Yui Kee Computing Ltd.

Newsletter

July 2006

Contents

WGA: Worm Genuine Advantage

It's not just Microsoft that wants to take of WGA to spy on you. A worm, W32/Cuebot-K (also known as Backdoor.Win32.IRCBot.st or Win32/IRCBot.OO) masquerades as the controversial Microsoft software. Cuebot-K spreads via AOL instant messenger and installs itself display name of "Windows Genuine Advantage Validation Notification". It also disables the Windows firewall and opens a backdoor. Users who attempt to remove the malware are falsely informed that getting rid of the program will result in system instability.

More information:

http://www.cw.com.hk/computerworldhk/article/articleDetail.jsp?id=353589

http://www.theregister.com/2006/07/03/wga_worm/

http://www.sophos.com/virusinfo/analyses/w32cuebotk.html

http://www.theregister.com/2006/07/07/wga_disadvantage/

http://www.pcadvisor.co.uk/news/index.cfm?newsid=6507

http://www.sophos.com/pressoffice/news/articles/2006/07/cuebotk.html

http://www.infoworld.com/article/06/06/30/HNwormmsantipiracy_1.html

http://www.webmasterworld.com/forum10/12123.htm

http://www.theinternetpatrol.com/new-windows-genuine-advantage-worm-cuebot-k-being-spread-by-aim-installs-self-as-wgvanexe-and-dcpromolog

Breaking TCP and the Great Firewall

A group of Cambridge researchers have investigated China's Internet content controls and found that the system works by sending a TCP RST packet to the client and server in a connection when a banned keyword is detected. However, other experts claim that this is a) not a new idea; and b) less effective compared to other methods.

More information:

http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

http://www.lightbluetouchpaper.org/2006/06/27/ignoring-the-great-firewall-of-china/

http://www.cw.com.hk/computerworldhk/article/articleDetail.jsp?id=353880

Drop your OS

The recent Sophos Security report notes the continued dominance of PC Trojans as a security threat, leading Graham Cluely to conclude, "It seems likely that Macs will continue to be the safer place for computer users for some time to come - something that home users may wish to consider if they're deliberating about the next computer they should purchase."

More information:

http://www.theregister.com/2006/07/05/trojans_mac_pc/

http://www.sophos.com/pressoffice/news/articles/2006/07/securityreportmid2006.html

Support Calls

The Register is holding a survey of favourite IT Support Call anecdotes.

The Poll:

http://www.theregister.com/2006/07/05/it_support_anecdotes/

US Judge Acts on Spam

A US Judge has ordered the US Navy not to use its sonar equipment, could which kill, injure, and disturb many marine species, including marine mammals.

More information:

http://www.theregister.com/2006/07/04/sonar_mammals/

Virus Researcher Virus

Virus writers have created a proof-of-concept virus, dubbed Gattman, that targets an Interactive Disassembler Pro (IDA), a popular reverse engineering tool from Data Rescue, widely used by anti-virus researchers. The malware were authors presumably hoping to embarrass incautious researchers by spreading a virus using the tools of their trade. However, professional anti-virus

labs work under strict rules concerning the exchange and handling of executables, so Gattman is more likely to spread among amateur researchers, or malware authors.

More information:

http://www.theregister.com/2006/07/06/gattmann_virus/

Hong Kong's Anti-Spam Bill

A Bill to regulate Unsolicited Electronic Messages (UEMs) was tabled at the Legislative Council on July 12 and it is hoped the Bill will be passed during the next legislative year. The bill proposes an "opt-out" regime, whereby the sender of a commercial regulated message is required to provide a functional unsubscribe facility. The messages should also include accurate sender information, while their subject heading should not mislead recipients and number identification should not be concealed. Address harvesting software is also banned.

To support the opt-out regime, the bill will empower the Office of the Telecommunications Authority (OFTA) to form "do-not-call registers" for recipients opting out of receiving further messages. The registers will initially cover pre-recorded voice or video messages, fax messages and SMS or MMS messages.

This falls short of the hopes of many anti-spam proponents, who would prefer an "opt-in" regime.

Also, the wording of the Bill has raised technical concerns; including that it may, inadvertently, ban DNS resolvers. The fear rises from the inclusion of "Internet Protocol address" in the definition of electronic message in the Bill. Coupled with the definition of "address harvesting software" as, "software that is specially designed or marketed for use for (a) searching the Internet or a public telecommunications network for electronic address and (b) collecting, compiling, capturing or otherwise obtaining those electronic addresses", it is clear that DNS resolvers are covered by the restrictions on address harvesting software, which include supplying, acquiring, and using such software, "in connection with, or to facilitate, the sending of electronic messages…". The possible punishment is a fine of $1 million, and 5 years jail – something to consider the next time you type in a domain name.

More information:

http://www.news.gov.hk/en/category/businessandfinance/060706/html/060706en03006.htm

http://www.citb.gov.hk/ctb/eng/legco/pdf/LegCo_message.pdf

Computers in US State Department Break-ins By Sources From Asia

The US State Department said it was conducting a forensic probe after hackers in East Asia tapped into computer systems at its Washington headquarters and diplomatic posts in the region. The attacks reportedly targeted the bureau in the department dealing with North Korea and China.

A State Department spokesperson downplayed the incident, suggesting that early reports sensationalised the incident.

http://news.yahoo.com/s/afp/20060712/pl_afp/usdiplomacycomputers

http://news.yahoo.com/s/nm/20060712/wr_nm/security_state_computers_dc

Man-In-The-Middle Phishing Defeats Two-Factor Authentication

Criminals have found a way around the token-based authentication systems that have been adopted by some banks. At least 35 phishing Web sites using the attack have been discovered. They attempt to trick users into divulging the temporary passwords created by security token devices.

Bruce Schneier predicted the rise of such attacks last year.

More information:

http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

http://www.f-secure.com/weblog/archives/archive-072006.html#00000921

http://www.schneier.com/blog/archives/2006/07/failure_of_twof.html

http://www.theregister.com/2006/07/13/2-factor_phishing_attack/

http://listmgr.questex.com/t/1650339/41252614/785485/0/

Prediction from Bruce Schneier:

http://www.schneier.com/crypto-gram-0503.html#2

Gmail Phishing

Phishers have expanded their target victims to Gmail users with a recent message that purported to be notification of a $500 cash prize from Google. Users who followed the embedded link reached a site hosting malware, and, combining Advanced Fee Fraud into the scam, they were invited to pay $8.60 to register for “Google Games” in order to claim their prize.

More information:

http://www.theregister.com/2006/07/12/gmail_phish/

Security by Obscurity

In a further demonstration of the weakness of “security by obscurity”, researchers at Cornell University have broken secret codes used by Europe’s Galileo navigation satellite. Galileo is still under development and it is intended to be a commercial, non-US controlled alternative to GPS. As Galileo is intended to be a charged service, this discovery could threaten the charging mechanism and therefore th viability of the project.

Among the comments on the topic on Bruce Schneier’s Blog was this gem by Darryl Smith, “And you know what time it is anyway, just not exactly when that time is.” Very profound.

More information:

http://www.theregister.com/2006/07/12/galileo_codes_cracked/

http://www.schneier.com/blog/archives/2006/07/galileo_satelli.html#comments

Hong Kong Controls Import and Export of Quantum Cryptography

The list of Strategic Commodities that require a license to be imported or exported to Hong Kong was updated with effect from 18 July 2006. The changes include a new measurement method for the speed of digital computers (Weighted TeraFLOPs on Adjusted Peak

Performance), a relaxation of the restrictions on computer speeds, and the addition of a control on encryption systems designed to use quantum cryptography.

Quantum cryptography has generated a lot of academic interest recently, but experts, including Bruce Schneier, have suggested that it is unnecessary, "Quantum cryptography has the potential for making the strongest link, in a series of very weak links, even stronger," says Schneier.

Other specifications for control of cryptographic products remain unchanged: including the limit of 56 bits for symmetric keys and the exemption of mass market products where the "cryptographic function cannot easily be changed by the user". Also, the Import and Export controls still only apply to tangibles, so cryptographic software downloaded from the Internet is not covered.

Five plant pathogens have also been added to the list:

Potato Andean latent tymovirus

Potato spindle tuber viroid

Xanthomonas oryae pv. oryzae (Pseudomonas campestris pv. oryzae)

Clavibacter michiganensis subsp. Sepedonicus (Corynebacterium michiganensis subsp. Spedonicum or Corynebacterium Sepedonicum)

Ralstonia solanacearum Races 2 and 3 (Pseudomonas solanacearum Races 2 and 3 or Burkholderia solanacearum Races 2 and 3)

More information:

http://www.stc.tid.gov.hk/english/circular_pub/2006_stc10.html

http://www.stc.tid.gov.hk/english/checkprod/sc_control.html

http://www.gld.gov.hk/cgi-bin/gld/egazette/gazettefiles.cgi?lang=e&year=2006&month=7&day=7&vol=10&no=27&gn=170&header=1&part=0&df=1&nt=s2&newfile=1&acurrentpage=12&agree=1&gaz_type=ls2

http://infosecuritymag.techtarget.com/articles/august01/features_crypto.shtml

http://www.theage.com.au/articles/2003/11/28/1069825960663.html

http://www.wired.com/news/privacy/0,1848,69841,00.html

http://www.schneier.com/blog/archives/2006/02/quantum_computi.html

http://www.newscientisttech.com/article/mg18925405.700.html

http://www.schneier.com/crypto-gram-0312.html#6

Octopus Under Attack

Ilan Kirschenbaum and Avishai Wool have demonstrated the feasibility of designing and building an extended range RFID skimmer on a very limited budget (US$100). Although the paper focuses on ISO-14443 RFID tags, these have the same operating frequency as the Octopus cards used on Hong Kong transportation networks (13.56 MHz). The Octopus system was designed before the publication of the ISO standard.

They used an antenna constructed from antenna from 5/16 inch cooking gas copper tube to read RFID tags at a range of up to 25cm, and believed that they could reach a range of 35cm with some more effort. They concluded that,

(a) ISO-14443 RFID tags can be skimmed from a distance that does not require the attacker to touch the victim;

(b) Simple RFID tags, that respond to any reader, are immediately vulnerable to skimming; and

(c) They are about half–way toward a full-blown implementation of the relay-attack predicted by Ziv Kfir and Avishai Wool.

Full Article:

http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html

Forget Y2K: First Report of Epoc Bug

If all the Unix Sys Admins saying in 1999 that their systems wouldn't be failing until 2038 annoyed you, check the first report of an Epoc Bug stopping a production system.

More information:

http://thedailywtf.com/forums/thread/78254.aspx

Malware Search

First, Websense came up with a way of leveraging Google's binary search capability to find malware on the web, but they decided to restrict the details of their technique to, "a select group of security researchers". So, H.D. Moore created an open version.

More information:

http://www.theregister.com/2006/07/18/malware_search/

http://metasploit.com/research/misc/mwsearch/index.html

http://www.pcworld.com/article/126371-1/article.html

http://www.cio.com/blog_view.html?CID=23075

Open Source Malware

McAfee's recently–published Global Threat Report notes that malware authors are using Open Source development models to collaborate and make more effective malware. The tone and presentation of the report have prompted some reporters to criticise it as anti–Open Source. As the report has the sub-heading, "Paying a price for the open–source advantage", and five of the seven articles discuss the open–source model, with titles including, "Good Intentions Gone Awry", and "Open–Source Software in Windows Rootkits", it is easy to get the impression that open–source equals bad.

However, closer reading of the articles reveals a familiar story: malware authors are increasingly professional criminals, and they are therefore using the most effective tools for the job. In this light, this is a resounding endorsement of the Open Source model: another group has recognised it as the most effective software development method. The implication that Open Source is somehow responsible for better malware is guilt by association, like noting that bank robbers have switched from horses to cars for their getaways, so taxi drivers have good intentions gone awry.

Why is McAfee putting this spin in its report? Is this a proprietry software developer trying to spread fear, uncertainty and doubt about Open Source?

More information:

http://www.theregister.com/2006/07/18/open_source_virus_development/

https://secure.nai.com/apps/downloads/free_evaluations/survey.asp?code=MW100

http://news.zdnet.co.uk/internet/0,39020369,39278942,00.htm

http://www.itweek.co.uk/itweek/news/2160344/malware-dangers-grow-criminals

http://www.theitshield.com/pr/8902

Google Earth and the Chinese Military

Google Earth users have discovered and identified a curiously detailed scale model of a disputed area on the Chinese/Indian border at the east end of the Karakoram mountain range. The model is located near an apparent military installation in Huang Yang Tan, an area also noted for a reforestation project.

More information:

http://bbs.keyhole.com/ubb/showthreaded.php/Cat/0/Number/484568/page/vc

http://regmedia.co.uk/2006/07/19/aksayqin_hu.kmz

http://bbs.keyhole.com/ubb/showthreaded.php/Cat/0/Number/510687/page/vc/vc/1

http://regmedia.co.uk/2006/07/19/huangyangtan.kmz

http://www.theregister.com/2006/07/19/huangyangtan_mystery/

http://www.theregister.com/2006/07/21/huangyangtan_letters/

Web Accessibility

A Google Labs project prioritises search results by their accessibility to visually impaired web users.

More information:

http://www.theregister.com/2006/07/23/google_search_engine_for_the_blind/

http://labs.google.com/accessible/

Ransomware vs. Defence in Depth

Researchers at Kaspersky Lab have successfully analysed a ransomware Trojan, Gpcode.ag, cracking a 660 bit RSA encryption key. They note that, “Currently, the longest factorized key on the RSA website is 640 bits”, so they are keeping their method a trade secret. However, the malware authors can continue to increase the key length until it is effectively unbreakable.

The objective of ransomware is to encrypt the victim’s important files, then demand money for their recovery. Although Kaspersky’s achievement is remarkable, analysis and cracking is not our strongest defence against this threat. The best defence for end-users is a good backup strategy – the important files can then be recovered from the most recent backup. Of course, keeping the backups offline, and preferable off site, will prevent any malware affecting them. The second approach, for law enforcement, is follow–the–money: tracing the ransom payments until the people profiting can be identified and prosecuted.

More information

http://www.viruslist.com/en/analysis?pubid=189678219

http://www.viruslist.com/analysis?pubid=191951869

http://www.theregister.com/2006/07/24/ransomware/

http://www.viruslist.com/en/analysis?pubid=189678219

Secure Destruction of Credit Cards

A Cambridge researcher has highlighted the difficulties of reliably destroying chip–and–pin credit cards:

http://www.lightbluetouchpaper.org/2006/07/20/new-card-security-problem/

Spam Relays

The United States is still the world's top spam–relaying nation, and its efforts to change this have stopped being effective:

http://www.theregister.com/2006/07/25/spam_relay_stats/

Fuzzing and "Responsible Disclosure"

Fuzzers are increasingly being used to search for flaws in software. A fuzzer sends randomised data to a program and looks for unexpected results that might indicate a vulnerability.

According to his Blog posting, HD Moore started using his own fuzzers to search for flaws in web browsers a few months ago, and he is now publishing the results as the Month of Browser Bugs Project.

Microsoft has criticised Moore's apparent failure to engage in what the company calls a "responsible disclosure of vulnerabilities." Moore has also drawn criticism from a Russian criminal who objected to the disclosure of the vulnerability he had been exploiting.

Microsoft's claim appears weak, given that they claimed to be investigating the flaws reported to them by Moore in April.

More information:

http://www.securityfocus.com/columnists/411?ref=rss

http://www.securityfocus.com/news/11400

http://www.securityfocus.com/news/11387

http://browserfun.blogspot.com/

http://www.theregister.com/2006/07/26/month_of_browser_bugs/

Mobile Viruses: Reality or Marketing?

CA and F-Secure are squaring up over a disagreement about the significance of mobile viruses. CA, a company that does not produce anti-virus software for mobile phones, claims that F-Secure, a company that produces anti-virus software for mobile phones, is hyping the threat to create a market.

CA is not claiming that mobile viruses don't exist, but that the threat they represent is "theoretical". "Dig below the skin and the message stops sounding pithy and starts smelling rather rotten. At the core of the rot is the mostly undeniable fact that there is no threat to protect against," said Simon Perry, European vice president of security for CA. CA cites the lack of economic incentive for developers, the lack of interoperability between platforms and phone models and the requirement for user interaction as barriers.

The early PC virus writers had no economic motivation, and numerous email worms have demonstrated users willingness to click on almost anything. The lack of interoperability has been a limitation, but malware authors have created cross-platform code in the past.

More information:

http://news.zdnet.co.uk/internet/security/0,39020375,39279551,00.htm

http://www.f-secure.com/weblog/archives/archive-072006.html#00000928

Wikipedia Accuracy: Hong Konger Front

Followers of the ongoing debate concerning the accuracy and usefulness of Wikipedia, "the free encyclopaedia that anyone can edit", may be interested in the article describing an unheard of political group, the "Hong Konger Front". The group appears to want to promote the *independence* of Hong Kong by advocating a flag with a device representing the *union* of England, Scotland and Northern Ireland.

More information:

http://en.wikipedia.org/wiki/Hong_Konger_Front

http://en.wikipedia.org/wiki/Talk:Hong_Konger_Front

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/