Yui Kee Computing Ltd.

Newsletter

February 2012

Contents

Internet Society Hong Kong Publishes 30 Second Information Security Clips

<web-link for this article>

The Internet Society of Hong Kong is promoting information security through a series of thirty second infosec video clips. The clips will be shown on Roadshow, a video service available on many Hong Kong buses. The videos feature Roy Ko of Hong Kong CERT, Chester Song and other well-known figures in HK's infosec scene. The clips are only available in Cantonese.

More Information

香港互聯網協會 - 資訊保安小貼士系列 (主持: Chester Soong 及 Sang Young. ISOC HK) RoadShow

February Hong Kong Honeypot Report

<web-link for this article>

This is the second 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.

Average Time To Infect: 13 Hours 39 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. A few minutes longer than January.

Summary

- Total number of attacks : 51
- 23 are brand new to this honeypot.
- 7 of these files have not been seen in other honeypots

Source of Attacks

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

Number of attacks	Source
18	Hong_Kong
16	United_States
2	Poland
2	Russian_Federation
2	Taiwan
1	Kazakstan
1	Estonia
1	Switzerland
1	Colombia
1	Malaysia
1	Netherlands
1	Germany
1	Japan
1	Canada
1	Gabon
1	Latvia

In a large change from last month, Hong Kong is the largest source of attacks. It seems too early to draw any conclusions from this.

Malware List

Checksum (md5)	This month	Previous count	Detection
566400d3216495f8c50ced8ddb088763	4	0 ***NEW	Y (W32/GenBl.566400D3!Olympus , UDS:DangerousObject.Multi.Generic , ,)
d3e1d87e83ed88aa3af137dda0fba87d	1	0 ***NEW	Y (w32/virut.7116 , virus.win32.virut.av , ,)
3875b6257d4d21d51ec13247ee4c1cdb	4	13	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
1a50b8f81ef6c9d27c4d97e59cb85e9e	7	0 ***NEW	Y (W32/GenBl.1A50B8F8!Olympus , Trojan.Win32.Jorik.IRCbot.hce , ,)
65c7bab2353e3c8a320e045d142ac976	1	0 ***NEW	Y (W32/GenBl.65C7BAB2!Olympus , Backdoor.Win32.Floder.gmq , ,)
f480ea8d14656480ff8b1e95c891ead8	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)

ad5d79b867875b98278118c70ea102c4	2	0 ***NEW	Y (w32/heuristic-kpp!eldorado , Trojan.Win32.Pincav.bbwc , ,)
b6cb9535a3c0e22137850f07460b510b	1	0 ***NEW	Y (w32/rbot.b.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
aae0f083745d16fe487c26844a50fa1c	1	0 ***NEW	Y (w32/trojan.mex , Virus.Win32.Virut.n Backdoor.Win32.Rbot.bni , ,)
9956071ca816c9145cb979c329c12a56	1	0 ***NEW	Y (w32/virut.7116 w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd , ,)
ced2ed2358f1fb56051d50f97229bfca	1	0 ***NEW	Y (w32/virut.7205 , Net-Worm.Win32.Allaple.e virus.win32.virut.bl , ,)
a903cc0344815191292c2f336df3e67a	4	0 ***NEW	N (, , ,)
0656e272e85a25caaece4591e24b4d35	5	2	Y (w32/conficker!generic , net-worm.win32.kido.ih , ,)
3e2085f27f837bcdf79a487395be20b4	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
81f65b31e6de6fe8abbf1195037e8414	1	0 ***NEW	N (W32/EmailWorm.HQK, Net-Worm.Win32.Allaple.b, ,)
527446f0af11fdbae209993477730f42	1	0 ***NEW	N (W32/EmailWorm.HQK, Net-Worm.Win32.Allaple.e , ,)
9be443d09b25157fcfbccb953f4a2cd4	4	0 ***NEW	N (, , ,)
7dad62d3ca84fcb56d9b2c9cafb65f90	1	0 ***NEW	N (W32/RAHack.A.gen!Eldorado, Net-Worm.Win32.Allaple.b , ,)
723e9315cdf986dae03e0a4500a2d1f2	1	1	Y (w32/virut.7116 w32/sdbot.aefv, Backdoor.Win32.Rbot.adqd , ,)
c84b0dbc5eeb6616553fa3aa7851c188	1	0 ***NEW	Y (W32/Virut.7116, Backdoor.Win32.Rbot.adqd , ,)
964ce9d8a0ce764061aaef080e550ffd	1	0 ***NEW	Y (W32/GenBl.964CE9D8!Olympus, Email-Worm.Win32.Agent.lp , ,)
d840d16176d2a34e8661e3340e263721	1	0 ***NEW	Y (w32/trojan2.kexn , Trojan-Spy.Win32.Agent.bmxb , ,)
33959bb2c48363ddd3637ea78c048b6c	2	0 ***NEW	Y (w32/sdbot.aefv , Virus.Win32.Suspic.gen Virus.Win32.Virut.n , ,)
2ba462c1230e9c6cf7ae06f09668c10a	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado, Net-Worm.Win32.Allaple.b , ,)
d905dafa06c4cd5d732e05a3b74a09c7	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado, Net-Worm.Win32.Allaple.b , ,)
4ed217391b897fc2d46ec9ce8af282cf	1	1	Y (W32/Virut.AG , Backdoor.Win32.Rbot.adqd , ,)
fed9acb515b6b61d60921a93ddf40057	1	0 ***NEW	Y (W32/Virut.7116, Backdoor.Win32.Rbot.adqd , ,)

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/