Yui Kee Computing Ltd.

Newsletter

January 2002

Contents

Editors Notes

We are happy to have several new contributors this month, including Robert Sim of CyberGuard. We do welcome interesting contributions related to Information Security, or polite discussion on the issues and topics raised.

Allan Dyer

Virus Update - New Platforms

Sophos, a world leader in corporate anti-virus protection, has discovered the first virus capable of infecting Macromedia Flash files commonly used on popular websites.

The SWF/LFM-926 virus targets webmasters who use Macromedia Flash to make their websites more attractive with animation and special effects. End users who browse an affected website may become infected if they download and open the Macromedia Flash file on their computer.

"Computer users visiting snazzy sites would get more than they bargained for if they downloaded this virus," said Graham Cluley, senior technology consultant for Sophos Anti-Virus. "The Macromedia Flash virus is not yet in the wild, but it is clear proof that virus writers continue to search for new ways to infect computer users. The best defence is to keep your security software up-to-date and practise safe computing."

Webmasters should put in place procedures and policies to ensure the integrity of the code they place on their websites, whether it be obviously executable (in the case of, for instance, EXE and COM files) or Macromedia Flash movies.

Sophos has issued a detailed analysis and protection against the SWF/LFM-926 virus.

January also saw the first virus for the .Net platform. Called Donut, it is a simple, direct action infector. The virus author posted samples of this virus directly to several anti-virus companies on January 9th, 2002. Jimmy Kuo, director of anti-virus research for McAfee Anti-Virus Emergency Response Team, once suggested that it takes virus writers about 2 years to release

the first virus for a new, virus-supporting platform. Donut is probably the first virus to be released before the (official) release of the platform it targets. Other than that, it is unremarkable - there is certainly no surprise that a virus can be written for .Net, all general-purpose operating systems are vulnerable to viruses.

F-Secure has a detailed analysis of Donut.

Idiotic Challenge

Allan Dyer

In an open letter responding to a vnunet.com article that suggested Linux will be a target of virus writers, David F. Skoll has challenged anti-virus companies to infect his computer with a virus. His challenge is highly irresponsible - because viruses spread, their creator looses control over them. This is like someone in a city with no fire service claiming their house is fireproof and challenging people to burn it down. Maybe they are correct, but if they are not, the whole city burns. No anti-virus company will do this, and Mr. Skoll will claim a win by default.

Mr. Skoll 'debunks' three 'myths':

"Myth: Widespread use equals widespread abuse" - pointing to data of Apache vs. Microsoft webserver defacement as evidence. However, he later contradicts this when explaining why Linux viruses are unlikely, "a virus which exploits a software bug in Outlook is far more likely to propagate than one which exploits a software bug on a Linux e-mail client. This is simply because of the huge array of Linux e-mail clients in use" and, "On Linux, this is harder. There is no uniform way for a virus to read your address book".

"Myth: Linux is not a secure OS" - He then immediately contradicts himself by saying, 'In fact, no commodity OS is "secure".' In fact, I agree with his general sentiment - a default Linux installation is more secure than a default Windows installation. Additionally, while it is possible to improve security on both Linux and Windows systems, it is more likely that a randomly chosen Linux system will be more secure because a higher proportion of people setting up Linux machines are experienced and knowledgeable.

"Myth: It is easier to write viruses if you have the OS source code" - Here, he cites independent code audit as the advantage that makes open source more secure. True, but viruses do not need security bugs to spread - Melissa used perfectly normal Word macro capabilities. In order to create viruses, the writer needs a programming environment, for several years most of the prevalent viruses were Word Macro viruses because the necessary programming environment (Word Basic, or VBA) was installed free with Word. It is not the OS source code as such, but the detailed programming documentation that implies which is important. Mr. Skoll also asked why there are so few Linux and so many Windows viruses - this is the main point that he missed in the Vnunet.com article: Virus writers want to have the maximum effect, therefore they choose a popular platform. Linux is becoming more popular; therefore it will become more of a target for virus writers.

Mr. Skoll overreacts to the Vnunet article, but some of his claims are correct, in particular his analysis of why Linux viruses are (currently) unlikely. Also, he has a lot to learn about viruses - he should have rejected all of the virus entries to his challenge, even if they *had* tricked him, because they are not viruses - they do not replicate. If I was to take up the challenge, my approach would be to *burn down the city* - Mr. Skoll is obviously highly suspicious of anything he receives, so I would instead target open source developers that he already trusts, and might be receiving patches by email from them. Of course, it would be necessary to infect the patch before it was signed, by tricking the developer. There would be substantial collateral damage - every other user of the same software would also get infected when they installed the patches, and I would be thrown in jail for the damage caused, and rightly so. Given the small prize,

$2000 Canadian, and that claiming the prize would be an admission of guilt, only the truly insane or stupid would do this for the prize.

That is Mr. Skoll's second challenge, unfortunately, he does not offer a prize for the first challenge: "If you have the courage and decency to do so, release products which block executable e-mail attachments". There would be a long queue claiming the prize if he did - most anti-virus gateway and content security products can do this (please contact us if you want to buy one). Many anti-virus companies specifically advise blocking executables and double-extensions (the Sophos SafeHex guidelines are one example), and wise organisations, such as AVIEN members and the Hong Kong Government are showing the success of that policy.

I like Linux; it has many advantages, but total immunity to viruses is not one of them.

"Exclusion of Cyber Risks" - Insurers Opt-Out

Karen Cheung
karen@.yuikee.com.hk

Our insurance company recently sent us a letter informing us that "“Terrorism and Cyber Risk” would be excluded from our policy starting from 1st January, 2002.' In short, they are excluding damage from acts of terrorism or any kind of loss of data or software from the risks they are willing to cover. I guess all or most of you have received similar letters by now. Indeed, the unexpected 911 incident has changed the world and have hardened the insurance and reinsurance market immensely, so it is everyone’s problem now. Why, precisely, violent, terrorist acts have made the potential risk from loss or damage of data or software unacceptable is unclear. However, let’s look into the impact of “Cyber Risk Exclusion” Clauses: Information security management does recognize alternative methods for handling risk, including avoiding, reducing, accepting and transferring. Transferring risk essentially means insurance: if an incident occurs, someone else pays, and the organization is protected. Exclusion of "Cyber Risks" by insurance companies implies that organizations will have to manage those risks by other means: avoiding, reducing or accepting. If you do not want to accept the higher risk, you will need to review your policies and be better protected. Probably, put more controls in place to compensate. In case you would like to do a risk assessment to your data protection mechanisms, talk to our consultants.

Email Anti-Virus for Linux

Lois So
lois@.yuikee.com.hk

The popularity of Linux continues to rise and Yui Kee is seeing more interest in Anti-Virus products for Linux. Email anti-virus scanning on Linux is becoming particularly popular.

The release of Sophos MailMonitor for SMTP is therefore very welcome. MailMonitor detects, reports and disinfects viruses in email sent via an SMTP (Simple Mail Transfer Protocol) server on Linux/Intel. Infected attachments are either quarantined or automatically disinfected before delivery to the recipient. Comprehensive messaging allows MailMonitor to notify administrators, senders and recipients of any viruses found. MailMonitor for SMTP on Unix

can find viruses in attachments compressed with ZIP and other popular compression utilities.

Yui Kee Computing Ltd can provide 30-days trial Evaluation CD to interested parties. To request this trial or for more information on the YK service please contact our Customer Services department at:

Tel: 2870 8553
Fax: 2873 6164
Email: offer@yuikee.com.hk

Microsoft's New Direction?

It is difficult to write responsibly about security without sounding like a Microsoft-hater. The fact is that most of the world's computers run Microsoft products, so any serious vulnerability will affect a lot of people. And there are lots of serious vulnerabilities. Even organisations that keep their critical systems and data on minis or mainframes have users or customers with Windows, so they must consider the risks when the systems interact.

The good news is that Microsoft is taking security seriously - Bill Gates sent round a memo in January emphasising that security is the new priority: "when we face a choice between adding features and resolving security issues, we need to choose security." This is the approach that is needed - complexity is the enemy of good security, and no one can deny that Microsoft products are rich in complex features.

The bad news is that even with total commitment within Microsoft, it will take a long time for the benefits to emerge - the existing vulnerabilities (known and unknown) will be with us until everyone changes to use the new, safe software. Also, this may be mere lip service, designed to combat recent bad publicity. Certainly, Steve Ballmer (Microsoft's CEO) is not showing a new commitment to security, he is still repeating the "all software contains vulnerabilities" spin. This is true, but some software contains more vulnerabilities than other software. Also, Scot Culp (manager of Microsoft's security response centre) is showing a remarkably selective memory in the face of the UPnP exploit for Windows XP, saying, "This is the first network-based, remote compromise that I'm aware of for Windows desktop systems." Perhaps Back Orifice, the Internet Explorer cross-frame scripting vulnerabilities and numerous other examples do not count. We will have to wait to see if Bill's memo is a real change of direction, or just hot air.

So, assuming that Microsoft is committed to doing the right thing on security, what do we need for end users? Perhaps it is a new definition of "User Friendly". When I invite a friend to my home, I do not expect him or her to bring a load of stuff and install a cat flap, "because I might need it one day". I would expect a friend to mention if I had left a window open, and to be honest if they have an accident in my home. So the default install should be minimal functionality - no installing a web server with the OS, macro capability should be optional in word processors and spreadsheets and so on. There should be warnings about unsafe configurations, and when fixes are needed, the users informed consent for the automatic fix will be sought. This will make computers more difficult to use, but a lot easier to use well.

Protecting Your Home Computer

Robert Sim
CyberGuard
robertsim@cyberguard.com

The basic problem for home or end user is lack of understanding and ignorance of the dangers of the Internet. The Internet at the moment is like Wild West, full of dangers and pit holes. Home users are using their computers for investing, banking, shopping and communicating with friends through e-mail or chat programs. We may not consider our communications as top

secret but intruder may read your email and use your computer to attack other systems. They may examine your personal data stored in your system like credit card information, bank's password and account information and other personal information.

Intruders do not care about the identity of the users. They want to control your computer so that they can launch attacks against other more important computer systems like government or financial systems. By taking control of your computer allow them to hide their true identity and location. Once your computer is connected to the Internet to play games or to send email to friends, you are the target.

Intruders can control your computer and monitor every action on the computer. They can see what you see on the monitor screen, what is your bank account name and the password. They can switch on your microphone and web cam without you knowing it and they can see and hear what is happening in front of your computer. (Don't have your web cam facing your bed.)

Control your system is as easy as "ABC", intruders are always discovering new vulnerabilities to exploit in computer software. Some software applications have default settings that allow others to access your computer unless you change the setting to be more secured. Examples chat programs that allow outsiders to execute commands on your system or web browsers that allow someone to put harmful programs on your system that run when you click it.

How do you protect yourself and minimizes the risk of an attack: -

- Use anti-virus software and keep it updated - many people do not regularly update the virus definitions.
- Use a personal firewall for your system.
- Email attachments are dangerous; you need to think where it comes from before opening. Even best friend can sent you dangerous attachments unintentionally.
- Don't run unknown programs from unknown origin.
- Install the vendors' security patches for all your software applications (IE) and operating system.
- Disconnect or turn off your computer (some computer can be turn on from the net) from the network.
- When it is possible turn off scripting features in email program
- When it is possible turn off Java, JavaScript and ActiveX.
- Backup your data regularly.
- Make a boot disk in case your computer is damaged or compromised.

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/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE