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

Yui Kee Computing Ltd.

Newsletter

July 2012

Contents

Banks Upgrade Security Advice (Humour)

<web-link for this article>

NewsBiscuit (*The news before it happens*) reports that banks are advising children on how to name their first pet. Our own correspondent provided similar advice a couple of years ago. Nice to see these ideas taking hold.

More Information

Children warned name of first pet should contain 8 characters and a digit
Protecting Your Identity Online

Internet Still Not Dead - Goodbye DNSChanger

<web-link for this article>

In May, we reported that up to 1200 computers in Hong Kong might loose their internet connection on July 9th, along with many others around the world. Writing now, a safe time after the deadline, nothing much happened.

In a blog posting, F-Secure reports that infection numbers continue to fall and many ISPs are redirecting DNS requests for infected customers.

Yui Kee's Chief Consultant, Allan Dyer, commented, "How long should the ISPs continue redirecting? I suspect that, in most of the remaining cases, the user will only notice their machine is affected when they loose their connection."

More Information

DNSChanger Wrap Up
DNS Changer - how not to lose your internet connection on July 9
How to detect and fix a machine infected with DNSChanger
FBI kills DNSChanger network, but how many will be affected?
DNSChanger apocalypse: Like Y2K, but even snoozier
How the DNSChanger malware works

July Hong Kong Honeypot Report

<web-link for this article>

This is the seventh 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 jumped up sharply, with most coming from Finland.

Average Time To Infect: 2 hours 44 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 : 263

17 are brand new to this honeypot.

Source of Attacks

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

230	Finland
7	Taiwan
6	Japan
5	United_States
2	Kazakstan
2	Brazil
2	Spain
2	Vietnam
2	Canada
1	Indonesia
1	Singapore
1	Australia
1	Malaysia
1	Hong_Kong

Malware

Checksum (md5)	This month	Previous count	Detection*
e42f4d2d96bea46838e780b2b40cd54b	1	0 ***NEW	Y (w32/sdbot.aefv W32/Backdoor2.AJVM , Backdoor.Win32.Rbot.bni , ,)
5857bdf42f797445cfa3b09ed7c77f6b	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
3dd2c2b97fc8824ebc7c770752899bed	1	3	Y (w32/genbl.3dd2c2b9!olympus , Trojan.Win32.Jorik.Poebot.eq , ,)
94109e9b3f2b045350db9a5cb592b178	4	8	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
382fdcff132b058cfe50065b84fd8a4c	1	0 ***NEW	Y (w32/virut.7116 W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)
0ab0fa91709a5fb0b48b9b10e51b16d1	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
961dcb5a7c03b7f9acceab3e7e66c134	1	2	Y (w32/virut.7116 , Virus.Win32.Virut.av

			Net-Worm.Win32.Allaple.e , ,)
2f26fd2edab6f916d686604db20264f2	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado , Net-Worm.Win32.Allaple.b , ,)
865915650a85e7c27cdd11850a13f86e	2	11	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
5db68cd45f0c95c9cba56ae6a2bacc6b	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
3875b6257d4d21d51ec13247ee4c1cdb	2	26	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
4711e0fccd0565f1826fe10909f1698e	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado , Net-Worm.Win32.Allaple.b , ,)
9987b5cbff8f6942a29b707d1a549b77	230	0 ***NEW	N (, , ,) * not a new file but with limited detection
65dfcfe7988418e7b7eb084c96051b92	1	0 ***NEW	Y (w32/genbl.65dfcfe7!olympus , Backdoor.Win32.Azbreg.awc , ,)
4d6c4cc06bacbab059ba52607530d1ec	1	0 ***NEW	Y (w32/genbl.4d6c4cc0!olympus , HEUR:Backdoor.Win32.Generic , ,)
5fe9bf522fb0160b50e4737bd9e09fe7	1	0 ***NEW	Y (w32/genbl.5fe9bf52!olympus , Backdoor.Win32.Azbreg.bch , ,)
bbb5034e33568e100dd3dadabb5a57e9	2	12	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
4ed217391b897fc2d46ec9ce8af282cf	1	3	Y (W32/Virut.AG , Backdoor.Win32.Rbot.adqd , ,)
6e2fa9031a05b9649da062c550d14a3d	1	3	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
32610374d3922a1ae50fada7a684931e	1	0 ***NEW	Y (W32/Allaple.C , Net-Worm.Win32.Allaple.b , ,)
9cf15714790fd07ad2955dfef7255af0	1	0 ***NEW	Y (W32/Emailworm.AMX , Net-Worm.Win32.Allaple.b , ,)
15965bb88165d1eb06851d8f076130ba	1	14	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
4dc508b15c0b748ff16e79088a1179ea	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado, Net-Worm.Win32.Allaple.b , ,)
cb576cca04946b3d0829703d108ae270	1	14	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
33fdb683c37fe3d87a403a5db0cbe821	1	1	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
df630013dccf7c7741a924e9353005e2	1	0 ***NEW	Y (W32/Virut.AG , Backdoor.Win32.Rbot.adqd , ,)
85a786387d1511bececc87843631ddc2	1	0 ***NEW	Y (W32/Trojan.MEX , Backdoor.Win32.Rbot.bni , ,)
b0599b847e5df4109e7a0e4ad883e00e	1	0 ***NEW	Y (W32/Virut.AG , Net-Worm.Win32.Allaple.e Virus.Win32.Virut.at , ,)

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

Drug Testing Highlights School Privacy Deficiencies

<web-link for this article>

A trial scheme to test Hong Kong school students for drugs has been criticised by the Privacy Commissioner for Personal Data, Allan Chiang Yam-wang.

The testing was performed by the Security Bureau's Narcotics Division and the Education Bureau, but they did not conduct a privacy impact assessment. Mr Chiang also highlighted problems in the protocols for handling the students personal data set by the Bureaus, including not stating how long the data should be retained, and not adequately protecting the data that was stored on a USB flash drive. The drive was password protected, but the password was stored with the drive. Teachers processed the data on their personal computers, but received no guidance on how to safeguard the data.

A spokesman for the Narcotics Division said that the protocol has already been revised, including requiring all computers storing students' data to shut down internet connections.

A wider question remains. Teachers routinely process personal data concerning their students, and some of it may be as sensitive, or more sensitive than drug test results. Do teachers has adequate training and resources to protect this personal data? Without proper training, teachers might easily misunderstand protocols - an internet connection is forbidden, but they might use a connection to a LAN (with an internet gateway) without realising the consequences, or may overlook that their laptop has silently connected to WiFi.

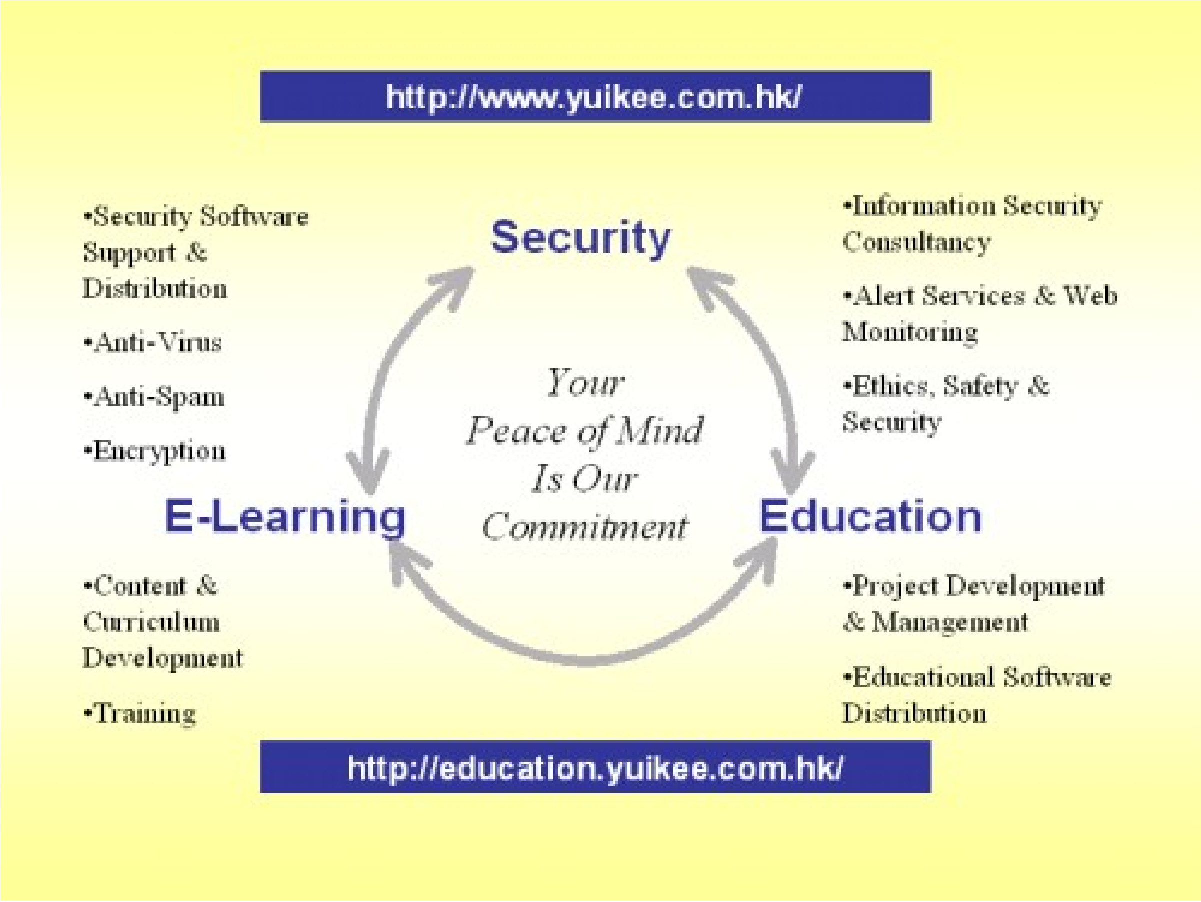
A piecemeal approach to personal data protection - one policy for drug test results, another for exam results, and so on - will increase the burden on teachers, and may introduce conflicting requirements, perhaps one protocol demands no internet connection, and another a secure connection to a server.

More Information

School drug testers hit for privacy lapses

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

•Content & Curriculum Development

•Training

Education

•Project Development & Management

•Educational Software Distribution

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