Yui Kee Computing Ltd.

Newsletter

October 2004

Contents

Incident Update

The main news this month is the number of new vulnerabilities Microsoft announced on its "Patch Tuesday" (see story below) and multiple new Bagle variants appearing on 29 October.

- Wed Oct 13 09:01:58 2004 TREND: OCT_12_MS_VULNERABILITIES High
- Thu Oct 14 23:02:19 2004 NAI: W32/Netsky.ag@MM Medium
- Tue Oct 19 09:32:06 2004 VM: Still waiting for JPEGs to kill the Internet
- Tue Oct 19 16:02:06 2004 NORMAN: Netsky.P Medium
- Mon Oct 25 15:31:28 2004 CA: Win32.Lovgate.AB
- Mon Oct 25 21:16:34 2004 VM: Still waiting for JPEGs to kill the Internet, part 2
- Tue Oct 26 23:46:33 2004 TREND: MS_VULNERABILITIES_OCT2004 High
- Fri Oct 29 16:46:34 2004 FSC: New Bagle variant spreading again
- Fri Oct 29 17:16:31 2004 TREND: WORM_BAGLE.AT Medium
- Fri Oct 29 18:01:54 2004 NORMAN: Bagle.AQ Medium
- Fri Oct 29 18:31:48 2004 NAI: W32/Bagle.bb@mm Medium
- Fri Oct 29 19:16:37 2004 SARC: W32.Beagle.AV@mm L3
- Fri Oct 29 20:46:36 2004 NORMAN: Bagle.AQ High
- Fri Oct 29 22:46:37 2004 NAI: W32/Bagle.bd@MM Medium
- Sat Oct 30 01:01:49 2004 TREND: WORM_BAGLE.AU Medium

Microsoft Releases Ten Security Patches on Octobers' Patch Tuesday

On 12 Oct 2004 (Tuesday, US time), Microsoft released ten security patches for Windows, Office and Exchange Server. Seven are rated as critical and the other three are rated as important. Users of the affected software are recommended to upgrade using Windows Update.

Seven were for Windows:

http://www.microsoft.com/technet/security/Bulletin/MS04-029.mspx (Important)
http://www.microsoft.com/technet/security/Bulletin/MS04-030.mspx (Important)
http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx (Important)
http://www.microsoft.com/technet/security/Bulletin/MS04-032.mspx (Critical)
http://www.microsoft.com/technet/security/Bulletin/MS04-034.mspx (Critical)
http://www.microsoft.com/technet/security/Bulletin/MS04-037.mspx (Critical)
http://www.microsoft.com/technet/security/Bulletin/MS04-038.mspx (Critical)

One critical patch for Office:

http://www.microsoft.com/technet/security/Bulletin/MS04-033.mspx (Critical)

And two for Exchange Server:

http://www.microsoft.com/technet/security/Bulletin/MS04-035.mspx (Critical)
http://www.microsoft.com/technet/security/Bulletin/MS04-036.mspx (Critical)

More information:

http://www.microsoft.com/security/bulletins/default.mspx
http://www.microsoft.com/technet/security/bulletin/ms04-oct.mspx

Google Phishing Vulnerabilities

Netcraft discovered a vulnerability in the application used to search Google's own site on the 20th October. The problem would have allowed fraudsters to inject their own content onto Google's site, thus making it far more likely that people would believe a scam. Google fixed the problem less than two days after being notified.

However. Salvatore Aranzulla, an Italian journalist, discovered a cross-site scripting vulnerability in the Google Desktop search application on 25th October. Google Desktop is currently offered as a beta test service, but there have been privacy concerns, which this vulnerability will exacerbate.

More information:

http://news.netcraft.com/archives/2004/10/22/google_fix_second_phishing_vulnerability.html

http://news.netcraft.com/archives/2004/10/25/new_google_desktop_exploit_discovered.html

Net Extortion

Online gambling site Blue Square has revealed that a telephone caller threatened to send out child abuse pictures in emails in its name unless it paid €7,000. The threat followed a DDoS attack on the site. "Two sites have come under 'distributed denial of service' attacks this week, Blue Square, and William Hill. However, Blue Square then received a follow-up phone call making the child pornography threat." a spokesman for the UK's Hi-Tech Crime Unit told BBC News.

Gambling sites have proved a popular target of criminals, presumably because they handle large amounts of money, often concentrated into short periods of time around sporting events.

More information:

http://news.bbc.co.uk/1/hi/business/3957757.stm

http://www.theregister.com/2004/10/28/blue_sq_blackmail/

Security Myths and Facts: Windows vs. Linux

With another ten important security patches (seven of those critical) released by Microsoft this month, and daily security announcements concerning Open Source systems, many people are looking for a comprehensible answer on which OS is "secure". Microsoft's "Get the Facts" information is a marketing campaign. Nicholas Petreley, writer, Linux guru and analyst, has published a new analysis addressing Microsoft's major points in detail.

However, security cannot be packaged in a box or OS; it is greatly affected by how systems are used.

More information:

http://www.theregister.com/2004/10/22/linux_v_windows_security/

http://www.theregister.com/security/security_report_windows_vs_linux/

http://www.microsoft.com/windowsserversystem/facts/analyses/vulnerable.mspx

World First: HK Police Introduce an Emergency Number Requiring Registration

People with speech or hearing problems can now send SMS text messages to the Police, but only if they have pre-registered for the service. This is an upgrade of the previously available 992 Fax Emergency Hotline, and it is the first SMS Emergency Number in the world.

More information:

http://www.info.gov.hk/police/hkp-home/english/smsemg.doc

Humour: Catching Virus Writers

http://ars.userfriendly.org/cartoons/?id=20040912

Defining Malware

Sophos has recently been taken to task for detecting dialler software produced by Coulomb Ltd, a UK-based developer. Sophos originally classified the software as a Trojan, but David Knell, chief exec of Coulomb Ltd, said its application did "exactly what it says on the tin". Its dialler is offered as a payment option on various adult entertainment (sex) websites. The dialler clearly states that a premium rate number will be used, and spending is capped at £20 per session in line with recommendations from premium rate regulator ICSTIS, Knell says.

Sophos confirmed that it had removed detection of the dialler, following legal advice. However, some users questioned the move, citing that Sophos specialises in the enterprise market, and few enterprises authorise the use of porn diallers on their computers. Some security software may still detect the dialler, Symantec has categorised it as an Expanded Threat, which are only detected by some of the company's products.

Deciding which software should be detected by security applications has always been a difficult decision. In the early days, some researchers fiercely advocated that anti-virus software should only detect viruses - programs capable of replicating themselves, and not programs that were intended to be viruses, but did not work, or corrupted samples that were incapable of spreading etc. Nowadays, anti-virus software should probably be called

anti-malware software. Later, there was disagreement over whether Back Orifice and NetBus should be detected, when the largely similar remote control software PCAnywhere was not.

The best option is to categorise the software accurately, and to let the responsible administrator choose which categories to allow, in line with the organisation's security policy. However, occasional mis-classifications are almost inevitable.

More information:

http://www.theregister.com/2004/09/30/sophos_porn_dialler_row/

US Congress Passes Anti-Spyware Law

The SPY ACT (Securely Protect Yourself Against Cyber Trespass), outlaws computer technology that downloads programs onto users' computers without their permission and makes it illegal to hijack control of a user's computer, expose users to pop-up ads that can't be closed, modify a user's personal settings, and download personal information without permission. The bill was passed by 399 votes for to 1 against.

Rep. Joe Barton (R-Texas), chairman of the House Committee on Energy and Commerce says he hopes the United States can set a standard for international spyware law that would be adopted throughout the world. However, Hong Kong's Computer Crimes Ordinance already outlaws unauthorised addition of software to computers. The main difficulty appears to be in identification of the culprits.

More information:

http://www.pcworld.com/news/article/0,aid,118069,00.asp

HK Intellectual Property Department fights Piracy with Game Give-Away

The game, enticingly called "Anti Piracy Action Team" (APAT), was developed by the Hong Kong Polytechnic University and aims at delivering copyright protection ideas to young people in an entertaining format.

More information:

http://production.mic.polyu.edu.hk/%7Eapat/index.htm

http://www.info.gov.hk/ipd/eng/news/news/IPD games-e _ISD_.pdf

ISP DoS

How reliable is your Internet connection? A recent study by Dutch group Bits of Freedom found that seven out of ten ISPs test shut down a website without either scrutinising the "offending" website or demonstrating a basic understanding of copyright law when faced with unsubstantiated legal threats.

http://www.theregister.co.uk/2004/10/14/isp_takedown_study/

Sasser Trial Delayed

Sven Jaschan's trial in Germany for computer sabotage amounting to a total of $157,000 related to the spread of the Sasser worm has been rescheduled for January 2005. The court in Verden, a North German town decided to delay the case because it proved impossible to agree an earlier date with all the parties involved.

Security experts have received the delay with disappointment. "A strong message needs to be sent out to the computer underground that writing and distributing viruses is criminal behaviour," said Graham Cluley, senior technology consultant for Sophos. "Home users and companies around the world who were struck by the Netsky and Sasser worms will be watching with interest to see what happens in this case."

More information:

http://www.sophos.com/virusinfo/articles/sasserdelay.html

Vmyths Stands Up for a Laugh

Rob Rosenberger, creator and editor of Vmyths, the website that aims to use humour to educate about computer virus myths, hoaxes, urban legends and hysteria, has announced he has started in stand-up comedy to hone his skills. Writing in a special edition of his newsletter, Rob emphasised the potential of stand-up comedy for his professional development, "I've learned many of today's best writers did stand-up at one time or another. … These people use stand-up as a blade sharpener. It gives them the edge they need in their real jobs. I'm a computer security critic, and right now I'm sharpening my blade."

Rob will be performing at Penguin's Comedy Club, Cedar Rapids, IA on 24 November 2004, 8pm CT, and generously offered, "I'll even waive your cover charge if you say 'Vmyths' to the cashier".

Rob has a strong belief in the educational potential of humour, "we need more humor in the computer security world". [*I thought that was Microsoft's role, no, wait - that's tragedy… Ed.*]

Scientific Literacy

Lord May of Oxford, the president of the world's oldest scientific research body, the Royal Society, has told the UK Government that scientific reasoning must be a core part of school education up until the age of 19.

http://www.theregister.co.uk/2004/10/27/scientific_education/

http://www.royalsoc.ac.uk/templates/press/releasedetails.cfm?file=560.txt

WiFi Dangers

A Sydney man who installed a wireless access point in his garden became the focus of an anti-Terrorist raid. Neighbours thought it might be a bomb.

http://www.theregister.com/2004/10/29/wireless_ap_bomb_scare/

Return of the Removable Media Virus

In recent years we have been almost overwhelmed by the prevalence of viruses and worms spreading across networks. However, we have a wake-up call that viruses on removable media are still a threat. W32/Barcos.A copies itself to floppies and CD-Rs, and it also drops another type of virus not in the news recently, a Word Macro virus, W97M/Bacros.A, and carries a destructive payload. When infecting CD-Rs, it creates an AUTORUN file, so that it will get executed automatically when the disk is inserted into a default-configuration Windows PC.

W32/Barcos.A is reported to be spreading in Scandinavia.

More information:

http://www.theregister.com/2004/10/14/bacros_retro_virus/

http://www.f-secure.com/v-descs/bacros_a.shtml

Sender-ID On-Hold, SPF Marches On

The Internet Engineering Task Force has disbanded its MTA Authorization Records in DNS (MARID) working group because it failed to reach a consensus regarding whether to ratify the proposed Sender-ID specification, which combines Microsoft's Caller-ID and the Sender Policy Framework (SPF). However, adoption of SPF is still growing, with 180,000 domains known to be publishing SPF records as at 27th October.

More information:

http://www.messagelabs.com/emailthreats/intelligence/reports/monthlies/september04/

http://spf.pobox.com/adoption.html

Steve Ballmer Reaffirms Commitment to Security

Speaking to the UK press, Microsoft CEO Steve Ballmer recognised that security is a never-ending battle, "We will be working on Trustworthy Computing for the rest of my days at Microsoft - which I hope are many. There are bad people out there in cyberspace and they are not going to go away. We are going to have to be vigilant. That's going to last for the duration".

Some analysts have suggested that Microsoft might get into the security business itself, possible by acquiring a major anti-virus or firewall company, but Ballmer refused to elaborate.

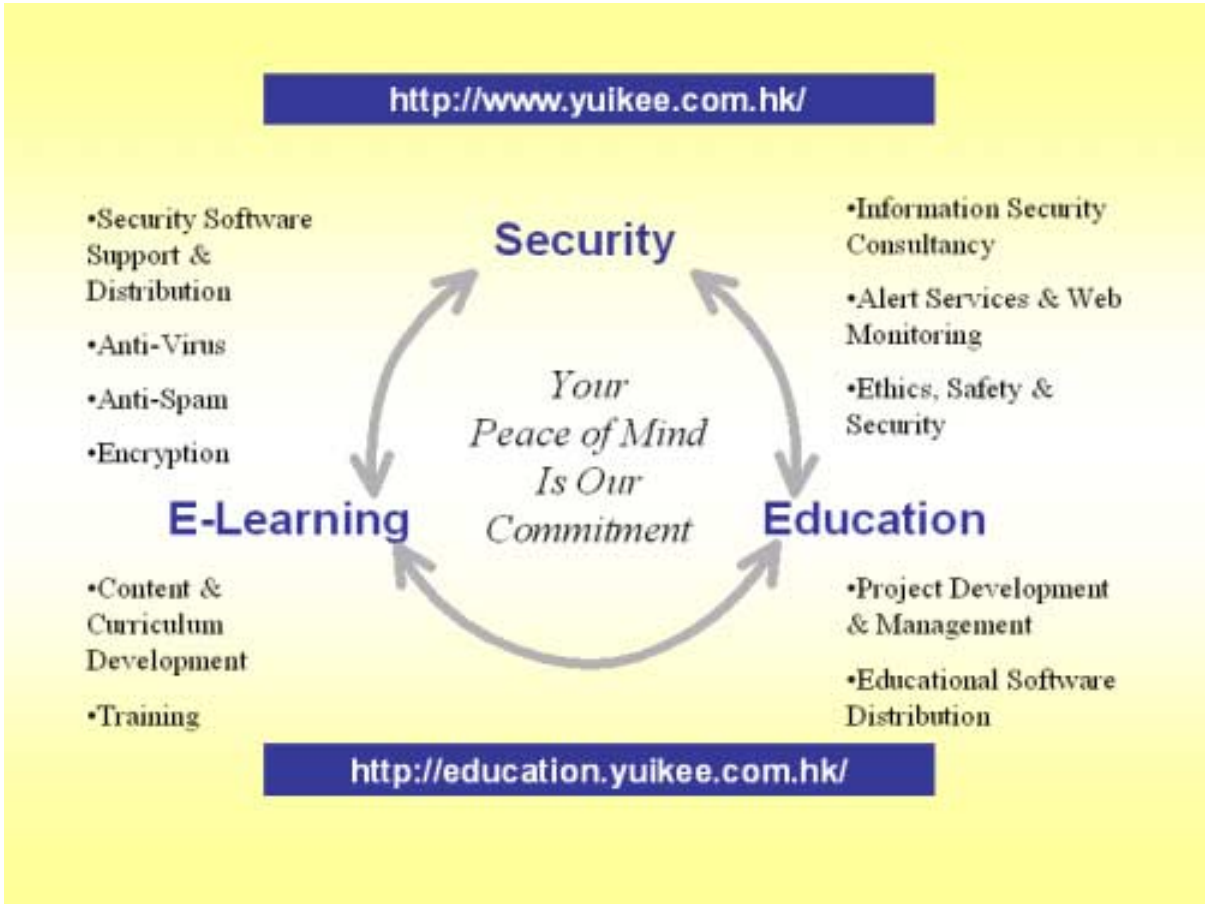
Ballmer did highlight the concept of "isolation" - preventing a computer from reconnecting to a corporate network until it was up-to-date with the latest security patches and virus definitions, promising that Microsoft would ship the technology "certainly by Longhorn".

More information:

http://software.silicon.com/security/0,39024655,39124616,00.htm

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: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/