Yui Kee Computing Ltd.

Newsletter

August 2013

Contents

Bogus Wing Hang Bank Website Shut Down

<web-link for this article>

The Hong Kong Monetary Authority has an alert about fraudulent website www.wghgbkhk.com, which resembled the official Wing Hang Bank site. The bank has clarified it has no connection with the bogus site and the site has been taken down.

The Police are investigating, anyone who has provided personal information to the website or conducted financial transactions through it should call the bank on 3199 9188 or the Police on 2860 5012.

More Information

Alert issued on bogus website
Fraudulent website: www.wghgbkhk.com

August Honeypot Report

<web-link for this article>

Technical problems prevented the publication of a June report. This is the nineteenth 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 remains at a low level.

Average Time To Infect: 30 hours

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 : 24
- 6 are brand new to this honeypot.

Source of Attacks

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

7	United_States
3	China
3	Taiwan
2	Japan
2	Venezuela
1	Russia
1	Germany
1	Israel
1	Netherlands
1	Spain
1	Sweden
1	Vietnam

Malware

Checksum (md5)	This month	Previous count	Detection*
0152fe5f6bd7ca1a99d3cfbfe7da45fc	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado ,Net-Worm.Win32.Allaple.b , ,)
3875b6257d4d21d51ec13247ee4c1cdb	3	50	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
9107c0f3a3749f4495e190a790bda964	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
f4f4a89637f123324efcad3e4225edfe	2	X	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
fc09612173236ba724837546ef2b5f82	1	0 ***NEW	Y (w32/virut.7116 , backdoor.win32.rbot.adqd , ,)
0f51974913a4f5be110ab1069c93e13f	2	X	Y (W32/Virut.AG , , Backdoor.Win32.Rbot.adqd ,)
405594052cc451d83c1bb33bf8df6846	1	0 ***NEW	Y (W32/Endom.A , Net-Worm.Win32.Allaple.a , ,)
644ea081625064565c7e9816f235f264	1	1	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
dca8713db4f5b7b84a66b51d925e7f9c	1	3	Y (w32/sdbot.aefv , Virus.Win32.Virut.n Backdoor.Win32.Rb ot.vqt , ,)
64b4345a946bc9388412fedd53fb21cf	1	1	Y (W32/Trojan-Sml-SDCW!Eldorado , Email-Worm.Win32.Update r.k , ,)
6e92036c8ed5b0824f9ba48ae4922ed1	1	0 ***NEW	N (, , ,)
b37f561aaa4cd24259197f3cd228eae7	1	3	Y (W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)
532a46e3f70dc640344f68e9c3908d90	1	2	Y (w32/virut.7205 , Backdoor.Win32.Rbot.adqd , ,)
fd28c5e1c38caa35bf5e1987e6167f4c	1	1	Y (W32/Trojan5.DCW w32/backdoor.zzr , Net-Worm.Win32.Kola bc.dls Backdoor.Win32.Rbot.aftu , ,)
ac78b607517e12904fc29d2582571b11	1	2	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
c5ff7232868333107fa3efe895f12361	1	4	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
1f8a826b2ae94daa78f6542ad4ef173b	1	7	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.phv Backdoor.Win32.Rbot.ion , ,)
6f06e39cb6df0908d5ab6e661c6b0386	1	2	Y (W32/Sdbot.OTR , Backdoor.Win32.Rbot.adqd ,)
382fdcff132b058cfe50065b84fd8a4c	1	2	Y (w32/virut.7116 W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)

c97f4c7d3ed204c21225432e4c4be6af	1	0 ***NEW	Y (W32/Trojan.MEX , Backdoor.Win32.Rbot.bni , ,)

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

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/