Yui Kee Computing Ltd.

Newsletter

December 2012

Contents

Contents....1
No Privacy for Security Conference Invitees....1
Hong Kong Police Launch Cyber Security Centre....1
December Hong Kong Honeypot Report....2
- Average Time To Infect: 20 hours 27 minutes....2
- Summary....2
- Source of Attacks....2
- Malware....3

No Privacy for Security Conference Invitees

<web-link for this article>

An email Call for Papers for SERE 13, the Seventh IEEE International Conference on Software Security and Reliability, included the email addresses of 899 researchers in the "To:" field. Truncation of the last address suggests that a longer list was not disclosed only because of software limitations, and the full list was probably much longer. The last address started with "c", and the addresses were in alphabetical order, so the partial list has probably been disclosed to the full list of thousands of recipients.

SERE 13 will be held in Gaithersburg, Maryland, USA, but the message originated from Swinburne University, near Melbourne, Australia. Dr. Fei-Ching (Diana) Kuo, Senior Lecturer in Faculty of Information and Communication Technologies at Swinburne is Publicity Chair of SERE 13.

Updated: 10th December 2012

In an email message, Dr. Kuo wrote, "Sorry for this mistake. We have some issues with the Outlook2010. Somehow the mailing list was added to TO instead of BCC this time. I am very sorry for the problem caused."

More Information

SERE 13 Conference Website
Swinburne University of Technology

Hong Kong Police Launch Cyber Security Centre

<web-link for this article>

The Hong Kong Police have launched a Cyber Security Centre, costing HK$9 million, to react to the growing threat of attacks on critical infrastructure.

Speaking at a press conference, Commercial Crime Bureau Chief Superintendent Chung Siu-yeung explained that the centre would strengthen the resilience of critical infrastructure in

Hong Kong. He emphasised that it would only monitor the traffic of critical infrastructure, and it would not monitor the data traffic or content of organisations or individuals.

The centre's 27 officers will provide 24 hour service in the detection and prevention of technology crime. Roy Ko, manager of HKCERT, said that his team would work closely with the centre. HKCERT will focus on cleaning up compromised machines, and the Cyber Security Centre would warn a protect HK organisations. Charles Mok, LegCo member for the IT functional constituency, said that the Police should use independent experts to review their procedures and protect against infringing upon the privacy and personal data of users.

More Information

Police launch Cyber Security Centre
Hong Kong Police invests HK$9M in cyber security center
Hong Kong cops open £700k cyber security centre
Privacy fears over police cybersecurity monitoring

December Hong Kong Honeypot Report

<web-link for this article>

This is the twelfth 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. Because of public holidays, this report covers up to 20th December 2012.

Average Time To Infect: 20 hours 27 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 : 27
- 10 are brand new to this honeypot.

Source of Attacks

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

9	Japan
5	United_States
2	Taiwan
2	Canada
1	Ukraine
1	Germany
1	Hungary
1	Thailand
1	France
1	Hong_Kong
1	Singapore
1	Vietnam
1	United_Kingdom

Malware

Checksum (md5)	This month	Previous count	Detection*
b0b39f058a958778b15a5c4589a2938d	1	0 ***NEW	Y (w32/sdbot.aefv W32/Backdoor2.AJVO , Backdoor.Win32.Rbot.bni , ,)
bbb5034e33568e100dd3dadabb5a57e9	1	18	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
6f06e39cb6df0908d5ab6e661c6b0386	1	1	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.advj , ,)
358895aabbb154baeb5524fa432dcfc9	1	0 ***NEW	N (, , ,) No information.
9e011ed0f754f58f18285db13e1ab55c	1	0 ***NEW	Y (w32/genbl.9e011ed0!olympus , Trojan.Win32.Jorik.IRCbot.vnh , ,)
1d53fb866c27a421f7557e3cda0592ac	2	12	N (, , ,) An old file with limited detection.
55ee25ea8a059994c9f1f672228171b6	1	0 ***NEW	Y (w32/sdbot.aefv w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
9b175f5f727bcf1153e1aaf99798556a	1	0 ***NEW	Y (w32/trojan-sml-sdcw!eldorado , Email-Worm.Win32.Updater.j , ,)
c2e9a9884a40f242bac1d7d9fe39056d	1	1	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
730498b8a6c676e2298d9b1ad7dd5d10	2	0 ***NEW	Y (w32/hll-sysdlrsharer!eldorado , Trojan-Downloader.Win32.Agent.bqkb , ,)
6d67beaffa64cd2f48d18269f3eb0966	1	0 ***NEW	N (, , ,) No information.
f8815cdca238ad5ab566f05f5a6335a4	2	3	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.voe , ,)
a64468ee57881595746501de90106fcf	1	0 ***NEW	Y (w32/emailworm.hqk , Net-Worm.Win32.Allaple.e , ,)
1295ae75e1d25a057bb6303e2040100d	1	0 ***NEW	Y (w32/virut.7116 , backdoor.win32.rbot.adqd , ,)
88ae2e29394f5b89329df4d483c0c9c7	1	0 ***NEW	N (, , ,) A new file with limited detection.
865915650a85e7c27cdd11850a13f86e	1	16	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
952098cf3c65cfcb52282d8959ddffd3	1	4	Y (W32/Allaple.H , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
1d419d615dbe5a238bbaa569b3829a23	3	6	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
15965bb88165d1eb06851d8f076130ba	1	18	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
3875b6257d4d21d51ec13247ee4c1cdb	1	36	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663 ,)
cb576cca04946b3d0829703d108ae270	1	17	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
10980f4df2060b86a72eb5e533102980	1	3	Y (w32/backdoor2.dstk , Backdoor.Win32.IRCBot.jwy Worm.Win32.AutoRun.tet , W32Ircbot!I484 ,)

Two of these files have appeared 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

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/