Yui Kee Computing Ltd.

Newsletter

July 2013

Contents

June Hong Kong honeypot Report

<web-link for this article>

First, an apology for the late publication of this report. This is the eighteenth 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 remains at a low level.

Average Time To Infect: 57 hours 14 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 : 13
- 7 are brand new to this honeypot.

Source of Attacks

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

2	United_States
2	China
2	India
1	Latvia
1	Thailand
1	France
1	Brazil
1	Sri_Lanka

1	Pakistan
1	Taiwan

Malware

Checksum (md5)	This month	Previous count	Detection*
052494f76e3a1f7b998c56e07062f535	2	2	Y (w32/genbl.052494f7!o lympus , Trojan-Spy.Win32.Zbot.lrjw , ,)
d827af7f090a488019622c87fcaa3dd3	2	0 ***NEW	Y (w32/hll-sysdlrsharer!eldorado , Trojan-Downloader.Win32.Agent.drun , ,)
e6d5b370ecd87702e43aa2498e0f72d0	1	0 ***NEW	N (, , ,) no detection
feb643c489c048083554aedac50126a9	1	1	Y (w32/virut.7116 , Bac kdoor.Win32.Rbot.adqd , ,)
c4af6e846c046ae87f4be59685405f49	1	0 ***NEW	Y (w32/trojan.mex , Backdoor.Win32.Rbot.bni , ,)
a276921e5dc3c0ebfc9e5d45c9be7f35	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
3875b6257d4d21d51ec13247ee4c1cdb	1	47	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
49cccd30a564410d1f9bbce89fa15890	1	3	Y (W32/Sdbot.AEFV , Bac kdoor.Win32.Rbot.adqd Backdoor.Win32.Rbot.bni , ,)
85e2ab71e6b2729bd83d6f533d8bf781	1	0 ***NEW	N (, , ,) script
879008eb69a270d41611b5fbff7acd85	1	0 ***NEW	Y (w32/emailworm.hqk , Net-Worm.Win32.Allaple.e , ,)
1b7379ba141c428b8a33153756dab1e6	1	0 ***NEW	Y (w32/allaple.d , Net-Worm.Win32.Allaple.b , ,)

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

HKMA Warns of Fake China CITIC Bank Email and Website

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned the public about an e-mail purporting to be sent from China CITIC Bank International Limited (CNCBI). The e-mail asks customers to go to a fraudulent website

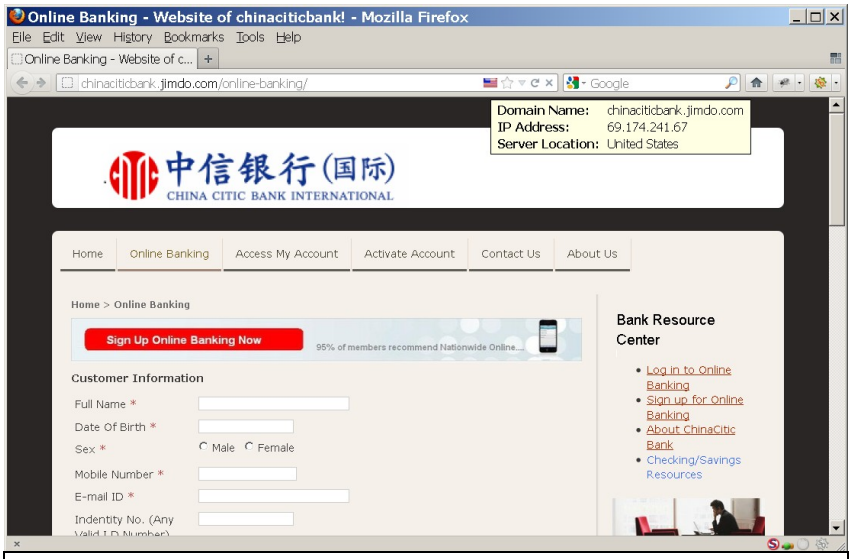

Figure 1 Fake bank website, showing geolocation report

(http://chinaciticbank.jimdo.com/online-banking/) and verify their account information by entering their user name and password. The fraudulent website, which was still active when this article was written, looks similar to the bank's logon webpage. CNCBI has clarified that it has not sent these e-mails to its customers and has no connection with the fraudulent website and CNCBI does not have the policy of sending e-mails asking its customers to provide their passwords or verify their account information online.

The Hong Kong Police are investigating the fraud. Anyone who has provided personal information to the website, or has conducted any financial transactions through it should contact CNCBI at 2287 6767 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The HKMA 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".

More Information

Fraudulent email purporting to be related to China CITIC Bank International Limited
Alert issued on bogus email

Fake HKMA Email Warning

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about fraudulent emails purporting to be from the email accounts hkma_invoice@hkma.gov.hk and invoice@hkma.gov.hk. The HKMA says it has no connection with the fraudulent emails and the Police are investigating. Anyone who has received the email should contact any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

As a central banking institution, the HKMA does not provide any form of banking services to individuals or companies or serve as a representative of any financial institutions. The HKMA says that it does not initiate emails and telephone calls requesting individuals to disclose or confirm their personal or financial information.

More Information

Fraudulent emails purporting to be issued by the HKMA
Alert issued on bogus emails

HKMA warns of fake Wing Hang Bank website

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned that the website "www.whgbkhk.com" is fraudulent. The website looks similar to the official website of Wing Hang Bank, Limited and the bank has clarified that it has no connection with the fraudulent website. The website was unavailable at the time of writing.

The Hong Kong Police Force are investigating, anyone who has provided personal information to the website or has conducted any financial transactions through it should contact Win Hang Bank at 3199 9188 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent website: www.whgbkhk.com
Alert issued on bogus website

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/