Yui Kee Computing Ltd.

Newsletter

May 2012

Contents

HKCERT Raises Global Profile

<web-link for this article>

Last month, Hong Kong Computer Emergency Response Team (HKCERT) was celebrating the opening of its new centre, this month centre manager Roy Ko is interviewed by international IT industry news website The Register.

In the interview, Mr. Ko explained how the CERT was responding to the changing nature of incidents and taking a more proactive approach. HKCERT already checks all .hk sites for suspicious activity, notifying owners to clean up malware in their machines, and it plans to expand this to .com and .org addresses based in the region. HKCERT uses third party information sources and it is planning to deploy its own sensors, and to systematise and automate the process. He recognised that the CERT needs to expand the scope of their service, especially in the areas of monitoring, early analysis and preventative work, but HKCERT has a very small team compared to other CERTs.

Nevertheless, HKCERT takes an active role in the wider IT security community, liaising with the police's Technology Crime Division and the government's Office of the Government Chief Information Officer (OGCIO) and further afield, fellow regional CERTs, including the very well funded mainland China CERT, headquartered in Beijing and industry contacts. This type of cooperation was effective in April 2010 when HKCERT was instrumental in the takedown of Koobface servers in Hong Kong. The Koobface gang rapidly moved their hosting to mainland China, but that just highlights the need for better cross-border cooperation.

Not everyone fully recognises the importance of strengthening HKCERT, talking to The Register, IT Subsector Legislative Councillor Samson Tam recently emphasised the

importance of increasing resources for the Technology Crime Division, but failed to mention HKCERT.

More Information

- Hong Kong CERT wants bigger team to tackle cyber threats
- New HKCERT Centre Opens to Combat Emerging Cyber Threats
- A Milestone of HKCERT
- The Register
- Koobface server pops up in China after HK takedown

Chinese Passwords

<web-link for this article>

Allan Dyer

Sitting on a panel at an information security conference in Hong Kong recently, we were discussing our view of the security challenges that Asian businesses face, including cloud services, mobile devices, Bring Your Own Device (BYOD). Then we had a question from the audience, "Why can't we use Chinese (and Japanese or Korean) characters in our passwords?" This was a change of gear, we were debating enterprise strategy, and parts of the audience were down at the grass roots.

The question is easy to dismiss as naive, but we should listen to our users, and try to understand the deeper meaning and requirement. Perhaps the message behind that question is that users know they can choose stronger, more memorable passwords in their own language. I would be sceptical about that as a general rule - if someone uses their pet's name as a password it is not going to be any more secure by typing it in Chinese, but helping some users become more secure is an improvement.

My initial reaction was that there are serious practical constraints. Chinese users usually enter text by multiple keystrokes based either on the pronunciation of the words, or on the components of the written characters, but there are many different schemes or input methods. If you have ever tried entering your password without realising Caps Lock was on, you will have some idea of the confusion that could result when the user needs to choose between multiple input methods. Also, the final selection of the character is often from a pop-up list, making shoulder-surfing easy. An alternative is written entry, using a touchpad, but the strokes are often displayed on-screen, again allowing shoulder-surfing. In any case, most systems are simply not set up to accept Chinese text entry at password prompts. A system administrator would be wise to carefully consider all the implications of doing that, would it enable shoulder-surfing?; would there be excessive support calls?; what are the compatibility issues?

End-User Approaches

What if an end-user wants to use a Chinese password, but their systems administrator has, for whatever reason, not provided a method? One way would be to use the keystrokes for an input method, and ignore the final character selection, but this would significantly reduce the entropy of the resulting password: several characters would map to the same keystroke sequence.

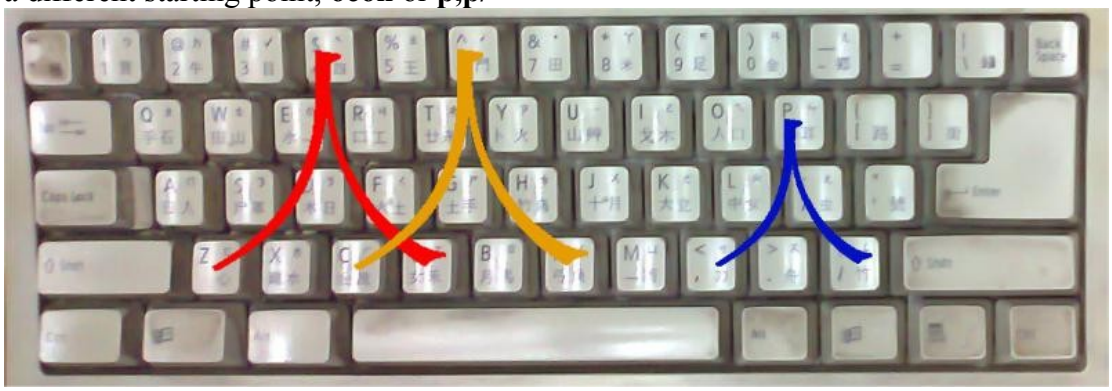
One method I sometimes use for simple 4 to 6 digit PINs is to remember the *shape* the digits make on the keypad. Six digits is probably the limit for this, I'm not good at remembering complex shapes. But, of course, Chinese readers have already memorised thousands of complex shapes, could they use those?

A Suggestion

This is not a method I would use, and it would probably need more refinement before being usable, but I invite feedback from anyone who wants to try it.

1. Choose a phrase of several Chinese characters

2. Take the first character, and imagine it drawn on your keyboard, press the keys corresponding to the stroke ends, for example, 人 could become **4z4v**, or, if you chose a different starting point, **6c6n** or **p,p/**



3. Repeat for the remaining characters of the phrase.

   The passphrase then depends on the characters chosen and where they are placed on the keyboard.

   Naturally, more complex characters like 米 or 馬 can be used, becoming, perhaps, **4cwt3e5rrzrv** and **707h8juouohl,bnm,** respectively.

   But some characters, like 麟 seem just too complex.

The advantages and disadvantages:

- Easy of memorisation: a few characters and positions on the keyboard

- Good length: a three character phrase might become 48 keystrokes
- No dictionary words
- The stroke order of Chinese characters might make some key sequences much more likely, reducing the entropy of the final password
- Because the user does not remember the actual keys pressed, changing to a different keymap (e.g. QWERTY to Dvorak) would prevent user access

Well, that's the idea, let me know if you try it.

July 9th is Death of the Internet Day for 1200 Hong Kong Users

<web-link for this article>

What would you do if you suddenly could not access the internet? No email, no web, just mysterious error messages. According to a spokesman for HKCERT, this might happen to around 800 to 1200 computers in Hong Kong on 9th July 2012.

Calling a technical friend, or your ISP would probably be high on your list, but you probably would not think to blame Estonian cyber-criminals who were arrested in November 2011. The arrests last year were the culmination of an investigation that started in 2006. The criminals were spreading malware known as Trojan:W32/DNSChanger, and building a network of infected computers. The infected computers were used for various lucrative activities including click fraud, selling dodgy pharmaceuticals and selling fake antivirus software. As its name suggests, the DNSChanger malware altered the Domain Name Server (DNS) settings on infected computers, pointing them at the criminal's servers so that, whenever any internet address was used, the criminals could control what site was reached. They could replace advertisements on sites victims visited, generating more income for themselves, install more malware, and prevent victims reaching genuine security sites.

The suspects were arrested and the controlling computers seized last November, so why is there still a problem? Every one of the about 4 million infected computers worldwide was still looking up every internet address using the rogue DNS servers. Shutting down the servers would have immediately "killed the internet" for them. Therefore, the FBI formulated a plan and obtained permission to continue running the servers (now providing good information) while efforts were made to contact the victims and clean up the infected machines. The initial permission lasted until 8th March 2012, but this was later extended until 9th July 2012. The effort has involved publicity and cooperation from ISPs, and over 90% of affected devices have now been cleaned. This still leaves about 350000, of which 800 to 1200 are in Hong Kong.

Is my Computer Infected?

DNSChanger can infect Microsoft Windows and Apple Mac OS X operating systems, but it can also change the DNS settings on some broadband routers. The simplest method for checking whether your computer is infected is to visit a DNS Changer Check-Up webpage. Green is good, red, you have a problem. More details about this, other methods of checking and how to correct the DNS settings are on HKCERT blog and the DNS Changer Working Group website.

More Information

- Impact of terminating the DNS server of DNSChanger
- DNSChanger Rogue DNS Servers Taken Down
- Esthost Taken Down – Biggest Cybercriminal Takedown in History

- DNS Changer Working Group
- DNS Changer Check-Up
- US Judge Postpones Death Sentence For Ghost Click Machines
- Rogue security software
- Click fraud
- Trojan:W32/DNSChanger

May Hong Kong Honeypot Report

<web-link for this article>

This is the fifth 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. This month, Taiwan and Japan tie for top attack source, each outnumbering all the other sources added together. The number of attacks has risen slightly.

Average Time To Infect: 9 hours 21 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 : 77
- 25 are brand new to this honeypot.
- 8 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
28	Taiwan
28	Japan
4	Singapore
3	Vietnam
2	Romania
2	United_States
2	China
1	New_Zealand
1	India
1	Austria
1	Canada
1	Italy
1	Russian_Federation
1	Portugal
1	Philippines

Malware List

Checksum (md5)	This	Previous	Detection*

	month	count	
df51e3310ef609e908a6b487a28ac068	8	5	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.rgk , ,)
0aaddde049fd4507effe596c04b73890	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
8d9a4ff99fcb614b99d572e06a2a3d1a	1	0 ***NEW	Y (w32/virut.7205 w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd , ,)
15965bb88165d1eb06851d8f076130ba	5	4	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
fd06f97c6c2ca431c77be7bfa87b6b8b	1	0 ***NEW	Y (W32/GenBl.FD06F97C!Olympus, Trojan.Win32.Jorik.IRCbot.kjf , ,)
46f4046abda82df2ab96c59807ed8e56	1	0 ***NEW	Y (W32/Trojan5.DCW W32/Backdoor.ZZR , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.rax , ,)
8a5ce07df6a5357dafa84f5317aaad35	2	3	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
bbb5034e33568e100dd3dadabb5a57e9	2	6	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
9019b23f2a5a51c33671739af2f30992	1	3	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
cc16ca0cb8befc56a3b564e41de5227e	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
036ee49ada38f73f2f5c51c9aced4ea4	2	0 ***NEW	Y (W32/GenBl.036EE49A!Olympus, Backdoor.Win32.Floder.ila , ,)
b82698a30e07fc71349f06750cae2664	2	1	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
865915650a85e7c27cdd11850a13f86e	4	3	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
cb576cca04946b3d0829703d108ae270	3	4	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
f9dc3945bdd7406bd8db06a47963ec14	5	8	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
925dabe1aa7a95811d363bf3441c74b4	1	3	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.xri , ,)
51767999be799dbcc493e3ecaeb19d44	1	1	Y (w32/virut.7116 , Virus.Win32.Virut.av , ,)
39b8ab14eaf444c6a873685e4fc644d3	1	0 ***NEW	Y (W32/WormX.JE W32/Allaple.H , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
22646e61e3e92158696169ca682a8372	1	0 ***NEW	Y (W32/GenBl.22646E61!Olympus, Trojan.Win32.Jorik.IRCbot.kun , ,)
6f06e39cb6df0908d5ab6e661c6b0386	1	0 ***NEW	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.advj , ,)
a6ea960823e477bb7ac2f81987428f08	1	0 ***NEW	Y (w32/emailworm.gvd , Net-Worm.Win32.Allaple.b , ,)
94109e9b3f2b045350db9a5cb592b178	4	1	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
27c818dd620d8e4ed23953b6befa1a4a	1	0 ***NEW	Y (W32/GenBl.27C818DD!Olympus, Trojan.Win32.Jorik.Poebot.ei , ,)
f11d86b86efb1d523a07ec8bcb94a61e	1	1	N (, , ,)
7867de13bf22a7f3e3559044053e33e7	1	3	Y (w32/susppack.cy.gen!eldorado , Backdoor.Win32.Agent.aknp , ,)
585e40a82204221a4ba2c2675cde293b	1	0 ***NEW	Y (W32/GenBl.585E40A8!Olympus, Trojan.Win32.Jorik.IRCbot.kyn , ,)

33fdb683c37fe3d87a403a5db0cbe821	1	0 ***NEW	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
3228f8bc721572422c268f244476dbb8	2	0 ***NEW	Y (W32/Trojan5.DCW W32/Backdoor.ZZR , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.abpn , ,)
519af1366c32618d1f807457d0b588ad	1	0 ***NEW	Y (W32/GenBl.519AF136!Olympus, Trojan.Win32.Jorik.IRCbot.ldr , ,)
7a177db9d14c4db6b8ddfafd65b21b68	1	0 ***NEW	Y (w32/virut.7116 w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd , ,)
f4a200f7818dfb166b9a3d238ac55a2d	2	6	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
1f8a826b2ae94daa78f6542ad4ef173b	1	4	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.phv Backdoor.Win32.Rbot.ion , ,)
a80fe85bb810220a0c064191ee65d2b5	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
cf263991bb889c28e6185ac4dd24668f	2	0 ***NEW	Y (W32/Trojan5.DCW W32/Backdoor.ZZR , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.uca , ,)
3875b6257d4d21d51ec13247ee4c1cdb	1	22	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663 ,)
0434308fd8833c7fafd48070cd230d00	1	0 ***NEW	Y (w32/virut.ag , Virus.Win32.Virut.at , ,)
60b4208a6f75857992ecc9ebd9a03131	1	0 ***NEW	Y (w32/genbl.60b4208a!olympus , HEUR:Backdoor.Win32.Generic , ,)
f8815cdca238ad5ab566f05f5a6335a4	1	2	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.voe , ,)
1d419d615dbe5a238bbaa569b3829a23	1	2	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
9f34976f45bb7c1acbf5fcf378339d5c	1	0 ***NEW	Y (w32/emailworm.hqk , Net-Worm.Win32.Allaple.e , ,)
2fa0e36b36382b74e6e6a437ad664a80	1	1	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.yqj Backdoor.Win32.Rbot.yol Backdoor.Win32.Rbot.wjd Backdoor.Win32.Rbot.sds , ,)
bbdd42f070c62a2f0341cd4ba86701b7	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.a , ,)
3f56c131ee2ec17b6b417df2c35db681	1	0 ***NEW	Y (W32/GenBl.3F56C131!Olympus, Trojan.Win32.Jorik.IRCbot.lqh , ,)
b4d9dd3a19e7fdd2211d81983f8e4d75	1	3	Y (w32/allaple.h , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
10980f4df2060b86a72eb5e533102980	1	1	Y (w32/backdoor2.dstk , Backdoor.Win32.IRCBot.jwy Worm.Win32.AutoRun.tet , W32Ircbot!I484 ,)
ad581e1ac598b18bf0b87452b7b5599b	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
a4eef4a4b56cbdd44990bc4fa191aaed	1	0 ***NEW	Y (w32/virut.7116 , Virus.Win32.Virut.av , ,)

Two of these files have been 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

- January Hong Kong Honeypot Report

- West Coast Labs

Flame, Failure of the Antivirus Industry and Cyber Cold War

<web-link for this article>

W32/Flame, also known as SkyWiper, is the current cyber-weapon *de jour*, joining Stuxnet and DuQu as evidence of State-sponsored cyber attacks. It is currently known to be highly complex, capable of gathering information (including via the infected computer's microphone) and probably has been spreading undetected at least a couple of years. The Laboratory of Cryptography and System Security (CrySyS), Budapest University, notes that one filename, WAVESUP3.DRV, was first seen on Dec 5 2007 in Europe by the Webroot community, so it might be 5 years old.

The pattern of infections is similar to Stuxnet and DuQu, mostly in the Middle East, with Iran and Israel at the top according to Kaspersky labs, but with the odd addition of Hungry, according to ICSAlabs. The Iran National CERT (MAHER) first announced their investigation of Flame on 28th May 2012 and provided a list of its known capabilities. Interestingly, they include physical (via removable media) and local network distribution methods, but not internet distribution, suggesting that, like Stuxnet, this is intended to be introduced to an "interesting" target site via rogue devices, and spread within the site for maximum effect. It is certainly not network-incapable, other modules include network sniffing, and uploading gathered information to command and control servers on the internet by encrypted channels, SSH and HTTPS. It also detects many anti-virus applications and reduces its activity accordingly to avoid being flagged as suspicious.

In a blog post on Flame, Mikko Hyppönen of F-Secure admits, "Stuxnet, Duqu and Flame are all examples of cases where we — the antivirus industry — have failed. All of these cases were spreading undetected for extended periods of time."

It appears that we have quietly moved to a period of cyber cold war, where nation states secretly develop and deploy sophisticated attacks on each other's information systems. Like the USA/USSR Cold War, the battles are normally fought in secret, and with complete deniability. Even when an attack is discovered, possibly years after it was deployed, we can only guess the target and the attacker. Stuxnet is an example of cyber sabotage, and Flame an example of cyber espionage, but these are not the only examples. In the same blog post, Hyppönen notes, "Chinese actors prefer attacks targeted via spoofed e-mails with booby-trapped documents attached. Western actors ... instead use USB sticks or targeted break-ins to gain access". Hardware attacks are also possible, Bruce Schneier discusses a hardware backdoor found in a US-designed, Chinese manufactured chip in his blog, but who put it there, how an what it was used for, or if it was used at all, is unknown. Deniability is complete.

More Information

- Identification of a New Targeted Cyber-Attack
- Case Flame
- The Flame: Questions and Answers
- Researchers identify Stuxnet-like cyberespionage malware
- Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East
- Duqu
- Backdoor Found in Chinese-Made Military Silicon Chips
- Countries Rushing to Cyber Weapons: First Stuxnet, Now Advanced Iran W32/Flame, Flamer or SkyWiper
- Lua Programming Language

- Microsoft Security Bulletin MS10-033
- sKyWIper: A complex malware for targeted attacks
- Complex cyberwar tool 'Flame' found ALL OVER Middle East

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/