Yui Kee Computing Ltd.

Newsletter

April 2013

Contents

HKMA Warns of Fraudulent Standard Chartered Email

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned the public about an e-mail purporting to be sent from Standard Chartered Bank (Hong Kong) Limited (SCBHK). The e-mail links to a fraudulent website that redirects to another domain where users are asked to enter their SCBHK Internet banking username and password.

SCBHK has said that it has not sent these e-mails to its customers, it has no connection with the fraudulent website and it does not have a policy of sending e-mails asking its customers to provide their passwords or verify their account information online.

At the time of writing, the redirection domain olecram.name has been disabled, and the destination webpage has been replaced with an account suspension notice.

The case has been reported to the Police. Anyone who has entered personal information or conducted transactions on the fraudulent website should contact SCBHK at 2886 8868 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 Standard Chartered Bank (Hong Kong) Limited
Alert issued on bogus email

OFCA Clarifies Unsolicited Electronic Messaging Rules

<web-link for this article>

In a response to Yui Kee's Chief Consultant Allan Dyer's questions, reported in last month's newsletter, the Office of the Telecommunications Authority has clarified the meaning of sender, writing:

> We note that you may like to know more about the meaning of "send" under the Unsolicited Electronic Messages Ordinance (UEMO), Section 4 of the UEMO will be of relevance. Section 4(1) of the UEMO stipulates that "send" includes cause to be sent and attempt to send. Section 4(2) stipulates that if an individual authorizes the sending of a commercial electronic message ("CEM") and he does so on behalf of an organization, then the organization shall be treated as authorizing the sending of the message; while the individual shall be treated as not authorizing the sending of the message. Section 4(3) of the UEMO further stipulates that if a CEM is sent by an individual or organization; and if the sending of the message is not authorized by any other individual or organization, the first-mentioned individual or organization shall be treated as authorizing the sending of the message.
>
> In order to help the senders to have a better understanding of the regulatory framework under the UEMO as well as their responsibilities, we have posted the Information for the Industry in our website at http://www.ofca.gov.hk/en/industry_focus/uemo/index.html. Besides, Industry Guide is also available at http://www.ofca.gov.hk/filemanager/ofca/common/uemo/uemo_industry_guide_e.pdf. Senders are always reminded to read the legislation in its entirety and consider seeking independent legal advice where necessary, so as to decide whether their practices are within the scope of the legislation or not, and how to comply with the law. To enforce the UEMO and ensure its compliance, we encourage the public to lodge reports with us in case of any suspected contravention of the UEMO.

Dyer said, "I leave it to readers of this newsletter to decide whether this is a clear and unequivocal answer to the questions I raised, that is, has OFCA clearly communicated these responsibilities to Hong Kong organisations and does OFCA have any system to detect when companies are not fully complying with the transitive nature of unsubscribes?"

More Information

ACMA Warns Groupon about Multi-List Subscribes
Unsolicited Electronic Messages Ordinance - Industry Focus
The Unsolicited Electronic Messages Ordinance An Industry Guide [pdf]

In the News

<web-link for this article>

Yui Kee Chief Consultant Allan Dyer made a short appearance in a recent episode of The Pearl Report, a weekly public affairs program aired on TVB Pearl in Hong Kong.

The episode dealt with identity and privacy, particularly in relation to recent government proposals to remove some personal details of company directors from the Companies Registry and the more stringent rules for the use of personal data in marketing that took effect

on 1st April. Dyer is seen from about 20:07, explaining his refusal to use his Hong Kong ID card number as an authenticator.

TVB contacted Dyer for an interview after finding a 2011 article from this newsletter. After viewing the finished program, Dyer commented, "I don't need the Privacy Commissioner telling me to treasure an authentication method that is fundamentally broken. There are alternatives, such as digital signatures. If a service provider does not offer a better method of remote authentication then it should be the user's decision to choose between bad remote authentication and inconvenient face-to-face authentication."

More Information

The Pearl Report 2013.04.29 - ID privacy
Privacy Protection in Hong Kong Allows Identity Theft

April Hong Kong Honeypot Report

<web-link for this article>

This is the sixteenth 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 fallen since February.

Average Time To Infect: 57 hours fourteen 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
- 6 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	China
2	United_States
2	Brazil
2	Japan
1	Latvia
1	Belgium
1	Russian_Federation
1	Panama
1	Vietnam

Malware

Checksum (md5)	This month	Previous count	Detection*
02a4232d99467318d62791c731bb0b3a	1	0 ***NEW	Y (w32/allaple.h , Net-Worm.Win32.Allaple.e , ,)
70ec5c4b3ff662232eacb0192fae42ac	1	1	Y (w32/ircbot.add , Backdoor.Win32.IRCBot.idc , W32Ircbot!I560.exe ,)
a03d41a33e925e9bcc54b6297d8dbfb5	1	0 ***NEW	Y (w32/virut.7116 , Net-

			Worm.Win32.Allaple.e Virus.Win32.Virut.av , ,)
9be443d09b25157fcfbccb953f4a2cd4	2	8	Y (W32/HLL-SysDlrSharer!Eldorado, , ,) old file with low detection rate
feb643c489c048083554aedac50126a9	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
952098cf3c65cfcb52282d8959ddffd3	1	7	Y (W32/Allaple.H , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
48048cfbf579c73b9587333d8768c282	1	0 ***NEW	Y (W32/Trojan.HNVI-3607, Trojan.Win32.Jorik.Llac.shk , ,)
e3bb292eff0a5bfbf768f42dcbea845d	1	1	Y (W32/WormX.TV W32/Allaple.H , trojan.win32.genome.rioo Net-Worm.Win32.Allaple.e , ,)
382fdcff132b058cfe50065b84fd8a4c	1	1	Y (w32/virut.7116 W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)
b7f91029e45e38b9d5530377195b46a1	1	0 ***NEW	Y (W32/Trojan.KEZW-6572, Trojan.Win32.StartPage.bclb , ,)
88ba6298fc1aa17ae96081667d6a0a65	1	0 ***NEW	Y (w32/allaple.h , Virus.Win32.Virut.n Net-Worm.Win32.Allaple.e , ,)
3875b6257d4d21d51ec13247ee4c1cdb	1	45	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)

Note:

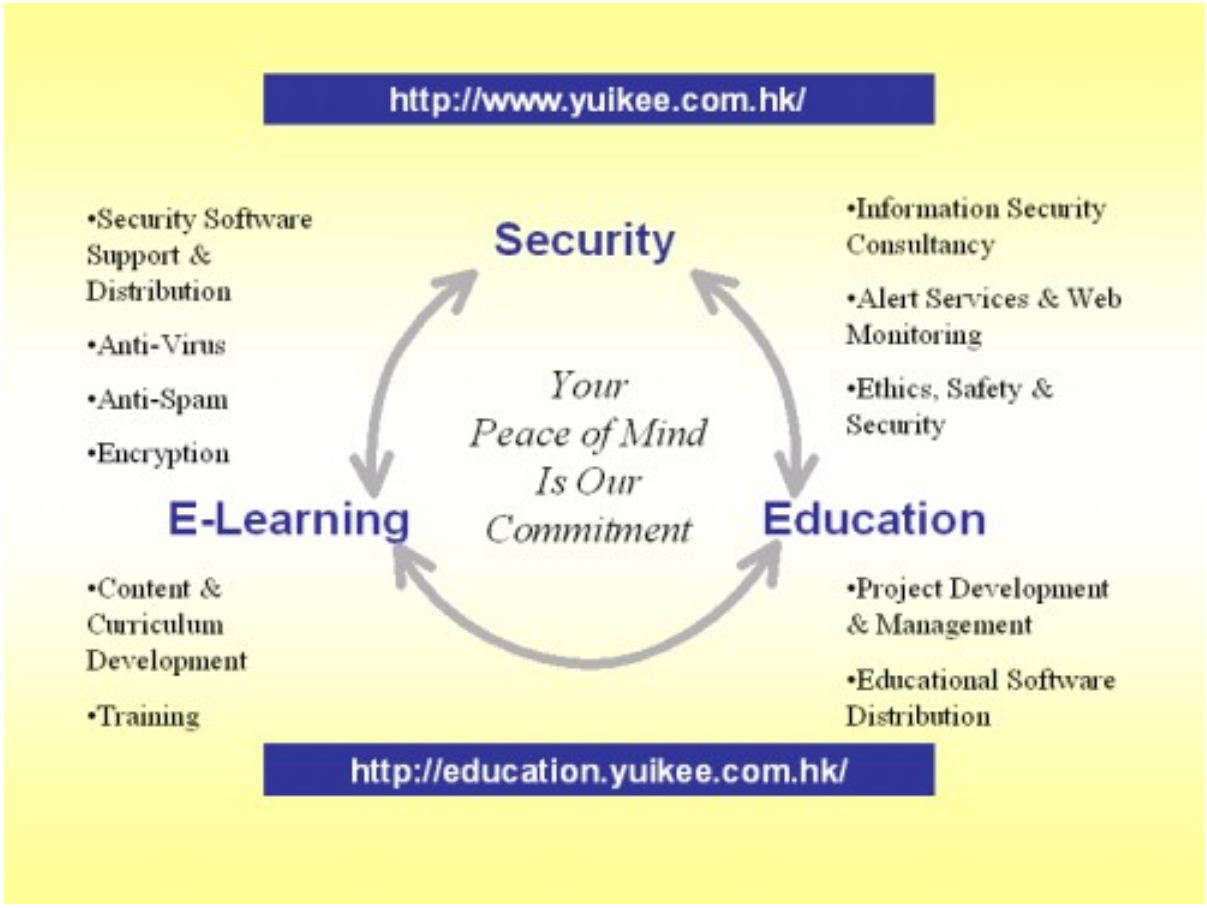
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

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/