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

Yui Kee Computing Ltd.

Newsletter

April 2014

Contents

Criminals use HKMA name to spread trojan

<web-link for this article>

Early on 1st April, emails with the subject "March Remit file - " followed by a 6-digit number were sent to Hong Kong-based email addresses. The emails appeared to be from the Hong Kong Monetary Authority, but in reality were sent from a variety of overseas IP addresses. The contents of the message encouraged the recipient to open the attachment:

> Attached is the remit file for the last month (Remit_6310536.zip) received from your accountant.
> Please print this label and fill in the requested information. Once you have filled out all the information on the form please send it to hkma_invoice@hkma.gov.hk .
> For more details please see the attached file.
> Please do not reply to this e-mail, it is an unmonitored mailbox!
> Thank you ,
> HONG KONG MONETARY AUTHORITY 55th Floor Two International Finance Centre
> 8 Finance Street Central Hong Kong
> © 2014 Hong Kong Monetary Authority. All rights reserved.
> **
>
> This e-mail is confidential. It may also be legally privileged. If you are not the addressee you may not copy, forward, disclose or use any part of it. If you have received this message in error, please delete it and all copies from your system and notify the sender immediately by return e-mail. Internet communications cannot be guaranteed to be timely, secure, error or virus-free. The sender does not accept liability for any errors or omissions.
>
> **

The attachment appeared to be a ZIP file, but is a trojan, variously identified as Troj/Agent-AGOJ, Trojan.GenericKD.1627845, or Trojan-Dropper.Win32.Injector.kbcs by Sophos, F-Secure and Kaspersky.

Similar malicious emails were sent out later the same day and on the morning of 3rd April.

The Monetary Authority has issued an alert about these fraudulent emails and the Police are investigating. Anyone who has received such emails should call Police at 2860 5012 or email crimeinformation@police.gov.hk.

More Information

Alert issued on bogus emails

Fake Wing Hang Bank Website Shut Down

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about a fraudulent website with the domain name "iwinghbhk.com". The HKMA reported that the website looks like the official website of Wing Hang Bank, Limited (Wing Hang Bank). The Police are investigating and, at the time of writing, the website had been removed.

People who have used the fake site for personal information or financial transactions should contact Wing Hang Bank at 3199 9188 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

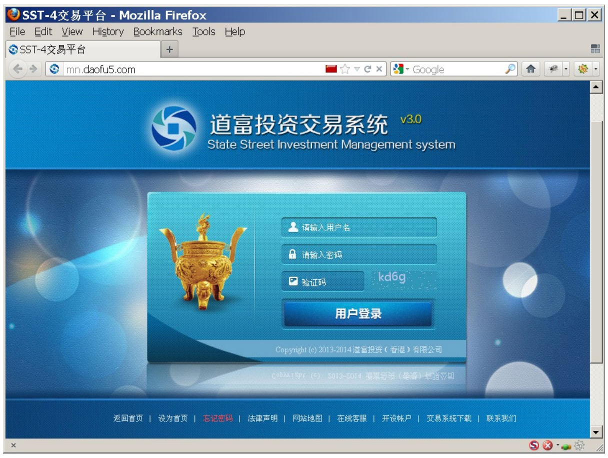
More Information

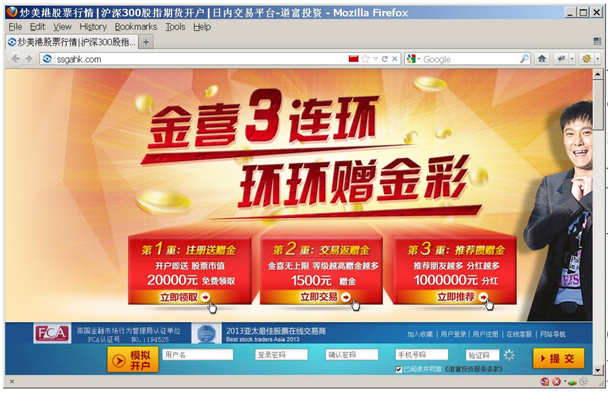
Fraudulent website: iwinghbhk.com
Alert issued on bogus website

Flurry of Fake Websites Target State Street Bank and Trust Company Customers

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about five suspected fraudulent websites: "www.ssgahk.com", "www.ssgahk.net", "mn.daofu5.com", "my.daofu5.com" and "www.daofu100.com". The site claimed they were operated by State Street Bank and Trust Company, a licensed bank in Hong Kong. The bank has stated they are not associated with these fraudulent sites and the Police are investigating.


SST-4交易平台 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SST-4交易平台
mn.daofu5.com
Google
道富投资交易系统 v3.0
State Street Investment Management system
请输入用户名
请输入密码
验证码
kd6g
用户登录
Copyright (c) 2013-2014 道富投资（香港）有限公司
返回首页 | 设为首页 | 忘记密码 | 法律声明 | 网站地图 | 在线客服 | 开设帐户 | 交易系统下载 | 联系我们


炒美港股票行情|沪深300股指期货开户|日内交易平台-道富投资 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
炒美港股票行情|沪深300股指...
ssgahk.com
Google
金喜3连环
环环赠金彩
第1重：注册送赠金
开户即送 股票市值
20000元 免费领取
立即领取
第2重：交易返赠金
金喜无上限 等级越高赠金越多
1500元 赠金
立即交易
第3重：推荐攒赠金
推荐朋友越多 分红越多
1000000元 分红
立即推荐
FCA
英国金融市场行为管理局认证单位
FCA认证号 NO.:194525
2013亚太最佳股票在线交易商
Best stock traders Asia 2013
加入收藏 | 用户登录 | 用户注册 | 在线客服 | 网站导航
模拟开户
用户名
登录密码
确认密码
手机号码
验证码
提 交
☑ 已阅读并同意《道富投资服务条款》

At the time of writing, four of the sites were still active on Mainland China IP addresses and showing either an investor login page or a garish products and services introduction.

Anyone who has used the sites should contact State Street Bank and Trust Company at 2840 5484 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Suspected fraudulent websites: www.ssgahk.com, www.ssgahk.net, mn.daofu5.com, my.daofu5.com and www.daofu100.com

Fake Bank of China and Standard Chartered Bank Email Warning

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned about e-mails supposedly from the Bank of China (Hong Kong) Limited (BOCHK) and Standard Chartered Bank (Hong Kong) Limited (SCBHK). The e-mails requests customers to use an embedded hyperlink to connect to a fraudulent webpage and enter their Hong Kong Identity Card number and credit card information. The banks have confirmed that the emails are fake and the Police are investigating. Anyone who has entered their sensitive information on the webpages should contact BOCHK at 2214 3417 or SCBHK at 2886 8868, and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The example fraudulent webpages listed by the HKMA had been dropped on webhosting services, probably without the knowledge of the hosting service provider or the legitimate user. The pages had been removed at the time of writing.

An HKMA spokesperson offered some security advice, "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. In addition, banks are not expected to send e-mails asking their customers to provide their account information (e.g. Internet banking logon passwords) or verify their account information online. If in doubt, they should contact their banks".

More Information

Fraudulent email purporting to be related to Bank of China (Hong Kong) Limited and Standard Chartered Bank (Hong Kong) Limited
Alert issued on bogus emails

HKMA Warns about fake BNP Paribas webpage located in Hong Kong

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned about a fraudulent webpage "http://www.focusgroup.hk/js/formulaire.html" that purports to be the official website of BNP Paribas. BNP Paribas has clarified that it has no connection with the fraudulent webpage, and the Police are investigating. Anyone who has provided personal information to or conducted financial transactions through the webpage should contact BNP Paribas at 2825 1116 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The webpage had been removed at the time of writing. The page was hosted on the website of Focus Asia Strategic Group, based in Hong Kong. Focus Asia uses hosting services from DYXnet, apparently at their Hong Kong data centre.

More Information

Fraudulent website: http://www.focusgroup.hk/js/formulaire.html
Fraudulent website: www.focusgroup.hk/js/formulaire.html

Lazy Guide to Heartbleed

<web-link for this article>

The biggest IT security story this month, the Heartbleed bug in OpenSSL, has reached the mainstream news media, so it would be a glaring omission not to mention it in this newsletter. Enough has been written about it elsewhere, so this is a summary and some pointers for anyone wondering about it a little.

What is Heartbleed?

It is a bug in some versions of software used to protect data being transferred across the internet.

Which software?

OpenSSL 1.0.1 to 1.0.1f. OpenSSL is software to make SSL connections, other packages do the same thing.

What does that do?

It encrypts data before sending it across the internet and, at the other end, decrypts the data.

How does Heartbleed Work?

The webcomic XKCD has an excellent cartoon explaining how Heartbleed works.

Am I Affected?

Yes. SSL is very commonly used to protect sensitive web pages. If you have noticed an address starting https: instead of http:, that site was using SSL to encrypt the data for transfer - both the webpage contents, and anything you sent to the website. It is also used in many other situations where sensitive data is transferred.

Now, your computer may be using different software for SSL, but, if the other end is using OpenSSL, an attacker could target that and get your information. So, you are affected even if you are not using OpenSSL yourself.

What Do I Do?

Are you a system administrator or a user?

System Administrators

1. Patch your systems. OpenSSL 1.0.1g has been released. Install it as soon as possible.
2. Then, get new certificates for your servers.

   Is a change of certificates a must?
   Yes, it is. You're worried that your users will have trouble with the applications dependant on the certificate. Unfortunately, there is no way of knowing whether your server's private key has been copied, so, to be safe, you must get new certificates. This will be a real pain if your users have added an exception for your server certificate, you will have to tell them all about the new one, and what to do with it.

   However, if you know the private keys of the certificate chain have not been exposed (i.e., they have never been present on a vulnerable host) it shouldn't be necessary to change those certificates. So, if you generated your own self-signed root cert and kept the private key safe and your clients have imported that root cert, they will accept the new server certs you generate using the same root.

   This also will not be an issue if you are using a certificate issued by a widely-recognised CA.
3. Tell your users to change their passwords.

Users

When the systems administrators of vulnerable sites tell you that they have updated their systems and installed new server certificates, change your passwords.

If you use the same password on multiple sites, you are very naughty. Now you have to change the passwords on sites that were not vulnerable, but you used the same password as a vulnerable site. This time, please use different passwords on each site. Use a password manager if you find it difficult to remember them all.

What Data Has Been Stolen?

No-one knows.

The good news is, if systems administrators and users promptly follow the advice, no more data will be compromised by Heartbleed.

The bad news is, we do not know if anyone else knew about the flaw and used it before the announcement was made. There are no clues left if it is used, so, in the worst case, criminals (or hostile governments, etc.) could have been quietly exploiting the Heartbleed flaw for up to two years.

On the other hand, the more criminals that knew about it, the more likely it would be that someone got careless and left clues that would lead security researchers to realise what was happening. So, perhaps only a small number of criminals were using it, presumably to attack high-value targets. It's all guesswork.

What does this mean for Open Source Projects?

This will add fuel to the open source/proprietary software argument. Open source says, "anyone can look for bugs" but, in reality, few do, and OpenSSL had only 4 overworked contributors. On the other hand, nothing about proprietary software makes bugs like this less likely or easier to find. The only thing guaranteed is that they will have a better PR team reassuring people that "there are no confirmed cases of this being exploited". Perhaps a few more techies can persuade their managers that contributing time to open source projects is valuable to their organisations.

More Information

xkcd: Heartbleed Explanation
Scramble to fix huge 'heartbleed' security bug
Heartbleed bug denial by NSA and White House
OpenSSL Heartbleed: Bloody nose for open-source bleeding hearts
Heartbleed exploit, inoculation, both released
Web data BLEEDOUT: Users to feel the pain as Heartbleed bug revealed
Running OpenSSL? Patch now to fix CRITICAL bug
Oh GREAT: Your factory can Heartbleed out

Fake Tax Returns Hit Hong Kong

<web-link for this article>

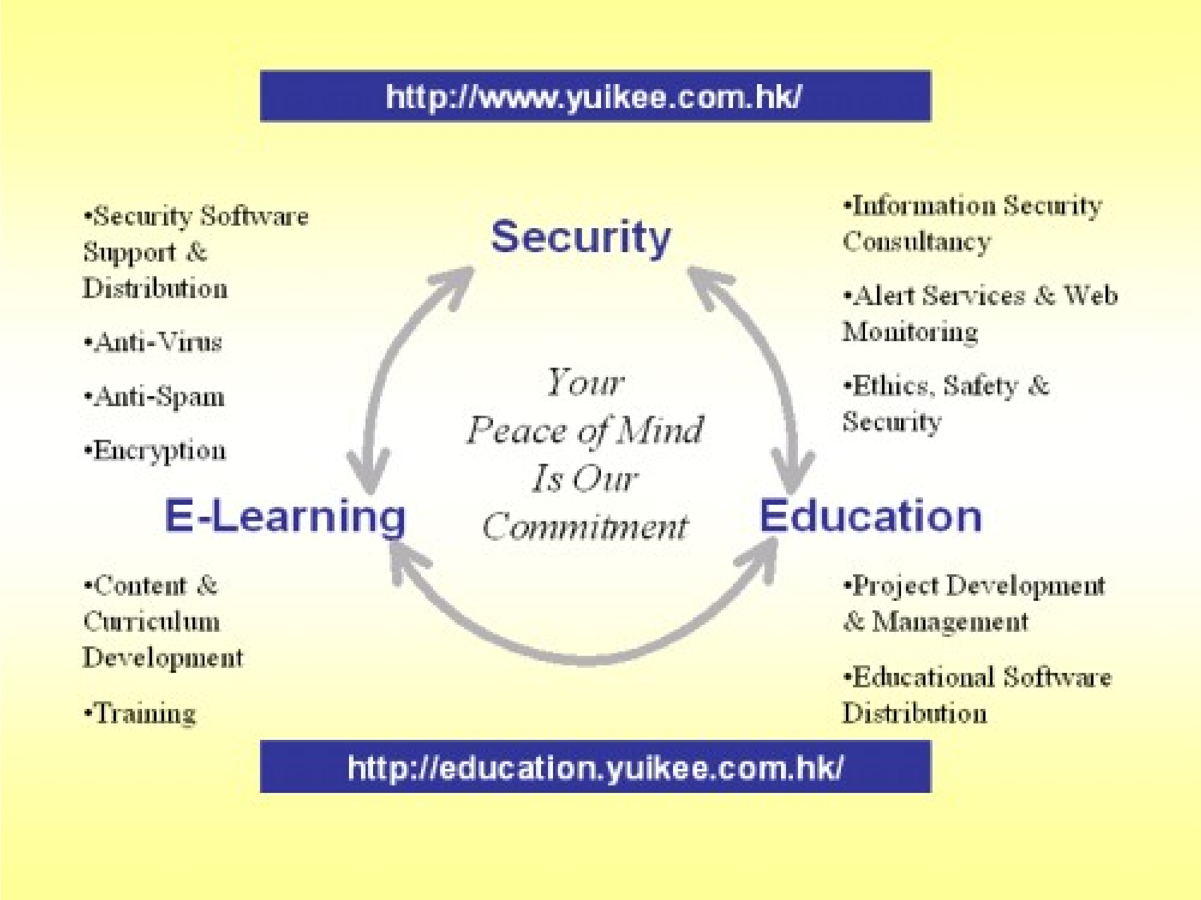
Hong Kong's Inland Revenue Department (IRD) has issued an alert about fraudulent emails purportedly issued by the department from the email address "noreply@ird.gov.hk". The emails have an attachment called "TaxReturnReport.zip", which, according to the IRD "may contain a computer virus". The Police are investigating and the IRD has reminded members of the public not to open any suspicious emails.

The case appears similar to an incident last October, also involving forged IRD messages.

More Information

有欺詐電郵冒認稅務局　附件或載有病毒
Fraudulent emails purportedly issued by Inland Revenue Department

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 Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

Security

- 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/