Yui Kee Computing Ltd.

Newsletter

October 2012

Contents

Wild Speculation Vindicated in Miss Hong Kong Fiasco

<web-link for this article>

In August 2012, TVB, the organisers the Miss Hong Kong beauty pageant, initially blamed the collapse of the online voting system for the contest on unknown hackers. This newsletter reported reported on the fiasco and quoted security consultants Allan Dyer and Richard Stagg speculating wildly about the possible causes. They agreed that the most probable scenario was incompetence, a failure of capacity planning.

TVB has now released the results of an investigation by PwC into the incident, saying that they found no evidence of hacking and that the number of transactions due to voting activity between 22:02 and 23:02 far exceeded the predefined hourly limit of 12.8 million transactions, resulting in system paralysis.

More Information

PwC: TVB underestimates Miss Hong Kong voting traffic
Was Incompetence, Enthusiasm or Greed Behind the Miss Hong Kong Voting Failure?

Businessman Convicted of Crashing Hong Kong Stock Exchange Website from Mother's Home

<web-link for this article>

Tse Man-lai, Director of Pacswitch Globe Telecom, a company that provides internet and telephony services, was convicted of a Distributed Denial of Service (DDos) attack against the Hong Kong Stock Exchange's regulatory disclosure website, HKExnews on 12th and 13th August 2011. He was found guilty on two counts of accessing a computer with criminal or dishonest intent and sentencing was adjourned to 9th November. Tse has a computer diploma from the Hong Kong Polytechnic University.

Judge Peter Longley said Tse knew the website, HKExnews, had been attacked on 10th and 11th August 2011, resulting in trading suspensions for seven companies including HSBC and Cathay Pacific, just before his attacks. Tse claimed that he did not intend to attack the site, but he thought he was offline while he fiddled with the attack software. He also claimed that the attacks resulted in the public being educated. The judge reject the claims as unreasonable. The judge accepted the prosecution's claims that, with his IT expertise, he must be aware of being online and that the attacks purpose were to promote his company's services. Tse admitted that he was the only user of the computer at the home he shares with his mother, which was used to launch the attacks.

The source of the earlier attacks on the HKEX website is still unknown.

More Information

IT boss found guilty of HKEx hacking attacks
Businessman Arrested for Stock Exchange Attack
Businessman Denies DDoS Attack on Hong Kong Stock Exchange
Trading at Hong Kong Stock Exchange Suspended after Cyber-Attack

October Hong Kong Honeypot Report

<web-link for this article>

This is the tenth 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 fallen slightly from last month's figure

Average Time To Infect: 32 hours 21 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 : 23

20 are brand new to this honeypot.

Source of Attacks

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

6	Japan
2	Taiwan
2	United States
2	Hong Kong
1	Israel
1	France
1	Romania
1	Austria
1	Vietnam
1	Philippines
1	Russia
1	Canada

1	Poland
1	Portugal
1	Malaysia

Malware

Checksum (md5)	This month	Previous count	Detection*
0e8f41329cb1bbe2230c83564fe16c01	1	0 ***NEW	Y (w32/emailworm.amv , Net-Worm.Win32.Allaple.d , ,)
bbb5034e33568e100dd3dadabb5a57e9	2	0 ***NEW	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
87247ad165eddf91ee2cd8b154c72abd	2	0 ***NEW	N (, , ,) an old file with little detection - probably a PUA
6e2fa9031a05b9649da062c550d14a3d	1	0 ***NEW	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , WL-dc1ca4287875927725689f45b31ba338-0 ,)
15965bb88165d1eb06851d8f076130ba	1	0 ***NEW	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
f9dc3945bdd7406bd8db06a47963ec14	1	0 ***NEW	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
c2e9a9884a40f242bac1d7d9fe39056d	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
04721e2041b088a0a1a175cbeb44febe	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.a , ,)
96843f69e602e96a04c5557ca96243f6	1	0 ***NEW	Y (w32/virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
94109e9b3f2b045350db9a5cb592b178	1	0 ***NEW	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
4d4c2729b8aa56e70eaf9ef84e9d5d3d	1	0 ***NEW	Y (w32/agent.ix.gen!eldorado w32/genbl.4d4c2729!olympus , Trojan-Spy.Win32.Agent.bmxb , ,)
3875b6257d4d21d51ec13247ee4c1cdb	2	0 ***NEW	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
9e209d037787e76d9c57e263ff86f335	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
33959bb2c48363ddd3637ea78c048b6c	1	0 ***NEW	Y (w32/sdbot.aefv , Virus.Win32.Suspic.gen Virus.Win32.Virut.n Type_Win32 , ,)
3be3a929774b8dc0ac56065a0c716e87	1	0 ***NEW	Y (w32/genbl.3be3a929!olympus , Backdoor.Win32.Azbreg.hik , ,)
95262bd40b2be4a9c2ef328e14286d00	1	0 ***NEW	N (, , ,) an old file with no detections
27e0cb71d5229bf0290590dc9eef70ba	1	0 ***NEW	Y (w32/allaple.h , trojan.win32.genome.rioo Net-Worm.Win32.Allaple.e , ,)
aab0b68982d2babcf3656cd686b3ac9f	1	0 ***NEW	Y (w32/trojan2.kexn , Trojan-Spy.Win32.Agent.bmxb , ,)
14c31fa0f1fdeee959074fda2fdb78fc	1	0 ***NEW	Y (w32/emailworm.amt , Net-Worm.Win32.Allaple.a , ,)
fbafdef020622e5c62c7a3be49faaa79	1	0 ***NEW	Y (w32/genbl.fbafdef0!olympus , Worm.Win32.Hamweq.hz , ,)

Two 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

Foxy Bites Police Again, Privacy Commissioner Investigates

<web-link for this article>

Hong Kong's Privacy Commissioner for Personal Data, Mr. Allan Chiang, has announced that he has launched a formal investigation into recent personal data leakage incidents involving the Police and the file sharing software Foxy. He has also started compliance checks about other data breach incidents which may lead to formal investigations in due course.

Mr Chiang met with Acting Commissioner of Police, Mr. Xavier Tang on 30th October to express his concern about personal data protection. Mr. Tang confirmed that the Police also take a serious view on the incidents and have started their own investigation.

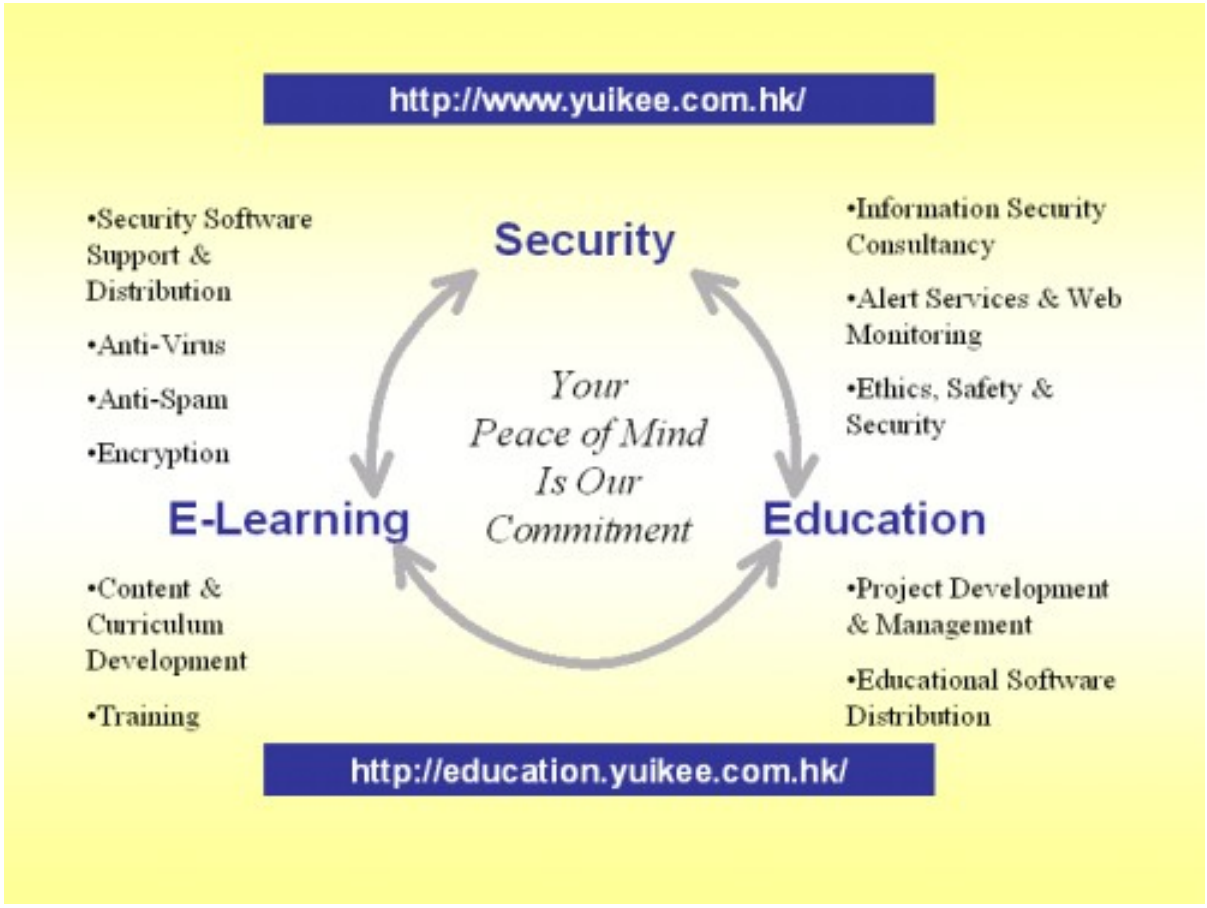
The recent leaks include leakage of 210 documents including witness statements, internal memos and letters via Foxy; loss of 79 children's Cross-Boundary Student Closed Area Permits; and loss of books and notebooks. Foxy was also blamed for leaks of personal data from the Police in May 2005.

More Information

Privacy Commissioner investigates Police data leakage incidents
Data Leak Disease Spreads to Police?
ICAC Claims it doesn't use Foxy

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/