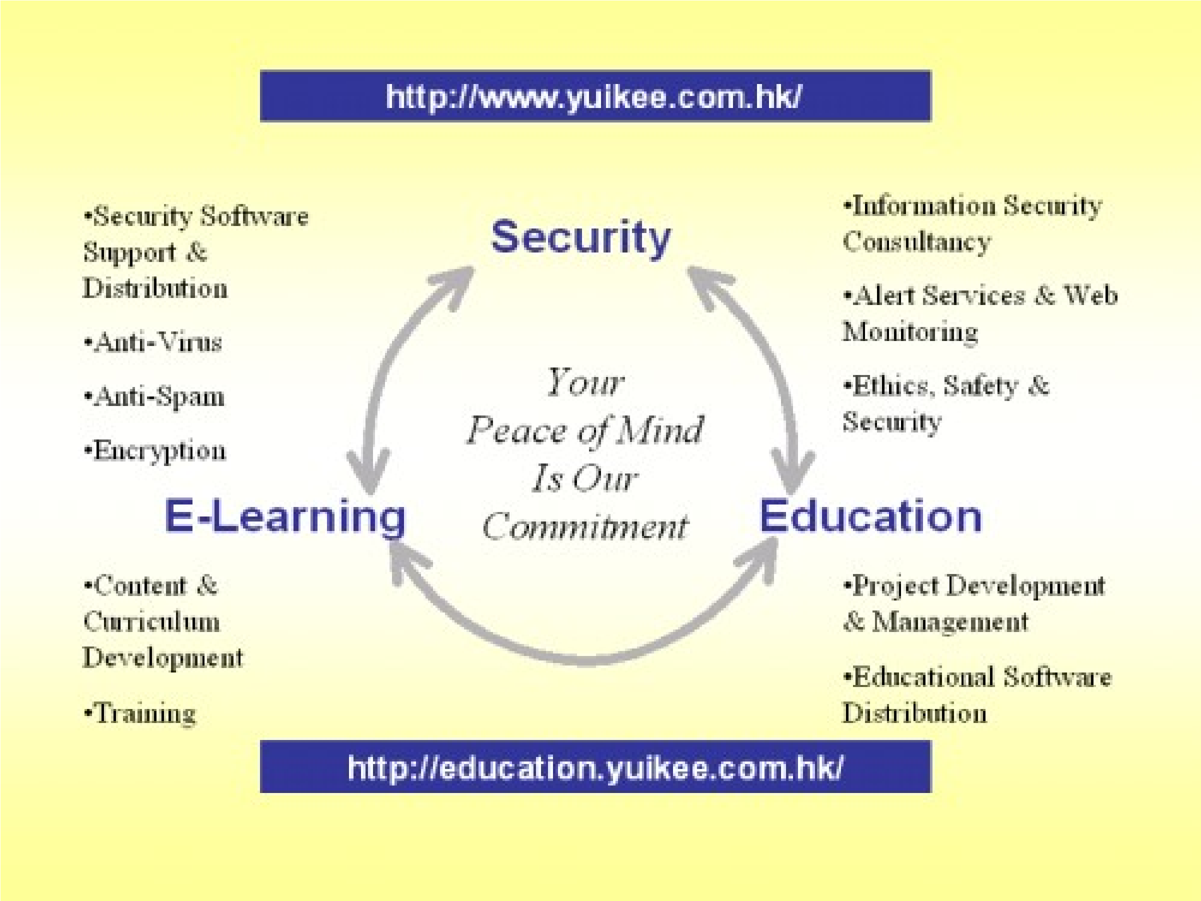
More Information

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/

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/