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

Yui Kee Computing Ltd.

Newsletter

August 2012

Contents

Creation of Stuxnet Exposed (Humour)

<web-link for this article>

Investigative reporter Scott Adams has uncovered the story behind Stuxnet.

More Information

Dilbert and Loud Howard, 02nd August 2012
Critical Questions on Critical Infrastructure
Flame, Failure of the Antivirus Industry and Cyber Cold War
Malware: The Anti-Personnel Mine of Cyberwar
Defensive or Offensive, Beijing has Genius Cyber-Army

Was Incompetence, Enthusiasm or Greed Behind the Miss Hong Kong Voting Failure?

<web-link for this article>

Uncertainty surrounds the collapse of the online voting system for the Miss Hong kong beauty pageant. The online poll was run by TVB, the broadcaster of the event, and it is thought to be powered by Windows Azure technology. TVB was quick to blame unknown hackers for disrupting the system with an overload of traffic that started 15 minutes before the 10 minute period allocated for voting. TVB expected about 500,000 votes to be cast during that time, however, reports varied about the traffic that caused the overload. TVB was claimed to have told local Chinese daily Ming Pao 800,000 to one million participants tried to vote, but also said that the number was unknown. A report in the South China Morning Post said that more than 14 million attempts to access the website were made.

Other details, such as the number of prior downloads of the smartphone App for voting and its operation were not available.

Yui Kee's Chief Consultant Allan Dyer speculated wildly about the cause, saying, "Was it incompetance, enthusiasm or greed?" He outlined these three scenarios in more detail:

1. Incompetence - TVB did not build a robust, correctly-sized service. Perhaps a catastrophic collapse caused by not considering what would happen in an overload. One

voter reported retrying "many" times, a natural reaction to an error message. Fourteen million page hits could be one million voters trying fourteen times each.

2. Enthusiasm - some voters tried to stuff the ballot, not for gain, perhaps triggering the first scenario. What mechanisms did TVB have in place to detect and reject multiple voting? How were voters notified?
3. Criminal Gain - The total prizes for the first three contestants (HK$4.8M) doesn't seem enough for someone linked to a contestant to try to rig the ballot, The difficulty and chance of getting caught are too high. Do people bet on Miss HK? An illegal bookie might consider it worthwhile to fix the result.

Dyer concluded, "There's not enough information available to choose between them. My guess would be the first scenario, it's easier to say 'we were attacked' than admitting you messed up."

Updated: 29th August 2012

Richard Stagg, Managing Consultant at Handshake Networking added a fourth scenario:

4. Political - By equating the pageant with universal suffrage TVB painted a big red target on their web server, just under the imaginary neon sign saying "Come on then if you think you're hard enough".

Stagg commented, "Speculation aside, my money is also on 'TVB don't understand capacity planning'."

Further information about the Miss Hong Kong voting saga is emerging. Asiacloud Forum has an interview with Chin-Tang Chin, a director at Microsoft Hong Kong. He explains that the underlying cloud platform was Windows Azure and voting could be done through a web application or a mobile application, each developed by different companies.

Chin also clarified that user scenarios including using multiple devices or even writing computer programmes to generate lots of web requests in order to win the lucky draw were within the designer's expectations.

To vote, a user needed to enter their HKID number and their choice of candidate. Each Hong Kong resident has a unique HKID number, so this might seem to be a simple way of ensuring voters are Hong Kong residents, and preventing ballot-stuffing. However, it is a trivial exercise to generate numbers that match the pattern of an HKID number, with a valid check-digit.

More Information

Miss HK turns ugly
TVB: Hacking might cause Miss HK voting system failure
Miss Hong Kong voting saga -- Microsoft explains

August Hong Kong Honeypot Report

<web-link for this article>

This is the eighth 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 this month has dropped and is the lowest recorded so far. Last month's high seems to have been a temporary spike.

Average Time To Infect: 39 hours 9 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 : 19

11 are brand new to this honeypot.

Source of Attacks

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

8	United States
3	Japan
2	Canada
2	Taiwan
1	Vietnam
1	Slovakia
1	Saint Vincent and the Grenadines
1	South Korea

Malware

Checksum (md5)	This month	Previous count	Detection*
9b89ef791c5ef4241cc28e30fd464ca2	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
dca8713db4f5b7b84a66b51d925e7f9c	2	0 ***NEW	Y (w32/sdbot.aefv , Virus.Win32.Virut.n Backdoor.Win32.Rbot.vqt , ,)
f71fd17390c73ab350b029027fe97622	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.e , ,)
46616880960079764e41ff1c1a005712	1	0 ***NEW	Y (, Trojan.Win32.Buzus.lwbh , ,)
796645533028c68a684cdaa8030f911f	1	0 ***NEW	Y (w32/virut.ag , Virus.Win32.Virut.at , ,)
0fc020bacbee5719246cf48485cfca7e	1	0 ***NEW	Y (W32/Virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
12fb7332920a7797c2d02df29b57c640	1	1	Y (w32/trojan2.kexn , Trojan-Spy.Win32.Agent.bmxb , ,)
7831454a23399c7ee6dc04fc9c132f3f	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
b4d9dd3a19e7fdd2211d81983f8e4d75	1	4	Y (w32/allaple.h , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
1d53fb866c27a421f7557e3cda0592ac	2	4	N (, , ,) This file has low levels of detection.
3875b6257d4d21d51ec13247ee4c1cdb	1	28	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
352a39c959121d2b0b04eae906371df7	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
865915650a85e7c27cdd11850a13f86e	2	13	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
7ef4aef81f21bd4d2740bfa0d3be5867	1	0 ***NEW	Y (W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd

			Backdoor.Win32.Rbot.vqt , ,)
d00b9e4680d4c3d641405fbbf2389895	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
644ea081625064565c7e9816f235f264	1	0 ***NEW	Y (W32/Virut.7116 W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd Virus.Win32.Virut.av , ,)

One of these files has 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

West Coast Labs
January Hong Kong Honeypot Report

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/