Yui Kee Computing Ltd.

Newsletter

May 2006

Contents

Zombie Attack Conviction

Christopher Maxwell, from Vacaville, California, pleaded guilty to an attack that disrupted thousands of computer systems. Systems at Northwest Hospital and Medical Centre were among those affected in January 2005, preventing operating room doors from opening, and disrupting doctors' pagers.

Maxwell had two juvenile co-conspirators, and the crime made them made more than $100,000 in advertising commissions. He agreed to pay $252,000 in compensation to the hospital.

More information:

http://www.mercurynews.com/mld/mercurynews/news/breaking_news/14508386.htm
http://www.theregister.com/2006/05/05/hospital_zombie_attack/

MySQL Vulnerability

Secunia has reported MySQL information disclosure and buffer overflow vulnerabilities. Users are advised to upgrade to version 4.1.19 or 5.0.21.

More information:

http://secunia.com/advisories/19929/

MS Not the Only Target

Remember, just because PC’s running Microsoft software are the biggest security target, they are not the only one.

More information:

http://www.theregister.com/2006/05/09/mcafee_mac_security_risk/
http://download.nai.com/products/mcafee-avert/WhitePapers/NewAppleofMalwaresEye.pdf
http://www.mcafee.com/us/about/press/corporate/2006/20060505_011515_u.html

HK Boy, 16, arrested for 'pirate website'

A 16-year-old was arrested by customs officials at his home in Sau Mau Ping, Hong Kong on 10th May. He is alleged to have made available more than 600 songs and 20 movies on his website. Jimmy Tam Yat-keung, head of customs' copyright investigation division, said, "Initial investigation showed that the suspect did this for his own interest and no profit was involved. He probably liked to set up websites."

In related news, in an interview with *The Guardian* Real Networks CEO Rob Glaser has claimed, "About half the music on iPods is music obtained illegitimately either from an illegal peer-to-peer networks or from ripping friends' CDs, which is illegal." He also said, "If you want interoperable music today, there is a very easy solution: it's called stealing... it's the only way to get non-copy protected, portable, interoperable music."

Do consumers deserve interoperable music?

More information:

http://hongkong.scmp.com/hknews/ZZZL8PDQ3ME.html

http://www.reghardware.co.uk/2006/05/11/half_ipod_music_stolen_real_says/

Schneier Slams Subversion of Ownership

Writing in Wired, the well-known security expert, Bruce Schneier has hit out at companies who try to take away our control of our own computers, “You own your computer, of course. You bought it. You paid for it. But how much control do you really have over what happens on your machine?”

More information:

http://www.wired.com/news/columns/1,70802-0.html

The Spammers are Winning

Anti-spam firm Blue Security has a controversial technique: they established a ‘Do Not Intrude Registry’ and participants downloaded a small tool, called Blue Frog, which systematically flooded the websites of spammers with opt-out messages.

In an escalating conflict in April, a spammer known as PharmMaster used increasingly disruptive techniques to attack Blue Security’s business. This culminated in PharaMaster launching a massive denial of service attack against organisations associated with Blue Security. The attack disrupted the net operations of five top-tier hosting providers in the US and Canada, as well as a major DNS provider for several hours.

Faced with this level of aggression, Blue Security has given up, "It's clear to us that [quitting] would be the only thing to prevent a full-scale cyber-war that we just don't have the authority to start," Reshef Blue Security CEO Eran Reshef told washingtonpost.com. "Our users never signed up for this kind of thing."

Regardless of whether you think Blue Security’s methods were acceptable, this makes it clear that, on the Internet, the biggest bully wins, and the spammers are the biggest bullies.

More information:

http://www.theregister.com/2006/05/17/blue_security_folds/
http://www.washingtonpost.com/wp-dyn/content/article/2006/05/16/AR2006051601873.html

Virus Nuclear Leak

Sensitive information about Japanese power plants has leaked online from a virus-infected computer for the second time in less than four months.

More information:

http://www.theregister.com/2006/05/17/japan_power_plant_virus_leak/

Zero–Day Word Vulnerability

A US-based company was targeted with emails that were sent to the company from the outside but were spoofed to look like internal emails. The mail had a Word file as an attachment that used a previously–unknown vulnerability to install a backdoor, hid it with a rootkit and allow unrestricted access to the machine for the attackers, operating from a host registered under the Chinese 3322.org domain. 3322.org is a free host bouncing service in China; anybody can register any host name under 3322.org so this does not indicate that China was the origin of the attack.

Microsoft Security Advisory (919637) describes the following workarounds:

- Run Word in Safe Mode (winword.exe /safe)
- Open Word documents with the Word 2003 Viewer
- Do not use Word as the email editor in Outlook

The advisory does not recommend using a different office suite, for some reason, though it is unlikely that other office suites have the same vulnerability.

More information:

http://www.theregister.com/2006/05/22/trojan_exploit_word_vuln/

http://ciac.llnl.gov/ciac/bulletins/q-202.shtml

http://www.f-secure.com/weblog/archives/archive-052006.html#00000883

http://www.microsoft.com/technet/security/advisory/919637.mspx

http://www.openoffice.org/

“Fingerprints” for Digital Cameras

Researchers at Binghamton University, State University of New York have applied for two patents for techniques to reliably link digital images to the camera that took them. The process analyses images, looking for variations caused by irregularities in the manufacturing process of the camera and its sensors that are unique to each camera. The analysis was 100% accurate in tests with 27,000 images taken by nine cameras. The technique can also indicate where an image has been modified, by showing where the expected pattern for a camera is missing.

The researchers expect the technique to be useful to law enforcers investigating child pornography cases.

More information:

http://www.eurekalert.org/pub_releases/2006-04/bu-bur041806.php

SpamOrHam.org Launched

John Graham-Cumming, the well-known anti-spam researcher, has recently launched SpamOrHam.org, a website to compare human and machine spam classification. Visitors can spend a few minutes reading messages and judging whether they are spam or ham (or

uncertain). The messages are from the Enron corporation, and were released into the public domain during the investigations into the organisation's bankruptcy.

References:

http://spamorham.org/
http://www.f-secure.com/weblog/#00000888
http://www.jgc.org/blog/2006/05/theres-one-born-every-minute-spam-and.html

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/