Yui Kee Computing Ltd.

Newsletter

May 2013

Contents

HKMA Warns of Fraudulent China Construction Bank Email

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) warns that an e-mail purporting to be sent from China Construction Bank (Asia) Corporation Limited (CCBA) is fraudulent. The e-mail contains a link to a fraudulent website (http://users9.jabry.com/onlinesafewebhk/ccb/) that requests user's internet banking user name and password. The fraudulent website looks similar to the bank's logon page. CCBA did not sent these e-mails to its customers and it has no connection with the fraudulent website. The fraudulent webpage is no longer available.

The Hong Kong Police are investigating, anyone who has provided personal information to the website, or has conducted any financial transactions through the website should contact CCBA at 2779 5533 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

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".

More Information

Fraudulent email purporting to be related to China Construction Bank (Asia) Corporation Limited
Alert issued on bogus email

OFCA Confirms Short Message Do-Not-Call Register Applies to WhatsApp

<web-link for this article>

Hong Kong's Office of the Communications Authority (OFCA) is responsible for administering and enforcing the Unsolicited Electronic Messages Ordinance (UEMO) and has established three Do-Not-Call registers. The registers allow a user to opt out from receiving commercial electronic messages, by voice, fax or short message, at a telephone / fax number from all senders.

Recently, the WhatsApp smartphone application has become popular for sending and receiving text messages. The app did not exist when the UEMO became law, or when OFCA established the Do-Not-Call registers, and descriptions of the registers on OFCA's website specifically mention SMS and MMS messages. The UEMO itself was intended to be technology-neutral, but subsidiary rules and guidelines address technology-specific differences.

On the 5th May, an information security consultant asked OFCA to clarify whether the do-not-call register relating to "short messages" also applies to WhatsApp etc. In an email reply, OFCA responded,

The Unsolicited Electronic Messages Ordinance ("UEMO") regulates the sending of commercial electronic messages ("CEMs") that has a Hong Kong link over a public telecommunications service to an electronic address, such as pre-recorded voice messages, SMS messages (including messages sent through mobile messaging applications like WhatsApp), faxes and emails. A message will be considered as a "commercial" message if it aims at advertising or promoting services or products, etc. A copy of the UEMO can be found in http://www.gld.gov.hk/egazette/pdf/20071122/es1200711229.pdf.

Under the UEMO, three Do-not-call ("DNC") Registers are established covering fax ("the Fax Register"), short messages ("the Short Message Register") and pre-recorded telephone messages ("the Pre-recorded Register"). Section 11 of the UEMO stipulates that sender must not send CEMs to electronic addresses registered in the DNC registers from the 10th working day starting from the registration date, unless prior consents from the registered users of the electronic addresses have been given. By registering the number onto the DNC Registers, the user in effect has opted for not receiving further CEMs of that category at the registered number from all senders except those to whom consent has been given.

OFCA also gave advice on registering a number on the DNC registers and reporting a contravention of the UEMO.

Yui Kee Chief Consultant Allan Dyer commented, "New messaging services generally have a short 'honeymoon' period when they are fast and useful, then they gradually fill up with unwanted marketing messages. OFCA's decision to take a broad definition of 'short message' gives WhatsApp users a critical opportunity to fight back against degradation of the service.".

More Information

UEMO [PDF]
Do-not-call Registers
How to report a suspected contravention of the UEMO?

HKMA Warns of Fraudulent Industrial and Commercial Bank Email

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) warns that an e-mail purporting to be sent from Industrial and Commercial Bank of China (Asia) Limited ("ICBC(Asia)") is fraudulent. The e-mail asks for confirmation on remittance related-matters ("Remittance Confirmation") and may have attached files. ICBC(Asia) did not sent these e-mails to its customers.

The Hong Kong Police are investigating and anyone who has received a similar suspicious message should contact ICBC(Asia) at 2189 5588 as soon as possible.

More Information

Fraudulent email purporting to be related to Industrial and Commercial Bank of China (Asia) Limited
Alert issued on bogus email

May Hong Kong honeypot Report

<web-link for this article>

This is the seventeenth 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: 51 hours 26 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 : 14
- 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.

3	Taiwan
3	Japan
2	Vietnam
1	Spain
1	China
1	Luxembourg
1	Germany
1	Bulgaria
1	Canada

Malware

Checksum (md5)	This month	Previous count	Detection*
022aeb126d2d80e683f7f2a3ee920874	1	0 ***NEW	Y (w32/agent.ix.gen!eldorado w32/genbl.022aeb12!olympus , Trojan-Spy.Win32.Agent.bmxb , ,)
8454eb77939c3f3d8c2b61dc6d6e5e19	1	0 ***NEW	Y (w32/allaple.c , Net-Worm.Win32.Allaple.b , ,)
954919ad5661e1b44803092360ac5d82	1	2	Y (W32/Trojan.MEX , Backdoor.Win32.Rbot.bni Virus.Win32.Virut.n , ,)

f9dc3945bdd7406bd8db06a47963ec14	2	27	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
c1989130056c32fa305e3de57f6f40f1	1	1	Y (W32/Trojan.MEX , Backdoor.Win32.Rbot.bni Virus.Win32.Virut.n , ,)
1f8a826b2ae94daa78f6542ad4ef173b	1	6	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.phv Backdoor.Win32.Rbot.ion , ,)
94109e9b3f2b045350db9a5cb592b178	1	14	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
f36fc8d2df690530b2032a4bad5ac285	1	0 ***NEW	N (, , ,) new file
14a09a48ad23fe0ea5a180bee8cb750a	1	18	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
bb39f29fad85db12d9cf7195da0e1bfe	1	8	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Net-Worm.Win32.Kolabc.eia , ,)
052494f76e3a1f7b998c56e07062f535	2	0 ***NEW	Y (w32/genbl.052494f7!olympus , Trojan-Spy.Win32.Zbot.lrjw , ,)
3875b6257d4d21d51ec13247ee4c1cdb	1	46	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)

Note:

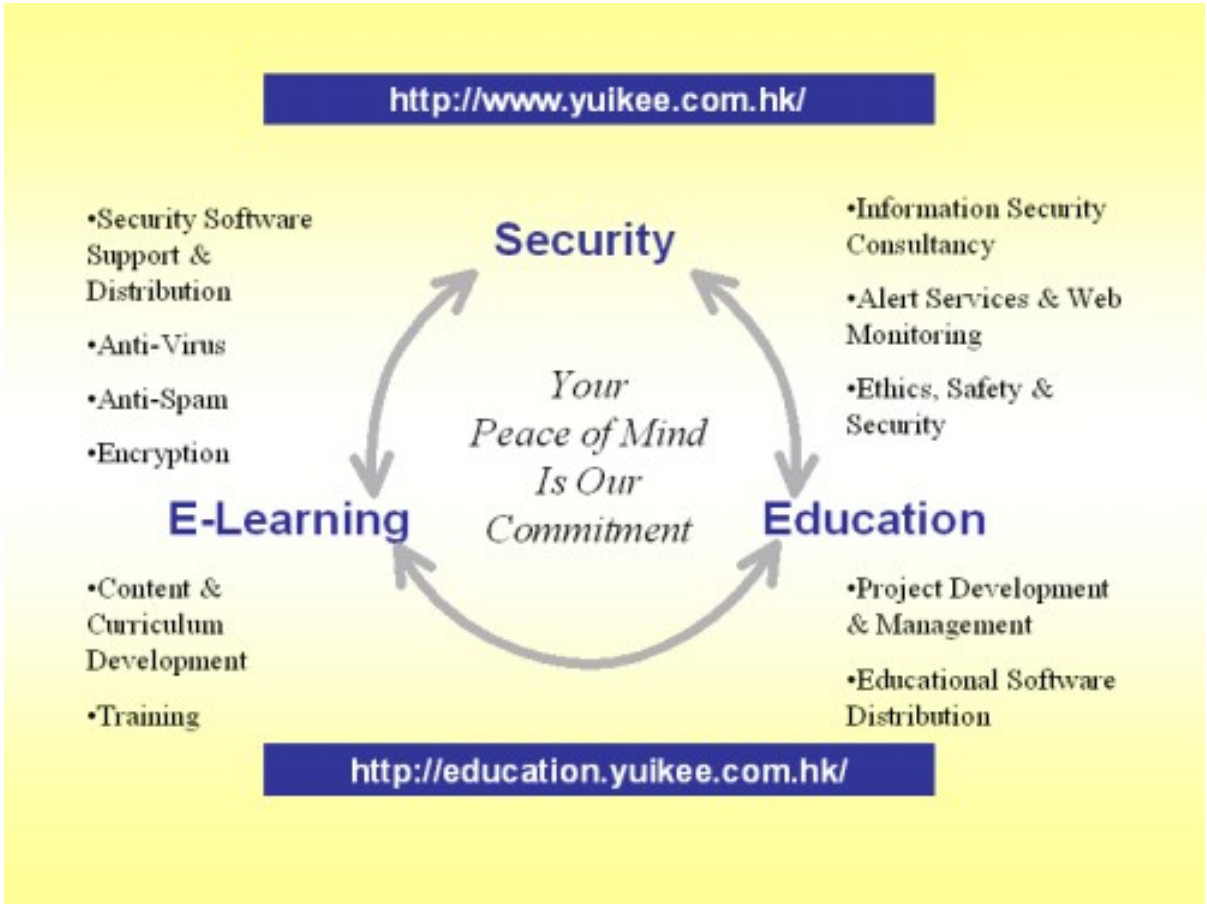
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

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/


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/