Yui Kee Computing Ltd.

Newsletter

December 2013

Contents

November Honeypot Report

<web-link for this article>

This is the twenty-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. The number of attacks has increased slightly.

Average Time To Infect: 37 hours 12 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 : 20
- 9 are brand new to this honeypot.

Source of Attacks

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

4	Macedonia
4	United States
2	Bosnia
2	Canada
2	Italy

1	China
1	Czech Republic
1	Indonesia
1	Russia
1	South Korea
1	Thailand

Malware

Checksum (md5)	This month	Previous count	Detection*
3875b6257d4d21d51ec13247ee4c1cdb	2	55	W32Rbot!I2663.exe ,Backdoor.Win32.Rbot.bni ,W32/Malware!44f4 W32/Sdbot.AEFV ,
64b4345a946bc9388412fedd53fb21cf	2	2	,UDS:DangerousObject.Multi.Generic Email-Worm.Win32.Updater.k Email-Worm.Win32.Updater.n ,w32/trojan-sml-sdcw! eldorado ,
c1989130056c32fa305e3de57f6f40f1	1	2	,Backdoor.Win32.Rbot.bni Virus.Win32.Virut.n ,W32/Trojan.MEX ,
6527ce860cd40ceda4e2a81782d46c2c	1	1	,Backdoor.Win32.Rbot.adqd ,W32/Sdbot.AEFV ,
a650c67e14cfb27879999036741478d5	1	1	,backdoor.win32.ircbot.jwy ,w32/backdoor2.dstk ,
0d4d64321a77e17c1637ef3b30290b31	1	0	,net-worm.win32.allaple.e ,w32/emailworm.hqk ,
952098cf3c65cfcb52282d8959ddffd3	1	9	,Net-Worm.Win32.Allaple.e Trojan.Win32.Genome.rioo ,W32/Allaple.H ,
741b9ecd6367ac9cbba5613cedaf53ea	1	0	,,, script file
c0276991baff7a50b6f774d7055c440b	1	1	,Net-Worm.Win32.Allaple.e Virus.Win32.Virut.n ,W32/Allaple.H ,
514ffff11e40ad60e1f58aa3f53facb7	1	0	,net-worm.win32.allaple.e ,w32/allaple.a.gen!eldorado ,
93b587a0f0652b17ed82846c83ef4aa5	1	0	,Backdoor.Win32.Rbot.adqd ,w32/virut.ag ,
b0599b847e5df4109e7a0e4ad883e00e	1	1	,Virus.Win32.Virut.at Net-Worm.Win32.Allaple.e ,W32/Virut.AG ,
8d9a4ff99fcb614b99d572e06a2a3d1a	1	1	,Backdoor.Win32.Rbot.adqd ,w32/sdbot.aefv w32/virut.7205 ,
c4f15c18c89c10df6fe5e01a2b678b3b	1	0	,Backdoor.Win32.Rbot.bni ,w32/rbot.b.gen! eldorado ,
a20d698fd1ff4c80dfc8096bfdd1f2ba	1	0	,net-worm.win32.allaple.e ,w32/emailworm.hqk ,
ac8a744e25af311cf1d07f2ca23306e2	1	0	,,, script file
3608f0fa72c8a01f39311511658b0d18	1	0	,virus.win32.virut.at net-worm.win32.allaple.e ,w32/virut.ag ,
2f6d1fbc05d0166c8f69242e8435dae7	1	0	,net-worm.win32.allaple.e ,w32/allaple.a.gen!eldorado ,

The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

Where an X is shown under Previous, the file has been seen before in this honeypot but the relevant logs are not available.

More Information

West Coast Labs
January Hong Kong Honeypot Report

Ten Arrested for Pirated Software

<web-link for this article>

Hong Kong Customs officers have arrested eight men and two women aged from 25 to 56 for using pirated computer software in the course of business. In the crackdown on software piracy in commercial organisations, Customs officers searched the offices of seven companies, including engineering, design, advertising, printing and catering businesses.

Officers seized 85 computers with suspected pirated software valued at about HK$360,000 installed, including operating system and office application software.

At a press conference on 22 December, Michael Kwan, head of the Intellectual Property Investigation (Operations) Group reported that the department had received 92 complaints about corporate software piracy from January to November this year, a slight increase from 87 in the same period last year. Mr Kwan also encouraged the public to report software piracy activities.

The Hong Kong Government provides various information about intellectual property law and how to comply with it, including an introduction to intellectual property protection and Guidance on Prevention of End-User Piracy in Business (PDF).

More Information

Guidance Note on Prevention of End-User Piracy in Business
Pirated software crackdown nets 10
Intellectual Property Protection

Who is Enabling State Surveillance?

<web-link for this article>

Allan Dyer

In October, cryptography expert Bruce Schneier and 24 others challenged the anti-virus industry to come clean about their involvement in government surveillance, which makes the recent revelation by Edward Snowden that the NSA paid cryptography company RSA US$10 million to make a weak algorithm the default in its products somewhat ironic. Perhaps the cryptography industry should be asking about its own ethics instead?

The questions that the open letter asked were:

1. Have you ever detected the use of software by any government (or state actor) for the purpose of surveillance?
2. Have you ever been approached with a request by a government, requesting that the presence of specific software is not detected, or if detected, not notified to the user of your software? And if so, could you provide information on the legal basis of this request, the specific kind of software you were supposed to allow and the period of time which you were supposed to allow this use?
3. Have you ever granted such a request? If so, could you provide the same information as in the point mentioned above and the considerations which led to the decision to comply with the request from the government?
4. Could you clarify how you would respond to such a request in the future?

I did not respond to the letter in October, because it was specifically directed at anti-virus developers, and while Yui Kee sells and supports anti-virus software, we do not develop it in-house so the answers would not have been useful. However, I would like, now, to discuss the different considerations affecting cryptography and anti-virus developers. I think that

cryptography development is a lot more susceptible to government manipulation than anti-virus development.

We have had this discussion before

In late 2001, it was revealed that the FBI had developed keystroke-logging software, called Magic Lantern and anti-virus companies were asked if they could or should detect it. Marc Maiffret of eEye responded, "Our customers are paying us for a service, to protect them from all forms of malicious code. It is not up to us to do law enforcement's job for them so we do not, and will not, make any exceptions for law enforcement malware or other tools."

That response is very similar to RSA's denial of the current allegations on 22 December, "we have never entered into any contract or engaged in any project with the intention of weakening RSA's products, or introducing potential 'backdoors' into our products for anyone's use". Both essential say, "we don't do that, we're the Good Guys", which may be true, but do you believe them?

Graham Cluley of Sophos, had a much better response, "We have no way of knowing if it was written by the FBI, and even if we did, we wouldn't know whether it was being used by the FBI or if it had been commandeered by a third party". This gets to the heart of the matter, if the product detects the "Government Approved Malware", it doesn't know who's controlling it. The criminals would be racing to find some way of subverting it, or developing something that looks close enough to be ignored.

What has changed since Magic Lantern?

A lot. In 2001, we were near the beginning of malware for criminal gain, there had been the largely unsuccessful AIDS trojan in 1989, and the term phishing had been coined in 1995, but the main growth was after 2001. The number of malware types has exploded, from about 50,000 in 2000 to millions today. The volume of samples that developers receive is staggering, hundreds of thousands per day.

This has forced malware analysis to become a highly automated team effort. Many anti-virus developers have established analysis labs in multiple jurisdictions to "follow the sun". Microsoft has a lab in Ireland; Kaspersky has researchers in Romania, Germany and Russia; Sophos has labs in Australia, Hungary, England, and Canada; F-Secure has labs in Finland and Malaysia.

The difference between subverting Cryptography and subverting Anti-Virus

To successfully subvert the market-leading anti-virus product, let's call it X, a government agency simply has to persuade the developers to not detect the government malware. A modern product uses multiple methods to examine software: virus specific scanning (commonly called signature scanning, but that is not a good name for it), heuristics, a sandbox with behaviour analysis, and perhaps a host intrusion prevention system (HIPS). These are updated multiple times daily. Avoiding the virus-specific scanning is relatively easy: if the malware is unknown, it is not detected. However, any update might bring a new rule or behaviour that picks out the malware as suspicious. In order to stay undetected, the malware needs to be whitelisted, so the government agency will need to give the anti-virus developer a sample to be stored in the database of "known good" software. So any researcher in the company will be able to access the government malware, and see the reason (or lie) why it was added to the database. What are the chances that one of them will have a different agenda to the government agency? Benjamin Franklin said, "Three can keep a secret, if two of them are dead".

But it gets worse for the government agency because anti-virus companies share malware samples. The developers recognise that this improves the protection they can give their customers. The competition is in detection, not collection. If any other developer obtains a sample of the government malware, they will share it like any other sample and the chances of someone realising that X is misbehaving rise. When someone reverse-engineers X and finds that obviously malicious code has been whitelisted, trust in X plummets, it is no longer the market-leader, and conspiracy-theorists have a smoking gun with government fingerprints.

On the other hand, cryptography software is developed by a relatively small team, probably in one location, and not updated daily. It can be subverted in quite a subtle way, perhaps by a single key person suggesting a default algorithm that is generally thought to be good, but which the government agency knows has a weakness. That key person might not even realise they have acted to weaken their product. If the weakness is discovered later, the developer has complete deniability, unless there is a whistle-blower inside the government agency. This scenario may sound familiar.

The Stuxnet Lesson

There is no such thing as perfect anti-virus. We have know this since Frederick Cohen wrote his mathematical proof. Knowing this, anti-virus developers strive to provide the best protection in a real-world environment. Stuxnet reconfirmed the non-perfection of anti-virus, but it also provided a blueprint for using malware to penetrate any system. This includes using zero-day exploits for breaking into systems, careful testing, and very specific targeting. Done right, it is possible to avoid notice by anti-virus developers for years. Stuxnet only got noticed when it spread beyond its intended targets.

The lesson for the government agency is obvious: don't tell the anti-virus developers, just make the stealthiest malware you can and limit its spread to your particular targets. If it eventually gets detected, deploy the new malware you've been developing.

My Answers

For completeness, even though questions intended for anti-virus developers are not strictly applicable to me, my answers to the fours questions in the open letter would be: 1. No, 2. No, 3. No, 4. I would say, "Have you any idea how dumb that is?" and point them to this article.

I was not paid to write this by a government agency, but I would say that, wouldn't I?

More Information

Letter to antivirus companies
Dear AV provider: Do you enable NSA spying? Yours, EFF
Exclusive: Secret contract tied NSA and security industry pioneer
Mikko Ashamed
Magic Lantern (software)
FBI ‘Magic Lantern’ reality check
How much did NSA pay to put a backdoor in RSA crypto? Try $10m – report
RSA comes out swinging at claims it took NSA's $10m to backdoor crypto
RSA Response to Media Claims Regarding NSA Relationship
AIDS (Trojan horse)
Stuxnet: How USA and Israel created anti-Iran virus, and then lost control of it
Trojan-Dropper:W32/Stuxnet
Flame, Failure of the Antivirus Industry and Cyber Cold War
Case Flame
Critical Questions on Critical Infrastructure
Broken Security Models

Police and Youth Groups Pilot Cyber Crime Prevention Service

<web-link for this article>

The Hong Kong Police and the Hongkong Federation of Youth Groups have launched the Project iSmart crime prevention programme. The programme uses short films based on real-life stories to educate youngsters, and a referral service from the Police to youth workers to help victims.

The films will be uploaded to the Youth Law website and broadcast in public places to raise awareness. Sadly, the website is only available in Chinese, so it neglects the needs of ethnic minority youths.

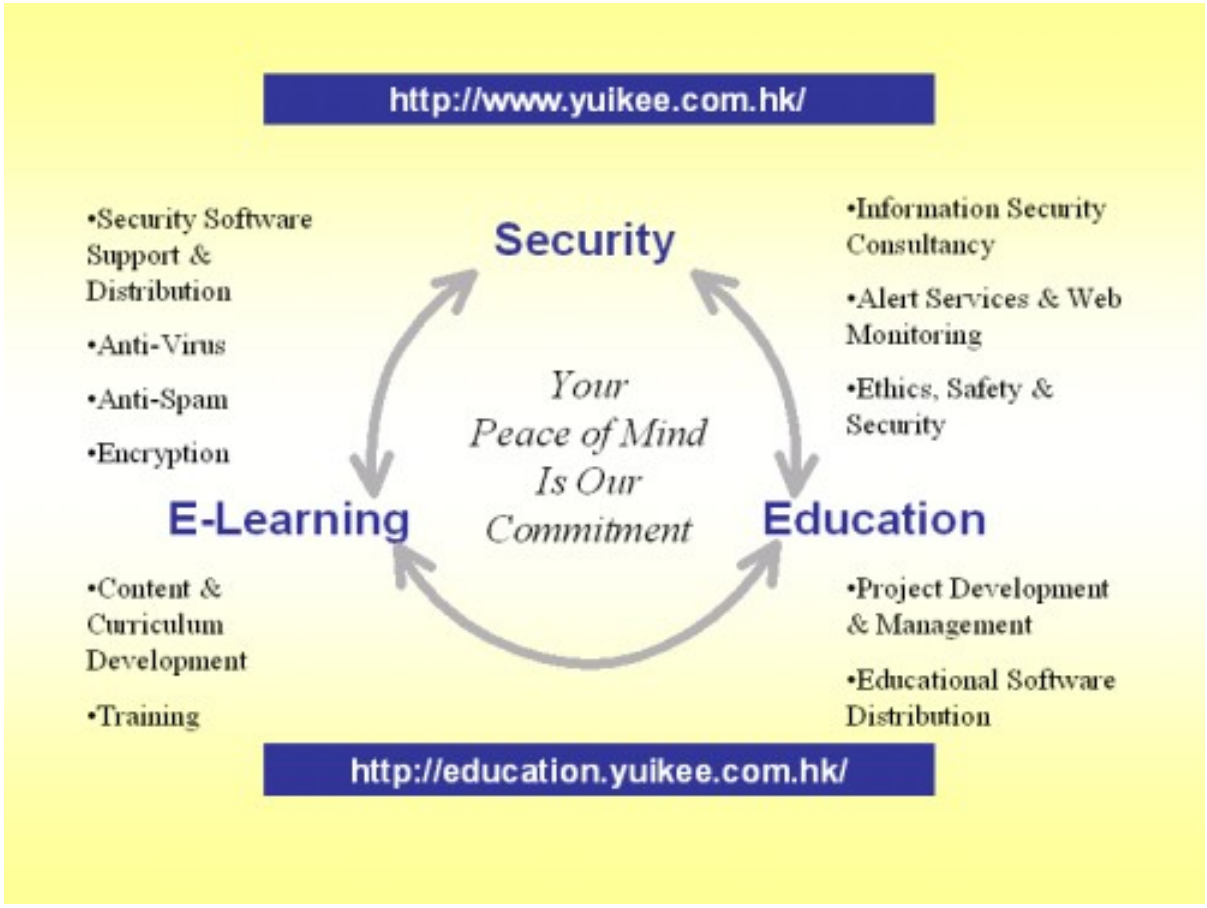
The referral service provides an early intervention for people under the age of 24. Police responding to reports and during other duties will identify young potential cyber crime victims and, with consent, will refer them to the project's youth workers for assessment and follow-up action. A 6 month pilot service will start on 1 January in the Tsuen Wan and Kwai Tsing Districts and the service might then be extended to other districts.

More Information

Cyber crime prevention plan launches
香港青年協會青年違法防治中心青法網

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/