Yui Kee Computing Ltd.

Newsletter

November - December 2006

Contents

Editor's Notes

Reflecting on the past year in Information Security, it seems we are heading down a dark and dangerous path. The numbers are against us, on one hand, massive malware outbreaks like Slammer, Blaster, and Loveletter have disappeared, but the replacement is worse. Criminals are using targeted malware in small numbers to steal, and they are generating huge numbers of variants to slip past scanners. We used to face polymorphic viruses, where the virus would modify itself on each infection, the response was to analyse the polymorphic engine so that the scanner could detect all possible outputs; now the malware creators are keeping the variant generator to themselves, frustrating analysis.

Numbers are against us in spam too, again, the profit motive is driving our opponents, and we have to run as fast as we can just to stay where we are. The draft law currently passing through the committee stage in Hong Kong's Legislature is too weak to have an effect. However, one interesting effect of the Taiwan earthquake is a reduction in spam: at my mail gateway, incoming spam has dropped about 50%, but legitimate messages are normal. Unfortunately, slashing bandwidth cannot be considered as a simple, long–term solution to spam.

Numbers are overwhelming us in terms of vulnerabilities, too. New, critical vulnerability announcements are no longer news, and we will soon have to cope with a huge, new operating system, packed with an unknown number of new vulnerabilities: Vista. The more complex a system is, the more likely it is there are flaws, and Vista is Microsoft's most complex operating system to date.

Numbers are making our job of protecting information more difficult, too, because of the continual increase in data storage capacity and accessibility. We are storing more data than ever before, and we often have little idea of what it is we are keeping, where we are keeping it, or who can access it. The data leakage from the Independent Police Complaints Commission (IPCC) earlier this year was just one example, the Privacy Commissioner's report is now available: http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf.

Is there a bright side? Information Security issues do seem to be getting more coverage and discussion than previously, now we need to face the difficult questions and take action. Have a Healthy, Prosperous and Secure New Year, and remember, Information Security is Everyone's Business.

Allan Dyer

AVAR 2006 Conference

The 9th annual conference of the Association of anti Virus Asia Researchers took place in Auckland, New Zealand on th3 3rd to 5th of December. The conference theme was "Digital Security – Prevention to Prosecution", speakers and participants came from around the world.

Shigeru Ishii of the Information-technology Promotion Agency, Japan (IPA) covered the threats seen recently in Japan, focusing on the Antinny Virus, which exploits the Winny peer–to–peer file–sharing software to leak information, and the phenomenon of "one–click billing fraud", where users are tricked and intimidated into paying on bogus websites.

Eric Chien of Symantec Security Response looked at the security threat of Gadgets, such as Google Desktop Gadgets, Yahoo Widgets and the Vista Sidebar. Gadgets are another potential route for untrusted code to enter our machines.

Maksym Schipka of MessageLabs analysed the prevalence of PE packers in email traffic. Blackhats are using PE packers to avoid detection of their malware.

Sungkeun Rhee and Jeong Wook Bang of AhnLab looked at the upcoming threats of RFID.

Igor Muttik of McAfee AVERT noted a shift in deployment vector from SMTP to HTTP, and urged developers and independent testing bodies to focus on perimeter scanning of HTTP traffic.

Ja-Way Hung and Pei-Wen Liu of the Information and Communications Security Technology Center in Taipei used Geographical Information Systems to correlate malware infection locations and discern the intended target of organised hackers.

Craig Johnston of IBM presented a case study of a phishing attack.

Eric Uday Kumar of Authentium gave a detailed technical description of rootkits on Windows, including various methods for hooking and patching DLLs and the kernel.

Enrique González Ochoa of Panda Software painted a daunting picture of threats against VoIP.

Jonathan Poon of Microsoft detailed the further development and expansion of an automated release scanning system.

Peter Ferrie of Symantec Advanced Threat Research explained attackers on virtual machine emulators, and showed how programs could detect they were running inside emulators such as Vmware, VirutualPC, Parallels and others.

Kimmo Kasslin of F-Secure looked at the challenge of kernel malware, using Haxdoor and Mailbot as case studies.

Cai Jun of FortiNet looked at malware on mobile devices.

Aditya Kapoor of McAfee AVERT described techniques to evaluate two different binaries and determine the amount of shared code and behaviour.

Sébasien Josse of Silicomp-AQL also delved into virtual machines and the kernel to consider unpacking using emulation.

Vesselin Bontchev discussed the problems of the Common Malware Enumeration (CME) initiative, concluding that the scheme was fatally flawed.

Babu Nath Giri of McAfee AVERT described the emergence of ransomware

One panel session discussed "Where have all the Outbreaks gone?", and the second considered, "Defensible Digital Boundaries". The Gala Dinner featured a show by Maori dancers.

AVAR website:

http://www.aavar.org/

HK Privacy Commissioner on Fingerprinting in Schools

The Hong Kong Privacy Commissioner for Personal Data, Roderick Woo, has ordered a school in the Kowloon District to remove a fingerprint system. The system was installed in 2005 but the Commissioner found that it was excessive, and there was a less privacy–invasive method that could be used.

The case attracted international attention after controversy over similar cases in the United Kingdom.

More information:

http://www.pcpd.org.hk/english/publications/newsletter_issue17.html
http://www.theregister.com/2006/11/09/hongkong_kiddyprinting/
http://www.theregister.com/2006/10/17/mps_on_kiddyprinting/

HK Spammer on Spamhaus' Ten Worst Spammers List

The independent anti-spam organisation, Spamhaus, has named "Vincent Chan" of yoric.net, based in Hong Kong, as number seven on their latest list of the ten worst spammers. According to Spamhaus, Vincent Chan is working together with Lap Chung Chan and a small group of Chinese spammers. They are heavily into pharmacy, but have also spammed for watches and some mailshots for OEM warez, toner and ink cartridges, and mortgages. Spamhaus claims that these people have been at it for years, are experienced and put out massive volumes.

The top ten spammer list also contains spammers from Eastern Europe and North America.

In the Spamhaus "10 Worst Spam Origin Countries" list, China came second (with 312 current known spam issues), behind the USA (with 1997).

More information:

http://www.theregister.com/2006/11/14/spamhaus_worst_spammer_list/
http://www.spamhaus.org/statistics/countries.lasso
http://www.spamhaus.org/statistics/spammers.lasso
http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK6921

Jail for BitTorrent Pirate

Hong Kong became the first jurisdiction to jail a BitTorrent user when Chan Nai-ming's conviction was upheld on appeal on 13th December. Mr. Chan, who used the alias "Big Crook" was convicted for attempting to distribute three Hollywood movies - Daredevil, Miss Congeniality and Red Planet - using the BitTorrent peer-to-peer file-sharing technology.

Tuen Mun Court originally sentenced Mr. Chan to 3 months in November 2005 and the appeal was based on the claim that making a work available on the Internet did not constitute "distribution" because each downloading act was initiated by the downloaders, and "distribution" must mean a positive act. In delivering her judgement, Madam Justice

Clare-Marie Beeson ruled that the magistrate had correctly used the ordinary meaning of "distribution" to convict Chan. She also rejected a claim that the section of the copyright ordinance used only applied to "tangible materials", not digital copies.

Madam Justice Beeson also noted the aim of Hong Kong laws to protect copyright owners and to help the city maintain its position as a responsible member of the global trading community.

Sound Insurance Investment

The Planetary Society is making a forward–looking bid to prevent humanity suffering the same fate as the dinosaurs by offering a US$50,000 prize for a mission plan to rendezvous with and "tag" a near-Earth asteroid. The competition rules designate the asteroid Apophis, which might collide with Earth in 2036, as the target, but the schemes devised could be used on any threatening asteroid.

More information:

http://planetary.org/programs/projects/near_earth_objects/apophis_competition/rules.html

http://www.theregister.com/2006/12/14/asteroids_competition/

Write Software, Pay Fine

Programmer Isamu Kaneko has been convicted of enabling copyright infringement by a Japanese court. Judge Makoto Himuro ruled that Kaneko was selfish and irresponsible and aware of the damage to society that would be caused when he developed and distributed Winny, the peer–to–peer file–sharing software. Kaneko was fined ¥1.5m.

There is no information on whether gun manufacturers will now be charged with enabling murder.

More information:

http://www.regdeveloper.co.uk/2006/12/14/winny_p2p_author_convicted/

http://www.yomiuri.co.jp/dy/national/20061214TDY02009.htm

End of ORDB

The Open Relay DataBase is closing down, after five and a half years of supporting the fight against spam. The use of networks of compromised PC's has made ORDB less useful in recent years, and the volunteer staff acknowledged this in their farewell message on the ORDB website, "the general consensus within the team is that open relay RBLs are no longer the most effective way of preventing spam from entering your network as spammers have changed tactics in recent years, as have the anti-spam community."

The website is scheduled to disappear by 31 December 2006.

More information:

http://www.theregister.com/2006/12/22/ordb_shutdown/

http://www.ordb.org/news/?id=38

Andrew Hopper Honoured

British microcomputer pioneer Professor Andrew Hopper becomes a Commander of the British Empire for services to the computer industry in the British New Year Honours list. Hopper founded the computer company Acorn that produced the Acorn Atom, BBC Micro, Acorn Electron and Archimedes.

The BBC Micro was used in a BBC television series that introduced the emerging personal computer technology in the early 1980's. The machine became very popular in UK schools, and a lot of educational software for it was developed. Although only based on an 8–bit processor, the 6502, it had many advanced features, such as real, interrupt–driven support for the serial port, built–in that were lacking in much more expensive machines, such as the IBM PC. The optional features included a network interface ("Econet"), a speech synthesiser and a range of second processors, including one that ran a favour of Unix.

The Archimedes was similarly ground–breaking, based around a RISC processor developed in–house by Acorn, the Acorn RISC Machine, later renamed to the Advanced RISC Machine, or ARM. ARM processors are found in many devices today, including PDA's and mobile phones.

More information:

http://news.bbc.co.uk/2/hi/technology/6217447.stm

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/