Yui Kee Computing Ltd.

Newsletter

January 2013

Contents

Imperva Study Claims Anti-Virus is Ineffective

<web-link for this article>

US security company Imperva has published a report on the effectiveness of anti-virus software based on their work with students from the Technion-Israel Institute of Technology. The team collected 82 samples of malware and used the VirusTotal website to test whether they were detected by 40 anti-virus products. Based on this, they concluded that initial detection rates were as low as 5%, and recommended that compliance rules should be eased, freeing up money for "more effective" security measures.

Yui Kee's Chief Consultant Allan Dyer took a different view and harshly criticised Imperva's study, saying, "I was surprised at the small sample set Imperva used - just 82 samples, collected from honey pots, google and hacker forums. Can this really reflect on effectiveness against the millions of malware samples known to exist?"

In comparison, AV-Test uses two test sets in its Protection tests:

- All malicious files they discovered in the last 6 - 8 weeks: around 100,000 – 150,000 files.
- Extremely widespread malicious files they discovered in the last 6 – 8 weeks: around 2,000 – 2,500 files.

Dyer continued, "A second surprise is that Imperva do not do their own testing, they threw the samples at VirusTotal. VirusTotal is a useful website, but they are quite explicit that it is unsuitable for product testing. Imperva takes the short form of VirusTotal's advice, 'not designed as a tool to perform antivirus comparative analyses', and counter it in the study's 'Limitations' section saying that they are not doing a comparison. Imperva ignore the longer advice, that details why VirusTotal is unsuitable for both comparative and effectiveness testing."

Dyer concluded, "Anti-virus testing is notoriously difficult, and competent researchers put a lot of work into making sure they use methodologies that will produce relevant, reliable results. Did Imperva?"

Updated: 07th January 2012

Imperva's study has generated a lot of discussion and criticism, including from David Harley on his blog, Max Eddy at PC Magazine, and Kurt Wismer on his blog.

More Information

Imperva "Assessing the Effectiveness of Antivirus Solutions"
AV-TEST - The Independent IT-Security Institute
VirusTotal - Free Online Virus, Malware and URL Scanner
Anti-virus products are rubbish, says Imperva
Anti-Malware Testing
Experts Slam Imperva Antivirus Study
imperva's anti-virus study is garbage
Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt
Antivirus industry struggles to keep up - Wilders Security Forums
Still Don't Like Our AV Study? A Response to The Critics

Hong Kong Lottery Scam Mule Jailed

<web-link for this article>

A man has been jailed for 28 months by a Hong Kong District Court for conspiracy to launder money as part of a lottery scam. During 2010 and 2011, the man received about HK$1.8 million in "handling fees" from 26 overseas victims who had been fooled by phones calls into believing they had won lotteries. The man withdrew the money and passed it to an unknown man, receiving up to $500 each time.

Yui Kee's Chief Consultant Allan Dyer commented, "Most email users will be familiar with the online variant of this scam, when they receive 'winning notifications' of lotteries they never entered, though it is worth remembering that the trick is more likely to succeed if the victim has entered a similar-sounding lottery recently. The scam depends on greed of the victim, who pays the 'handling fee' to get the non-existent prize, and the greed of the mule, who the Police can quickly find, that allows the mastermind to get away unidentified with the cash."

More Information

Man jailed for money laundering charge

Hong Kong Cybercrime on the Rise

<web-link for this article>

In his end-of-year review, Hong Kong Police Commissioner Andy Tsang Wai-hung admitted there had been an alarming rise in cybercrime during 2012. There were 430 reported commercial email scams last year, resulting in HK$430 million in losses, a 177% increase in the number of cases and 267% increase in losses from 2011. A further HK$26 million of losses were described as due to online business scams. About 820 cases were related to online shopping or auctions. The rate of increase in technology crime over the last three years was above 30%. Tsang cited difficulties in investigation, including ISPs refusing to disclose suspicious web addresses and jurisdiction issues. Only 15.4% of technology crime cases were solved.

The overall number of crimes fell slightly in 2012, and violent crime dropped 2%.

Yui Kee's Chief Consultant, Allan Dyer, commented, "Criminals find it easy to search for victims online. We must all be vigilant and strengthen our security practices. This includes companies and banks that are putting their customers at risk by adopting unsafe procedures."

More Information

Overall crime rate drops
Low success in cracking technology crime cases
Jump in e-mail fraud and cybercrime alarms police

Fake Citibank (Hong Kong) Alert

<web-link for this article>

The Hong Kong Monetary Authority has issued an alert about fraudulent website www.zzfwy.com, which resembles the official Citibank (Hong Kong) website. Citibank has confirmed that it has no connection with the site, and the Police are investigating.

People who have been tricked by the fake site should contact Citibank HK at 2860 0333 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Alert issued on bogus website
Fraudulent website: www.zzfwy.com

January Hong Kong Honeypot Report

<web-link for this article>

This is the thirteenth 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. Because of public holidays, this report covers from 20th December 2012. After six months of low numbers, there has been a sudden jump, and this is the highest number of attacks since July 2012.

Average Time To Infect: 6 hours 5 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 : 154
- 18 are brand new to this honeypot.

Source of Attacks

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

125	United_States
10	Japan
4	Germany
4	China
2	France
2	Canada
2	United_Kingdom

1	Malaysia
1	Singapore
1	Taiwan
1	Pakistan
1	Jordan

Malware

Checksum (md5)	This month	Previous count	Detection*
64b4345a946bc9388412fedd53fb21cf	1	0 ***NEW	Y (w32/trojan-sml-sdcw!eldorado , UDS:DangerousObject.Multi.Generic , ,)
662cc2048da87cc777261e8a7df27d23	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
8c30591c9abacd805711dc2c8f1639ee	1	0 ***NEW	Y (W32/Virut.7116 , Net-Worm.Win32.Allaple.e Virus.Win32.Virut.av , ,)
af1894848b6525c7882c33b59d1bbebd	1	1	Y (w32/allaple.h , Net-Worm.Win32.Allaple.e , ,)
f18d10439daaa8a760fcfedc39d4bfcd	1	0 ***NEW	Y (w32/newmalware-rootkit-i-based!maximus , Trojan.Win32.Genome.aixqc , ,)
a7fb7ecabf6c3ae0bdd6c970e10b3de1	1	0 ***NEW	N (, , ,) script
ed0dabd71a2bfd485259ad4ce30a6041	1	0 ***NEW	N (, , ,) script
ab866c52c0d90d0ea20fed2fe0ec259b	1	0 ***NEW	N (, , ,) script
340c1a84d216991f0f3f4dbe4756893c	1	0 ***NEW	N (, , ,) script
4d56562a6019c05c592b9681e9ca2737	1	0 ***NEW	Y (w32/trojan-sml-sdcw!eldorado , Trojan.Win32.Genome.ahpxd Net-Worm.Win32.Kido.ih UDS:DangerousObject.Multi.Generic , ,)
7327d60e3ca15556f57e2378e762c8fd	116	0 ***NEW	N (, , ,) script
267b7ddeae1e9601f9800f3b76ed45da	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
952098cf3c65cfcb52282d8959ddffd3	1	5	Y (W32/Allaple.H , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
3d19d0b6638bb7ccf65f8d25b4c13d6b	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
0da155b04f16dafafffbb1a485b3d0e1	1	0 ***NEW	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
bbb5034e33568e100dd3dadabb5a57e9	3	21	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
14a09a48ad23fe0ea5a180bee8cb750a	2	8	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.DsBot.vd , ,)
321e5688f6a04e8482cec37515fa85f8	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
8a5ce07df6a5357dafa84f5317aaad35	1	7	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
038edde0c5a188ea6eed9406923a9771	1	0 ***NEW	Y (w32/virut.7116 w32/sdbot.aefv , Backdoor.Win32.Rbot.adqd , ,)
a812cb8d6ca7e1b57dfffbc7ab6a8101	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
833cda5b5bef5989deb6bf57c557ce30	1	2	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.abfy , ,)
1d53fb866c27a421f7557e3cda0592ac	8	14	N (, , ,) script
a2ad8c9c758e07d6b5e37ed949360835	3	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
3875b6257d4d21d51ec13247ee4c1cdb	2	40	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
e1b0c382fe1aafe918765267440c2cb8	1	0 ***NEW	Y (w32/genbl.e1b0c382!olympus ,

			Backdoor.Win32.Ruskill.pqd , ,)

One of these files have appeared 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

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/