Yui Kee Computing Ltd.

Newsletter

January 2006

Contents

Contents 1
Incident Update 1
Editor's Notes 1
Free SSH Tectia Training for System Integrators 2
Zero-Day Exploit: WMF Saga Continues 2
    Microsoft Releases Patch: "Patch Tuesday" Schedule in Tatters 3
    Microsoft Exploits WMF Saga to eliminate NT 3
    Chinese Hackers Exploit WMF Vulnerability to Attack UK Government Targets 3
1 in 20 MMS Messages Virus Infected 4
Selling Malware 4
False Claims 5
Writs by Email 5
Be Your Own Intelligence Agency 5
F-Secure Security Bulletin: Vulnerability in ZIP and RAR Handling 5
20th Anniversary of PC Virus 5
Bill Gates Predicts "Spam will be Solved" in Two Years 6
Zombie Merchant Pleads Guilty 6
Oracle Accuses Litchfield 7
Public Consultation on HK Anti-Spam Bill 7

Incident Update

- Sat Jan 7 09:01:29 2006 FSC: Microsoft's WMF patch is out 2
- Sat Jan 21 00:31:37 2006 FSC: Nyxem.E is becoming more widespread 2

Editor's Notes

Twenty years after the first PC virus, the application and practice of Information Security is still lagging the threats dangerously. Possible attacks, that were originally dismissed as speculation and hysterical fear mongering, have not only occurred but become commonplace. Time and again, we have seen viruses developed for new platforms, then become widespread, and the MMS platform is simply the most recent to fall victim.

Developers have a wide range of reactions to flaws in their products: Oracle is, perhaps, among the worst, with a head-in-the-sand, "security through obscurity" approach: blaming the messenger. For problems they have failed to fix. Microsoft has greatly improved its approach to security, but it still seems to have left technical decisions about the severity of problems and how to describe them in the hands of its marketing department, only breaking its monthly patch cycle after considerable pressure. The spin-doctoring can also be seen in Microsoft's Security Bulletin, under Mitigating Factors we are reassured, "…an attacker would have to persuade users to visit the Web site…". That's OK then, it is not as if our users visit web sites frequently.

F-Secure also reminds us with their archive handling vulnerability that no developer, not even a security developer, is immune to security flaws.

Meanwhile, the attackers are becoming more professional, and more focused on profit, the case of the Zombie Merchant is just the tip of the iceberg of an underground economy. Worse, in some cases connectivity is so taken for granted that protective measures can cause significant loss, as in the Writs by Email case.

In the Chinese Calendar, we are now starting the year of the Fire Dog. This is linked to optimism, openness, social rights and wrongs, and defence. Therefore, I hope we can work for and see improvements in responsible disclosure, computer crime legislation and our systems defences.

Kung Hey Fat Choi

Allan Dyer

Free SSH Tectia Training for System Integrators

Yui Kee Computing Limited and SSH Communication Security Corp. will jointly organize a Free Seminar on SSH Tectia Solutions in February 2006. This seminar is intended for solution consultants, system integrators and system engineers. It introduces the SSH Tectia Solution and the new SSH G3™ Technology.

SSH Tectia Solution is a comprehensive application security solution targeted toward government, financial and large corporate organizations.

SSH as a technology is a de facto security technology supported by leading IT vendors and used by thousand of organizations worldwide. Traditionally however, customers procure SSH products on a case-by-case basis, mostly for system administration purpose.

With the introduction of the SSH Tectia Solution, SSH becomes a multi-platform / multi-application security solution, based on the existing SSH infrastructure. This allows IT solution providers to dramatically improve their solutions and services to their customers while lowering the system's cost of ownership, leveraging the trusted and reliable SSH technology.

Through this seminar, SSH hopes that the participants will be able to leverage their existing SSH related business towards higher added value solutions and services.

Date: 20 February 2006, 10:00 - 17:00

Speakers: JB Dumerc, Vice President, SSH Communications Security Corp

Nicolas Gabriel-Robez, SSH Communications Security Corp

Katsuhiro Shogawa, SSH Communications Security Corp

For enquiries or **registration**, please contact us: +852 28708500 or info@yuikee.com.hk

Zero-Day Exploit: WMF Saga Continues

Last month we reported on the latest security vulnerability found in Microsoft's products. This month saw a large number of developments in the case. While the world waited for a patch from Microsoft, security researcher Ilfak Guilfanov took the unusual step of releasing his own patch. Security commentators advised using the unofficial patch, citing Guilfanov's good reputation, and the lack of any other available response as reasons to go against normal security wisdom: only use patches from the original vendor.

By the second of January, we had the startling revelation that the vulnerability was not a bug at all, but a documented feature of WMF files. Despite all the effort Microsoft has been putting into making their products more secure, it seems that no-one got round to checking the

specifications and their implications. Mistakes like buffer overflows might have been made far less likely, but who knows how many more basic design flaws remain?

Microsoft Releases Patch: "Patch Tuesday" Schedule in Tatters

On the sixth of January, breaking their "Patch Tuesday" schedule, Microsoft released the official patch for the vulnerability. This really calls into question the purpose of "Patch Tuesday", it is clear that a sufficiently "important" vulnerability can result in a schedule change. This destroys the supposed advantage of bundling patches into a once-a-month package: administrators still face the challenge of unplanned maintenance. So what defines the "importance" of the vulnerability? Hopefully, it would be a rational evaluation of the problem. However, as late as the third of January reports showed no sign of the early release. They had already verified the vulnerability, the importance of the threat was known. At that stage, the most useful information for administrators would be to know that Microsoft was intending to release the patch as soon as testing was complete. The advisory still played down the importance of the vulnerability, "…Microsoft's intelligence sources indicate that the scope of the attacks are not widespread", which was true, but that could change in minutes, as numerous incidents of fast spreading malware have shown.

Two possibilities come to mind: Microsoft intended to stick to the Patch Tuesday schedule – in which case, why did it change its mind? The technical situation had not changed, so that suggests the mounting media pressure influenced them. Alternatively, they always intended to release the patch as soon as testing was complete, which implies that the intention was kept secret to avoid negative comment about them racing to release a fix. In either case, it is clear that the marketing department is in control of Microsoft's security response.

Microsoft Exploits WMF Saga to eliminate NT

Users of older Microsoft operating systems are in a worse position. Microsoft will only release updates for "critical" security problems on Windows 98, 98SE and ME; so, magically, the WMF vulnerability has been labeled "non-critical" for these operating systems, with the justification that an "exploitable attack vector" has not been identified. Did they look?

Windows NT and pre SP4 versions of Windows 2000 have reached the end of their support lifecycles, so they will go unpatched, no matter how critical the problem is. Microsoft recommends users of these systems to ~~pay more money to Microsoft~~ upgrade to later editions of Windows.

Chinese Hackers Exploit WMF Vulnerability to Attack UK Government Targets

Email security company MessageLabs has blocked targeted attacks on British MPs and other UK Government sites. Messages that apparently originated in China carried a trojan utilizing the WMF vulnerability. There is no indication whether the attack was initiated by the Chinese Government, independent Chinese hackers, or, indeed, by another attacker making use of compromised computers in China.

More information:

http://en.wikipedia.org/wiki/Windows_Metafile_vulnerability#Workaround

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

http://isc.sans.org/diary.php?rss&storyid=996

http://www.f-secure.com/weblog/archives/archive-122005.html#00000756

http://www.f-secure.com/weblog/archives/archive-122005.html#00000757

http://www.f-secure.com/weblog/archives/archive-012006.html#00000758

http://www.f-secure.com/weblog/archives/archive-012006.html#00000759

http://www.f-secure.com/weblog/archives/archive-012006.html#00000760

http://www.f-secure.com/weblog/archives/archive-012006.html#00000761

http://www.f-secure.com/weblog/archives/archive-012006.html#00000762

http://www.microsoft.com/technet/security/Bulletin/MS06-001.mspx

http://www.theregister.co.uk/2006/01/06/microsoft_wmf_vulnerability_patch/

http://www.theregister.co.uk/2006/01/05/secfocus_zeroday/

http://www.theregister.com/2006/01/13/security_wmf_microsoft/page2.html

http://www.theregister.com/2006/01/24/uk_gov_wmf_attack/

1 in 20 MMS Messages Virus Infected

Fortinet has found that an alarming 5% of MMS messages passing through a large mobile service provider in Germany were infected with a virus, Commwarrior.A in a third of cases. Commwarrior.A has been reported in at least 15 countries.

Clearly, mobile viruses are no longer just a theoretical possibility, or a rare nuisance; they are a growing threat. This should be no surprise to readers of this newsletter; our August 2005 issue warned that capable mobile devices were becoming common enough for epidemics to occur. Organisations that rely on mobile communications and service providers should implement protection strategies.

More information:

http://www.fortinet.com/FortiGuardCenter/roundup_december.html

http://www.f-secure.com/weblog/archives/archive-052005.html

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

http://www.f-secure.com/wireless/news/items/news_2005062800.shtml

http://www.yuikee.com.hk/info-ctr/newsletter/ykcl-news05-08.pdf

Selling Malware

Dutch company Frame4 Security Systems plans sell access to their malware collection, starting from 1 February. The scheme is called MD:Pro. The service is promoted as offering "developers of security systems and anti-malware products a vast collection of downloadable malware from a secure and reliable source". They claim that many of the samples would be "undetectable" by anti-virus products, which therefore suggests that the samples may not be viruses.

Anthony Aykut of Frame4 Security Systems claimed, "It will be a closed list and applications will be checked. Members would not be allowed to distribute virus samples." Members of the anti-virus industry have reacted negatively to the scheme, "The Malware Distribution Project is not that different from many of the VX [virus writer] websites that exist on the net. It presents itself as being available for research purposes, but mentions nothing about restricting access to trusted, responsible members of the security community. Indeed, its barrier for entry appears to be hard cash rather than trust," said Graham Cluley of Sophos.

More information:

http://www.frame4.net/mdpro

http://www.theregister.com/2006/01/10/malware_distribution_project/

False Claims

The US Federal Trade Commission has obtained a ruling that found Spyware Assassin and TrustSoft made false and misleading claims about finding and removing spyware. The companies must pay a total of over US$2 million.

More information:

http://www.theregister.com/2006/01/10/ftc_spyware/

Writs by Email

An English Judge in a maritime arbitration has ruled that serving a writ by email is just as valid as doing so by post or fax, and the fact that the email had been deleted as probably spam was an irrelevant internal failing. The judge, Mr Justice Christopher Clarke said, “The position is, to my mind, no different to the receipt at a company’s office of a letter or telex which, for whatever reason, someone at the company decides to discard."

More information:

http://www.theregister.com/2006/01/10/lawsuit_started-by_email_is_valid/

Be Your Own Intelligence Agency

The Internet has made a vast quantity of information (and misinformation) easily available on every conceivable topic. Now Tom Owad has demonstrated how to use freely available resources to identify and locate “subversives”.

More information:

http://www.applefritter.com/bannedbooks

F-Secure Security Bulletin: Vulnerability in ZIP and RAR Handling

F-Secure has announced that it is possible to create specially crafted ZIP archives that cause a buffer overflow in many versions of their anti-virus products. This allows an attacker to execute code of his choice on affected systems. It is in addition possible to create malformed RAR- and ZIP-archives that cannot be scanned properly. This can lead to a false negative scan result.

Patches have been released, users of F-Secure Internet Security 2004 – 2006, F-Secure Anti-Virus 2004 – 2006, and F-Secure Personal Express have been updated authomatically.

F-Secure Corporation thanks Thierry Zoller for bringing this issue to their attention.

More information:

http://www.f-secure.com/security/fsc-2006-1.shtml

http://www.zoller.lu

20th Anniversary of PC Virus

The PC virus celebrates its 20th year of existence following the detection back in January '86 of the boot sector virus, Brain, which infected computers via floppy disk. While the virus Brain itself was relatively harmless, it set in motion a long chain of events leading up to today's virus situation.

Boot sector viruses, now long extinct along with the floppy disk, held a relatively long reign from 1986 to 1995. Since transmission was via disk from computer to computer, infection

would only reach a significant level months or even years after its release. This changed in 1995 with the development of macro viruses, which exploited vulnerabilities in the early Windows operating systems. For four years, macro viruses reigned over the IT world and propagation times shrank to around a month from the moment when the virus was found to when it was a global problem.

As email became more widespread, so followed email worms and individual worms which reached global epidemic levels in just one day. Most notable in this connection was one of the very first emails worms, Loveletter aka ILOVEYOU, which caused widespread havoc and financial loss in 1999 before it was brought under control.

In 2001, the transmission time window shrank from one day to one hour with the introduction of network worms (such as Blaster and Sasser), which automatically and indiscriminately infected every online computer without adequate protection. Email and network worms still today continue to cause havoc in the IT world.

At present there are over 150,000 viruses and the number continues to grow rapidly. The biggest change over these 20 years has not been in the types of viruses or amount of malware: rather it has been in the motives of the virus writers.

"Certainly the most significant change has been the evolution of virus writing hobbyists into criminally operated gangs bent on financial gain," says F-Secure's Chief Research Officer Mikko Hypponen. "And this trend is showing no signs of stopping."

Hypponen continues: "There already are indications that malware authors will target laptop WLANs as the next vector for automatic spreading worms. Whatever the next step might be, it will be interesting to see what kind of viruses we will be talking about in another twenty years time – computer viruses infecting houses, perhaps?"

More information:

http://www.f-secure.com/news/items/news_2006011900.shtml

Bill Gates Predicts “Spam will be Solved” in Two Years

Speaking at the World Economic Forum meeting in Davos, Switzerland, Bill Gates has announced a three-part plan to eradicate spam in two years. In fact, as he spoke in January 2004, you should be experiencing a sudden drop in the size of your in-box just about… now.

More information:

http://www.theregister.com/2004/01/26/well_kill_spam_in_two/

http://www.theregister.com/2006/01/24/gates_spam_death_prediction/

Zombie Merchant Pleads Guilty

A 20-year-old California man, Jeanson James Ancheta of Downey, California, has pleaded guilty to charges that he sold access to networks of compromised PCs and made money from illicitly installed adware. "This is the first case to charge someone for using bots for generating profits," said James Aquilina, Assistant U.S. Attorney for the Central District of California.

More information:

http://www.securityfocus.com/news/11353

http://www.theregister.com/2006/01/24/zombie_herder_pleads/

Oracle Accuses Litchfield

David Litchfield, principal researcher of Next-Generation Security Software, disclosed a critical vulnerability in Oracle's application and Web software during a presentation at the Black Hat Federal security conference. Litchfield notified Oracle of the problem last October, and he also published a workaround the same day as his Black Hat presentation.

Duncan Harris, senior director of security assurance for Oracle, condemned this responsible behaviour, "What David Litchfield has done is put our customers at risk."

More information:

http://www.theregister.com/2006/01/26/security_researcher_versus_oracle/

http://www.securityfocus.com/archive/1/423029

Public Consultation on HK Anti-Spam Bill

Hong Kong's Secretary for Commerce, Industry and Technology (SCIT), John Tsang, has announced the start of public consultation on the "Unsolicited Electronic Messages Bill".

Key features of the Government's approach are the adoption of an opt-out regime, extra-territoriality for messages with a "Hong Kong connection", and a central "do not call register" that would not cover email.

Please make your opinions known to the Commerce, Industry and Technology Bureau.

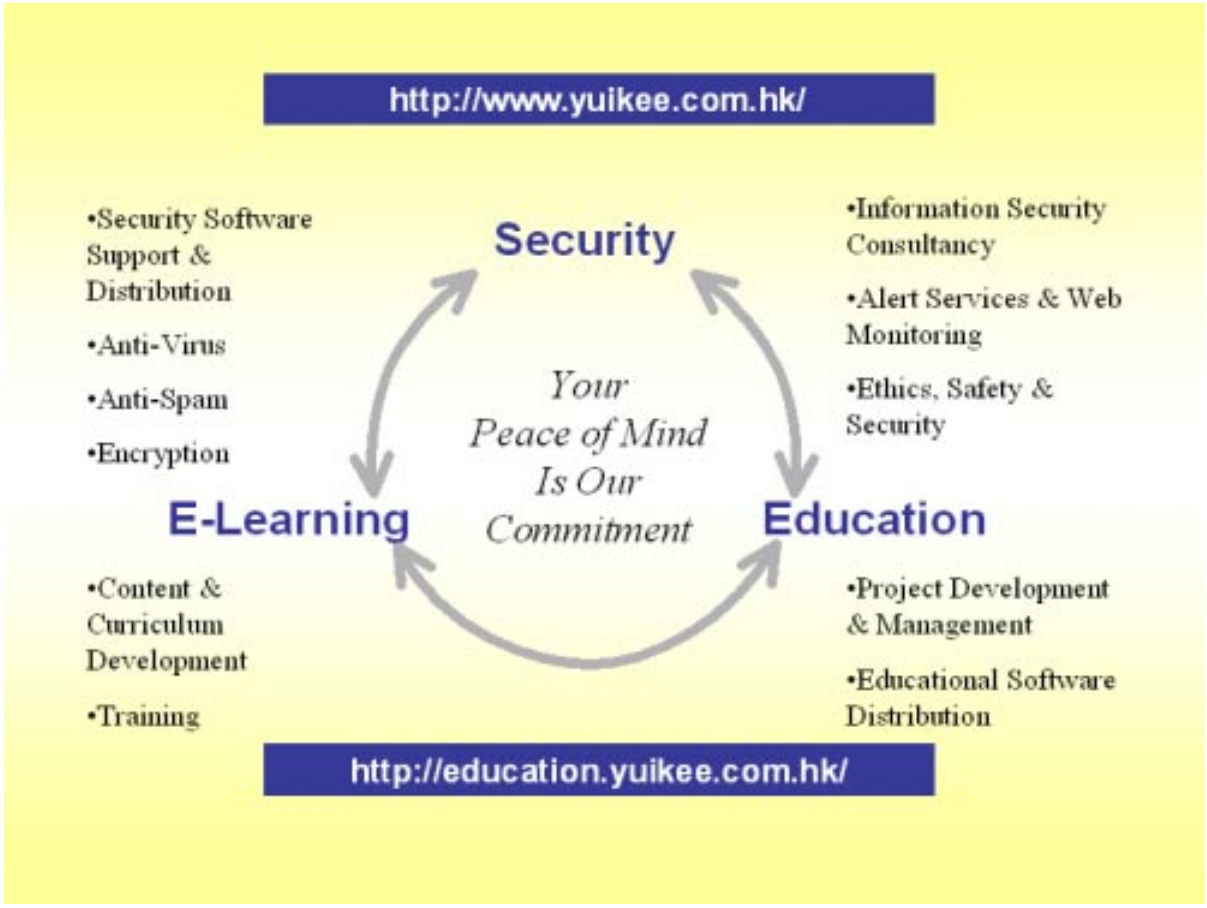
More information:

http://www.info.gov.hk/gia/general/200601/20/P200601200244.htm

http://www.citb.gov.hk/ctb/eng/paper/pdf/UEM(Eng)-final.pdf

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/