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

Yui Kee Computing Ltd.

Newsletter

January 2012

Contents

Journalist Sneaks Through Government Biometric Border Check

<web-link for this article>

A journalist from the Chinese-language Hong Kong newspaper Mingpau Daily reported using a fake thumbprint to fool the reader at the Hong Kong-China border control.

Hong Kong residents carry a "smart identity card" that stores thumbprint data. This can be used for self-service entry or exit from Hong Kong at any immigration control point. There are 391 so-called e-Channel devices distributed at the control points. To use the e-Channel, a person inserts their smart identity card into the card reader and the e-Channel gate doors will open. After entering the e-Channel, the person places their thumb flat on the centre of the fingerprint scanner, the print is recognised, matched with the ID card, and the exit opens.

In this case, the journalist reports using a fingerprint casting kit, bought on a popular Chinese auction website for HK$110, to produce the fake print. The journalist then tested five e-Channel devices at the Lo Wu and Lok Ma Chau border crossing points and found one device accepted the fake on two occasions.

The Immigration Department is following up the report and checking whether it was an isolated technical problem at just that device. The Department routinely tests the devices after maintenance and before they are put in service.

The e-Channels are used daily by thousands of people, and ease border crossings. However, this is a reminder that even well-maintained, well-tested equipment, that has been built to robust standards for high-volume usage can develop subtle faults. The reliability of the common, cheap, untested, unmaintained fingerprint readers used in many consumer-level "secure devices" must be questioned.

More Information

誤認假指紋 e 道機停用
Immigration Clearance through e-Channels
Report: Hong Kong-China border biometrics device spoofed

January Hong Kong Honeypot Report

<web-link for this article>

Near the end of 2011, West Coast Labs and Yui Kee Computing arranged for a honeypot to be installed on a Hong Kong IP address. Since then, it has been collecting malware and feeding in to West Coast Labs' research as one point in their global network of honeypots.

Yui Kee is now receiving a monthly report from this honeypot, and this will become a regular feature of the newsletter. The report may give 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 32 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 : 55

□ 37 are brand new to this honeypot. No file that attacked the honeypot in an earlier period has done so again.

□ 13 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	United_States
12	Japan
5	Taiwan
3	China
3	France
2	Latvia
2	Slovakia
2	Russian_Federation
1	Vietnam
1	unknown
1	Malaysia
1	Hong_Kong
1	Italy
1	United_Kingdom
1	Philippines
1	Bulgaria

The first report from this honeypot (not published) showed a predominance of attacks from local, Hong Kong IP addresses. As the address has become more widely known, the pattern of sources of attacks is becoming more global and closer to patterns seen elsewhere. Initially the majority of attacks come from the host country or region, normally expanding outwards during the life of the honeypot.

Malware List

Checksum (md5)	This month	Previous count	Detection
961dcb5a7c03b7f9acceab3e7e66c134	2	0 ***NEW	Y (w32/virut.7116 , virus.win32.virut.av , ,)
a71a59321a4860eb1410caface608964	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
a9bc9fe2f0425a9bb708e9b206313325	1	0 ***NEW	Y (w32/sdbot.aefv , , ,)
6285dd99fa8a01c461b6ea76bed71062	1	0 ***NEW	Y (w32/sdbot.aefv W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)
6a1132597dc25097807f73f30f36460d	1	0 ***NEW	Y (w32/genbl.6a113259!olympus , , ,)
f5204d5684b8090f09d89dd853ae4f82	1	0 ***NEW	Y (w32/virut.7116 w32/sdbot.aefv , backdoor.win32.rbot.adqd , ,)
723e9315cdf986dae03e0a4500a2d1f2	1	0 ***NEW	Y (w32/virut.7116 w32/virut.7116 w32/sdbot.aefv w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd Backdoor.Win32.Rbot.adqd , ,)
4a00614bfa7ab6042d540585f6dacf3c	3	0 ***NEW	Y (, Trojan.Win32.VBKrypt.irsc , ,)
df06c908c96c0929d8e2864c10998dea	1	0 ***NEW	Y (w32/sdbot.aefv W32/Sdbot.AEFV , Type_Win32 Trojan.Win32.Agent.ayuc , ,)
79655dbb36eb8fd7ab5f650471a48589	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.e , ,)
c2e282011574730502bd8def5bec77cc	1	0 ***NEW	Y (w32/injector.a.gen!eldorado W32/Injector.A.gen!Eldorado , Net-Worm.Win32.Allaple.e , ,)
0b4410d02a1a59a7d8c458841a8237c0	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.b , ,)
a594fb8abc907dd1683a0f7ee3447216	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.b , ,)
b4d9dd3a19e7fdd2211d81983f8e4d75	1	0 ***NEW	Y (w32/allaple.h w32/allaple.h , Trojan.Win32.Genome.rioo trojan.win32.genome.rioo Net-Worm.Win32.Allaple.e , ,)
a1f0861827129f39cfbd0f0a135f7023	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.b , ,)
979ed4871eb7ca2dad69c48cd924f4d5	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
755a34c24864f112a03849d72576e919	1	0 ***NEW	Y (, Trojan-Dropper.Win32.Injector.bslj , ,)
604caa2c37697b38a7dffad5b0157188	1	0 ***NEW	Y (w32/emailworm.hqk , Net-Worm.Win32.Allaple.e , ,)
ef60b77f16ae9433c0d03d432b280ee2	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
3875b6257d4d21d51ec13247ee4c1cdb	3	0 ***NEW	Y (w32/sdbot.aefv w32/malware!44f4 W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
2c7235f22ba58362cd4c9a2a03de252b	1	0 ***NEW	Y (w32/sdbot.aefv , Backdoor.Win32.Rbot.bni backdoor.win32.rbot.bni , ,)
38d5dc01cb67aadc2312a3821c4296a8	1	0 ***NEW	Y (w32/emailworm.amv , Net-Worm.Win32.Allaple.d , ,)
cf2b32e03d8985fc0b0afc55703850bf	1	0 ***NEW	Y (, Trojan.Win32.Jorik.Poebot.bt , ,)
4af7d99a78285487e6420f13ad92411c	1	0 ***NEW	Y (w32/virut.7116 w32/virut.7116 w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd Backdoor.Win32.Rbot.adqd , ,)
2cd9ae8e4c3b7fd697da8f2b67c20aea	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd backdoor.win32.rbot.adqd , ,)
85e64a8450070e7592fb53f7b275d386	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
aee462ee2a64cbffc46250bdb6b2e23d	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
8c6b3f437df9b0acb522093577d4a623	1	0 ***NEW	Y (w32/sdbot.aefv w32/virut.7116 , Backdoor.Win32.Rbot.adqd Backdoor.Win32.Rbot.adqd , ,)
d7fe7b4fee72c3bdb9a95a3328729417	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)

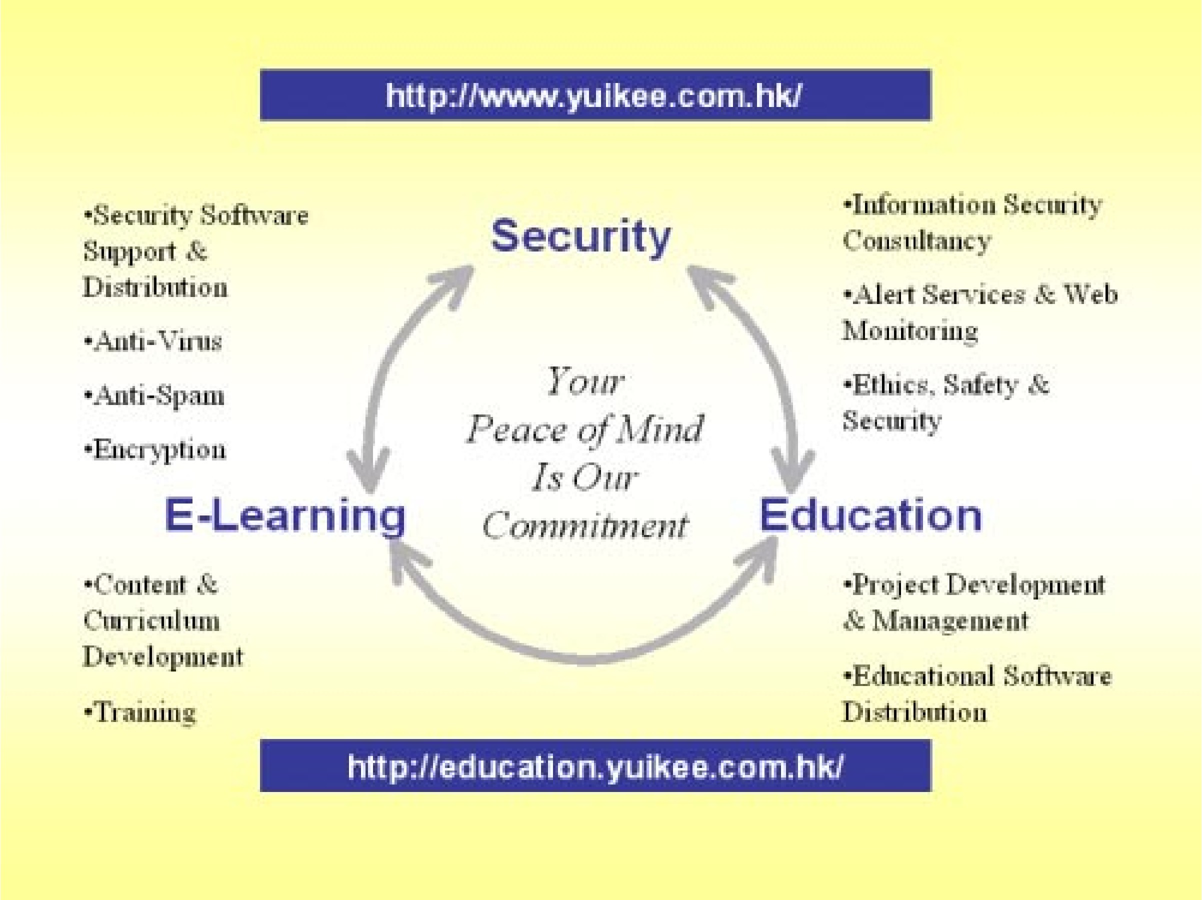
b43ad71209c5100b9ed71edb10041514	4	0 ***NEW	N (, , ,)
d41d8cd98f00b204e9800998ecf8427e	4	0 ***NEW	N Invalid file.
d36259c772f30258b31f42c6e1c99c8e	1	0 ***NEW	Y (w32/endom.a , Net-Worm.Win32.Allaple.a , ,)
5c6b2ca56695b63a18c3bd22fd006b69	1	0 ***NEW	Y (w32/allaple.c , Net-Worm.Win32.Allaple.b , ,)
55d4cabac53b6e8928f8e8f3ecf74293	1	0 ***NEW	Y (, Trojan.Win32.VBKrypt.ixcs Net-Worm.Win32.Kido.ih , ,)
94906386c37964fa58e2dc35e73c4080	1	0 ***NEW	Y (, Trojan.Win32.VBKrypt.ivyt Trojan.Win32.VBKrypt.ivyt , ,)
23afd4ad06d26f6442fa06f4ec944513	8	0 ***NEW	N (, , ,)
f5fbd1189db83db22d7e6cdb55eed193	1	0 ***NEW	Y (w32/injector.a.gen!eldorado w32/injector.a.gen!eldorado W32/Backdoor!d75d , 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.

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

•Content & Curriculum Development

•Training

Education

•Project Development & Management

•Educational Software Distribution

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