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

Yui Kee Computing Ltd.

Newsletter

September 2012

Contents

What is Cybercrime?

<web-link for this article>

A recent news report in the Hong Kong Standard suggests that Hong Kong Police are pushing the boundaries of cybercrime in an unexpected direction.

Two suspects, surnames Lui and Lam, were arrested for selling Taiwan-manufactured WiFi routers with a range of 1000 metres and are expected to be charged with "gaining access to a computer with criminal or dishonest intent". However, it is not explained what computer was accessed, and how this relates to the sale of the long-range WiFi routers. The Hong Kong Standard has not responded to a request for more information.

WiFi networking is usually limited to a distance of 100 metres, though local conditions can reduce that substantially. Longer ranges can be achieved by increasing transmission power, using a higher gain aerial or using a directional aerial and there is a wealth of information on enthusiasts' experience in setting up long range networks and building custom aerials on the internet.

The handling of the case raises many questions that are important to WiFi users in Hong Kong:

1. If the issue is breach of the telecommunications regulations in Hong Kong, why wasn't the Office of the Communications Authority (OFCA) involved?
2. Are particular types of WiFi equipment illegal? Which ones?
3. Can you be arrested for possession of illegal WiFi equipment?
4. Why were vendors arrested? Selling equipment is not the same as using it.

5. The only unusual feature of the WiFi routers mentioned was the range. If the issue is the range, what is the maximum permitted range of a WiFi connection in Hong Kong?
6. There are many public WiFi networks that are open for anyone to connect to, including GovWiFi. In the guides about connecting to these networks, there is no mention of a distance limit beyond which access is prohibited, how can users protect themselves against breaking the law when using public WiFi networks?

Updated: 24th September 2012

Police Clarification

During a telephone interview on 24th September 2012, the officer in charge of this WiFi case, Inspector Tai, DCS2, Shum Shui Po Police District gave some additional information, bearing in mind the requirements of the ongoing investigation.

The men arrested have not yet been charged, and more investigation of the many possibilities is required. The charge of "gaining access to a computer with criminal or dishonest intent" mentioned in the newspaper article is one of the many possibilities.

A device that was seized was capable of searching for WiFi networks and attempting to connect to password-protected networks. More detailed information, such as whether the device was WEP, WPA or WPA2 capable, was under investigation.

The Office of the Communications Authority (OFCA) was not involved in the investigation at the moment, but the Police could refer the case to other departments later, if necessary.

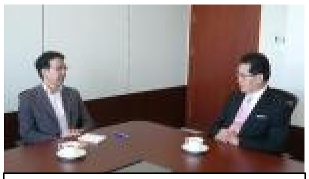
Inspector Tai could not offer general advice on choosing legal WiFi equipment and using it legally, but did comment that unauthorised access to password-protected networks was a point of interest in this case.

More Information

Traders face route to prison in WiFi racket

New IT Representative Meets Government Secretary

<web-link for this article>



r Charles Mok (left) and Mr Gregory So exchange views (photo: news.gov.hk)

Following his election last Sunday, Hong Kong's new representative for Information Technology, Hon. Charles Mok, has got down to work, meeting with the Secretary for Commerce and Economic Development, Mr Gregory So on September 12 for an exchange of views on policy matters.

A news.gov.hk press release reported Mr. So said, "I am glad that Mr Yiu Si-wing and Mr Charles Mok, the two newly elected members from the functional constituencies of Tourism and Information Technology respectively, accepted my invitation to meet today. We had very useful exchanges of views on matters that require our attention."

During his election campaign, Mr. Mok discussed the needs to review the Unsolicited Electronic Messaging Ordinance (UEMO) and update the Electronic Transaction Ordinance. He noted that the last review for combating cybercrime was in 2000 and that there could be an umbrella review of cybersecurity policy.

At the time of writing, the Legislative Council website had not been updated to show the new Members. The Members' Biographies and Members' Contact Directory still showed the composition of the fourth Legislative Council, not the fifth.

More Information

SCED meets with newly elected members of LegCo Election
Information Technology Functional Constituency Election Result
Legislative Council Members' Biographies
Legislative Council Members' Contact Directory

User Education: Advanced Fee Fraud

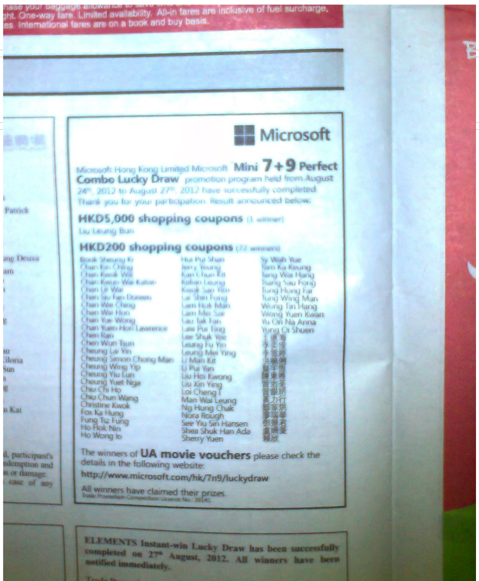
<web-link for this article>

Regular email users will be familiar with a variety of fraudulent messages arriving in their inboxes. The fact that these messages keep arriving suggests that some people fall for these scams. A common tactic is to tell the recipient they have won something. Let's take a look at some of these, and how to distinguish them from a genuine prize notification.

This table shows basic details of several messages:

Subject	Claimed Sender	Other details
$580,000.00 Winner	U.K Apple-iPhone	From: "APPLE-IPHONE PROMOTION ONLINE " <lr1@yale.edu> Reply-To: appleiphonep5@aol.co.uk
Your e-mail has won you £800,000	BBC LOTTERY BOARD	From: "BBC" <lr1@yale.edu> Reply-To: bbc.care@aol.co.uk
CLAIM!!	BBC LIVE UK	Your entitlement £1,000,000.00 BBC ONLINE PROMO
UK YAHOO AWARD/WINNER/OPEN ATTACHMENT FOR PRIZE CLAIM	Yahoo Awards United Kingdom	
Important Notification [You have Won]	Lucky Gold Strike Program	
MC Donald's Restaurants Ltd:	MC Donald's Restaurants Ltd:	Enjoy $650,000.00 from McDonald's in Spain
GOOGLE FAIR FUND	Google Awards Committee	Dear Google Active User, You have been selected as an eligible recipient of Google Grand Prize and attached to this email is the official letter of notification.
Reference Number: BMW:2551256003/23	BMW	A BMW SALOON CAR AND £45,000.00 pounds has been won by you on our BMW PROMOTION
NOTIFICATION!!!	2012 Petronas Free Lotto Corporation ©	We wish to bring to your notice that your email has been selected in Petronas on-going sweepstakes.
EuroMillions Friday night's draw	EuroMillions	63.8Million Pounds Winner Yet To Come Forward,
PLEASE VIEW YOUR WINNING NOTIFICATION	London Olympics Lottery	
Congratulations Read The Below Attached File	Microsoft Online Promotions	
CONGRATULATION'S FROM COCACOLA UK	Coca Cola UK	

Now let's take a look at a genuine lucky draw notice: . The first thing to notice is that it is a print advert in a newspaper. Secondly, the top prize is a single HK$5,000 (about UD$645) shopping coupon, and 72 other winners got HK$200 (about US$26) shopping coupons. This is a long way from winning a car or millions.



ght. One-way fare. Limited availability. All-in fares are inclusive of fuel surcharge,
es. International fares are on a book and buy basis.

Microsoft

Microsoft Hong Kong Limited Microsoft "Mini 7+9 Perfect Combo Lucky Draw" promotion program held from August 24th, 2012 to August 27th, 2012 have successfully completed. Thank you for your participation. Result announced below:

HKD5,000 shopping coupons (1 winner)

Liu Leung Bun

HKD200 shopping coupons (72 winners)

Book Sheung Ki
Chan Kin Ching
Chan Kwok Wai
Chan Kwun Wai Kelvin
Chan Lit Wai
Chan Siu Fan Doreen
Chan Wai Ching
Chan Wai Hon
Chan Yue Wong
Chan Yuen Hon Lawrence
Chen Ran
Chen Wun Tsun
Cheung Lai Yin
Cheung Simon Chong Man
Cheung Wing Yip
Cheung Yiu Lun
Cheung Yuet Nga
Chiu Chi Ho
Chiu Chun Wang
Christine Kwok
Fox Ka Hung
Fung Tsz Fung
Ho Hok Nin
Ho Wong To
Hui Pui Shan
Jerry Yeung
Kan Chun Kit
Kelvin Leung
Kwok San Yin
Lai Shin Fung
Lam Huk Man
Lam Mei Sze
Lau Tak Fan
Law Pui Ting
Lee Shuk Yee
Leung Fu Yin
Leung Mei Ying
Li Man Kit
Li Pui Yan
Liu Hoi Kwong
Liu Xin Ying
Loi Cheng I
Man Wai Leung
Ng Hung Chak
Nora Rough
See Yiu Sin Hansen
Shea Shuk Han Ada
Sherry Yuen
Sy Wah Yue
Tam Ka Keung
Tang Wai Hang
Tsang Sau Fong
Tung Hong Fai
Tung Wing Man
Wong Tin Hang
Wong Yuen Kwan
Yu On Na Anna
Yung Oi Shuen
[illegible]

The winners of **UA movie vouchers** please check the details in the following website:
http://www.microsoft.com/hk/7n9/luckydraw

All winners have claimed their prizes.
Trade Promotion Competition Licence No. 39141

ELEMENTS Instant-win Lucky Draw has been successfully completed on 27th August, 2012. All winners have been notified immediately.

The Sting

How do the criminals profit from sending these fake messages? They are hoping that gullible victims will reply, claiming their prize. Usually, they will be told that there is a "minor administrative fee", which is very small compared to the winnings, that they have to pay first, in order for their winnings to be released. Of course, the winning are never released. This is why these scams are called Advanced Fee Fraud, the victim pays in advance, on the promise of receiving a lot more in future.

Alternatively, the criminals may ask for bank details in order to pay the money to the victim's account. If they get enough details, they can access the account and withdraw all the victim's funds.

Advice

- **Don't Believe Everything You Read** Email, in particular, is easy to forge. Just because it says "Microsoft" in the From: field, it might not be from Microsoft.
- **You Will Never Win a Lottery that you Did Not Enter** Did you buy a ticket? Did you sign up for a promotion? Organisations run lotteries to promote their name or brand, so they want you to remember entering the competition. If you do remember entering a lottery, is it exactly the same name? Are the prizes the same? Does the notification method match what you were told? Check the details on your ticket.
- **The Bigger the Prize, the More Unlikely is Your Win** There is only one Grand Prize, a few smaller prizes and thousands of losers. Be suspicious.

Email is cheap, a fraudster can send millions of fake messages for almost nothing, hoping to catch one foolish person. Don't be that person.

You may use this article for educational purposes, so long as the source is quoted.

Sophos Self False-Positive

<web-link for this article>

Anti-Virus developer Sophos has issued an advisory concerning a false-positive detection for Shh/Updater-B on many binaries that have updating functionality, including components of Sophos Anti-Virus.

This can interfere with the capability of Sophos Anti-Virus to update itself. The advisory includes procedures for re-establishing updating in a number of scenarios. Fortunately, the central management tools can be used to correct the problem without manual intervention at each endpoint.

Sophos released a new identity to eliminate the false positives at Wed, 19 Sep 2012 21:32 +0000 (20 Sep 2012 05:32 a.m. Hong Kong time).

Most anti-virus vendors have, occasionally, shot themselves in the foot, releasing problematic virus identities.

Updated: 28th September 2012

In an email to customers, sent 28th September, Sophos have admitted that this false positive has resulted in large numbers of support calls. They have also provided additional information on the problem, by updating the original knowledgebase article and in a new knowledgebase article that includes a tool to help identify and fix applications that have been affected. Affected applications may include Adobe and Java.

Sophos also commits to publishing a root cause analysis including the steps we are taking to ensure it never happens again. In a letter, Sophos CEO Kris Hagerman apologises for the incident and explains the commitment of resources put behind ensuring all Sophos customers are returned to a normal, productive and protected state. He reaffirms the commitment to sharing the root cause analysis and preventative measures they will implement.

More Information

Shh/Updater-B false positive by Sophos anti-virus products
Advisory: Shh/Updater-B False positives
Message from the Sophos CEO
Shh/Updater-B false positive: Discovering and resolving potentially impacted products

Businessman Denies DDoS Attack on Hong Kong Stock Exchange

<web-link for this article>

Tse Man-lai Ernest pleaded not guilty in the District Court on 24th Septermber to two counts of obtaining access to a computer with criminal or dishonest intent in connection with Distributed Denial of Service (DDoS) attacks on the Hong Kong Stock Exchange news website (HKExnews) in August 2011. Mr Tse is a Director of Pacswitch Globe Telecom, a company that provides internet and telephony services. Pacswitch was licensed as an External Telecommunications Services (ETS) Operator by OFCA in 2010.

The prosecution claims that the DDoS attack was launched from a computer at Tse's mother's home, and a blog post titled, "Ernest Networking teaching", that demonstrated the attack on HKExnews, asked people to subscribe to the author's DDoS prevention method and included the web address of Pacswitch Globe Telecom.

The prosecution accuses Tse of launching the attacks and writing the blog post to promote the business of his company.

Pacswitch offers "1Gbps Internetional Bandwidth" *(sic)* and an Email Marketing Service that is more expensive for non-profit and educational users than it is for business users. The website does not currently mention security or DDoS prevention services.

More Information

Cyberattack on stock exchange website denied
IT boss denies HKEx attacks
Businessman Arrested for Stock Exchange Attack
Trading at Hong Kong Stock Exchange Suspended after Cyber-Attack
Pacswitch :: Hong Kong Ultra Speed Data Center
Pacswitch Globe Telecom Limited - Hong Kong
External Telecommunications Services (ETS) Operators
About Pacswitch
Pacswitch Globe Telecom

September Hong Kong Honeypot Report

<web-link for this article>

This is the ninth 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 this month has risen slightly from last month's low.

Average Time To Infect: 29 hours 46 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 : 25

18 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	Canada
3	Vietnam
3	South Korea
2	Singapore
2	Taiwan
1	Italy
1	El Salvador
1	United Kingdom
1	India
1	Sri Lanka
1	Indonesia
1	United States
1	Finland

Malware

Checksum (md5)	This month	Previous count	Detection*
ae80588386f3783d9fc47a105fc9a881	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
0fed4b31a0592a1a66ec71eb298d31d1	2	0 ***NEW	Y (w32/genbl.0fed4b31!olympus , UDS:DangerousObject.Multi.Generic , ,)
94109e9b3f2b045350db9a5cb592b178	1	12	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
8be3ff632500903d38013474346ea93f	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.a , ,)
b82698a30e07fc71349f06750cae2664	2	5	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
1d53fb866c27a421f7557e3cda0592ac	2	6	N (, , ,) not a new file but with little detection
df23f0e2860d26bc717c78759513238a	1	0 ***NEW	Y (w32/genbl.df23f0e2!olympus , Trojan.Win32.Jorik.Lethic.aqv , ,)
bbb5034e33568e100dd3dadabb5a57e9	1	15	Y (w32/sdbot.otr w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)

923fe97652d40e90b2416a3b1c2d8a22	1	0 ***NEW	Y (w32/genbl.923fe976!olympus , Trojan.Win32.Jorik.IRCbot.qrq , ,)
cb576cca04946b3d0829703d108ae270	1	15	Y (w32/sdbot.otr w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
90af8982f4c98882c173024cf931c474	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , , ,)
f895f41516d85bb7ad348237e2c4f4f7	1	0 ***NEW	Y (w32/allaple.c , , ,)
5e8dd2939aea462bd1116aa358e3d92f	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , , ,)
deb53113983eba1f68cc3c2f62329787	1	0 ***NEW	N (, , ,) not a new file but with little detection
41cc77ad6cf73276c2d421f536467f40	2	0 ***NEW	N (, , ,) a new file with little detection
b93decfbef74784ede9d20b5590550ee	1	0 ***NEW	Y (w32/genbl.b93decfb!olympus , Trojan.Win32.Jorik.Lethic.aqv , ,)
10980f4df2060b86a72eb5e533102980	1	2	Y (w32/backdoor2.dstk w32/backdoor2.dstk , Backdoor.Win32.IRCBot.jwy Worm.Win32.AutoRun.tet , W32Ircbot!I484 ,)
70cef8240529b5ab041964ac3e6f5db5	1	0 ***NEW	Y (w32/trojan.mex , Backdoor.Win32.Rbot.bni , ,)
93ea070aeba1be7c464e788350018bd5	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
ee94b06c5edc3f9e75a26c0108d08b55	1	0 ***NEW	Y (w32/genbl.ee94b06c!olympus , Backdoor.Win32.Azbreg.esn , ,)
7e6936d3e7fa8f92e7e34903335d326e	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
0b81d75db17f25d58491a5dc08a07be0	1	0 ***NEW	Y (w32/emailworm.amx , Net-Worm.Win32.Allaple.b , ,)
af1894848b6525c7882c33b59d1bbebd	1	0 ***NEW	Y (w32/allaple.h w32/allaple.h , Net-Worm.Win32.Allaple.e , ,)
7867de13bf22a7f3e3559044053e33e7	1	4	Y (w32/susppack.cy.gen!eldorado , Backdoor.Win32.Agent.aknp , ,)
01a75df3f3e7bf1a08632187e5965ac0	1	0 ***NEW	Y (w32/emailworm.hqk , Net-Worm.Win32.Allaple.e , ,)

One of these files has been in the Wildlist.

Note:

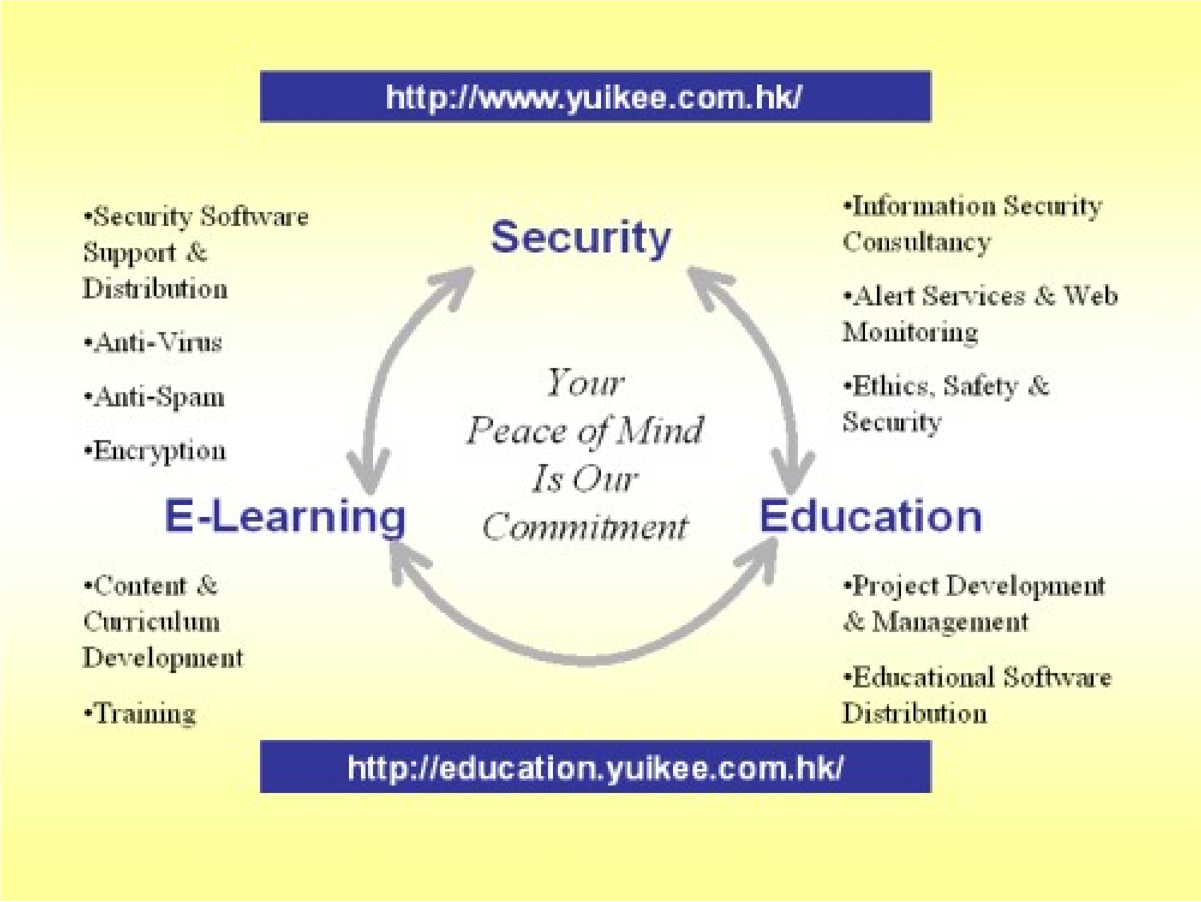
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

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 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

Education

•Content & Curiculum Development

•Training

•Project Development & Management

•Educational Software Distribution

http://education.yuikee.com.hk/