Yui Kee Computing Ltd.

Newsletter

March 2002

Contents

Editors Notes

First, an apology: last month I sent the email to you before I attached the newsletter, sorry for the extra email.

Secondly, we are asking all recipients to re-subscribe, and provide us with some feedback, please fill in the Subscription Renewal form at the end of this newsletter and return it to us.

Allan Dyer

Stop Press: WildList on Hold

The WildList is a co-operative listing of viruses that are actually causing problems on real users' computers (as opposed to just residing in collections). Joe Wells started the list in the early 1990's and detecting all the viruses listed on the current WildList has become an important criteria in anti-virus reviews, including those by ICSA, Secure Computing and Virus Bulletin. The strength of the WildList has been its' independence from corporate agendas, due to its' voluntary nature, and, of course, the integrity of the primary researchers behind it.

Unfortunately, the voluntary nature is now proving to be its' weakness. In a message to the anti-virus community, reported by the Register, Shane Coursen, the Chief Executive of the WildList Organisation said that the March 2002 list would be the last until further notice, and that he is now seeking a position as a full-time anti-virus researcher (see http://www.theregister.co.uk/content/56/24587.html). The care taken to ensure that the list is accurate, and does not include fake reports from virus writers, or non-viruses is a lot of work.

The WildList has been criticised by some anti-virus researchers for not being comprehensive, but a better methodology for measuring the virus problem has yet to be proposed. It is hoped that this will prove to be a temporary pause, and the WildList will re-emerge with a stronger support model that maintains its' independence.

Incident Update

W32/FBound.C@MM started spreading on 14th March 2002, and, according to MessageLabs' statistics, it affected Hong Kong the most. It is a simple mass-mailer, but it does have one interesting feature. In most circumstances, the Subject of the email it sends is "Important", however, if the recipient's domain name ends in ".jp" it uses one of 17 Japanese Subject lines. Initially, many different names were used for this virus, see the article on naming difficulties below.

A second mass-mailer hit on 22nd March 2002, W32/MyLife.B-MM arrives with the Subject "bill caricature" and has not yet been reported in Hong Kong. It tries to convince the user that it is not a virus by including the text, "No viruse found" in the email message. The spelling mistake should make users more suspicious, but it is useful to remember that any part of an email message might not be true.

Email Encryption and Signing: False Sense of Security

Recently, I received information on an email gateway designed for "security" that had features I immediately thought were stupid. I will not name the product, I did not test it, and the same comments would apply to any product with the same features.

Automatic Digital Signing of Outgoing emails: The gateway will digitally sign outgoing emails that match a rule set by the administrator. The attraction is that it could allow a company to start using digital signatures when the responsible staff (e.g., the computer-illiterate CEO) does not understand the technology. The flaw is that, as an SMTP gateway, the product depends on the SMTP headers to determine the identity of the sender - there is no authentication. Thus, every email matching the administrator's rules is a legal document signed by the company. So, a rogue employee could commit the company to a disadvantageous contract - a cleaner could forge an email from the CEO. Alternatively, a new, mass-mailer virus could enter the company and send itself (from the CEO) to the company's business partners. Apart from being embarrassing, a business partner who was damaged by the virus could use it as legal proof of the source, and claim damages.

Automatic Self-decrypting messages: The administrator defines passwords for recipients, and email to them is automatically encrypted by the gateway. Recipients decrypt the messages by double-clicking the attachment and entering the password. The attachments must be executables, so this goes against anti-virus Safe Hex guidelines. The administrator has the burden of managing passwords for many recipients; recipients are probably receiving messages from several sources, and therefore have to remember multiple passwords.

Scanning encrypted messages: The product will use third-party anti-virus products to scan the encrypted messages. So, the messages are decrypted at the gateway. Breaking into the gateway gives the attacker access to all the encrypted communications of the company.

Overall, the product tries to bring security buzzwords to SMTP email without changing the user's behaviour, but fails to address the problems that make this difficult. If you want digitally-signed messages that really authenticate the sender, then the sender must have control over their private key and the signing process, and understand what this means. If you want secure, encrypted messages to many parties, PKI is the simplest. If you want end-to-end confidentiality, you cannot block viruses at the gateway. Shortcuts might be attractive, but they will not provide real security.

Yui Kee at HKIIE

Chris Lee explaining new trends in malware at HKIIE

Yui Kee participated in the Hong Kong Information Infrastructure Exhibition on 7th-10th March. Apart from a booth, our Chris Lee spoke at two of the on-site forums and Johnny Cheng and Chris Lee hosted sessions at the SME IT Clinic.

The Yui Kee Booth, in partnership with HP

Difficulties in Naming Viruses

A search of Anti-Virus websites on the 14th and 15th March showed alerts about a confusing number of virus names, but, it became clear, the alerts were about a single virus. Differences in naming are common, and users frequently ask for unified naming. On the whole, anti-virus researchers agree that unified naming would be good, but, so far, it has proved impossible. Let us take W32/FBound as an example, and examine the reasons for the differences.

On the right is a listing of the names and the companies' sites they were taken from. The names in brackets are listed on the sites as aliases. The companies are in no particular order. So, it appears that the author included his (or her) suggested name in the virus itself, Symantec, at different times, called it by three different names, Trend Micro by another three, and so on.

Before examining the list in detail, it is worth looking at the naming standard defined by the Computer Anti-Virus

Author	JAPANIZE
Symantec	W32.FBound.gen@mm W32.Impo.gen@mm W32.Dotjaypee@mm *(W32.Impo.gen@mm, W32.Dotjaypee@mm, Win32/Japanize.Worm, I-Worm.Zircon.B, Win32.Fbound.C, W32/Fbound.c@MM, W32/FBound-C)*
Trend	WORM_FBOUND.B JAPANIZE.A FIDAO.A *(FIDAO, W32/Fbound.b@MM, Win32/Japanize.Worm, I-Worm.Zircon.B,)*
Kaspersky	I-Worm.Zircon.c
MessageLabs	W32/Fbound.C-mm W32/Impat.A-mm
McAfee	W32/Fbound.c@MM *(I-Worm.Zircon.c, W32.Dotjaypee@mm, W32.Impo@mm, W32/FBound-C, W32/FBound.C@mm, Win32.Fbound.C, WORM_FBOUND.B, WORM_JAPANIZE.A)*
CA	Win32.Fbound.C *(Worm_Fbound.B , W32/Fbound.c@MM, W32.Impo.Gen@mm, I-Worm.Zircon.C)*
Norman	W32/FBound.C
Sophos	W32/FBound-C *(W32/Impatt-a, WORM_JAPANIZE.A, W32/Impat, W32/DotJayPee@mm, Worm_FBound.B, F/Bound.C, I_Worm.Zircon, FBound.C, W32/Fbound.C@mm, Fidao, W32.Impo.gen@mm, Impo)*
F-Secure	Fbound.C *(W32/Impat.A-mm, I-Worm.Zircon)*

Research Organisation. They recommend:

- No personal or company names
- No rude or obscene words
- Do not follow the author's suggestion
- Use the form *Platform/Family.Size.Variant@Suffix*

The parts of the name are:

Platform: The environment or platform that the virus requires, such as W32 for 32-bit Windows (i.e., Windows 95, 98, NT, 2000 etc.) or VBS for Visual Basic Script.

Family: A name for the family of related viruses. It must not clash with the name of any existing, unrelated virus. Normally, the first researcher to identify the family names it.

Size: For binary file viruses, the size, in bytes of the virus code.

Variant: A letter or letters assigned sequentially as variants are identified. So, the first variant is .A, the second .B, the twenty-seventh .AA and so on.

Suffix: If a virus emails itself to addresses individually, the suffix m for "mailer" is used, if it emails itself to many addresses (for example, the whole address book), the suffix mm for "mass mailer" is used.

So, this defines the structure of the name, and most companies follow this (with minor variations in punctuation, like "." instead of "/"). Trend Micro is a notable exception; first, they use different abbreviations for the platform (e.g., PE for Portable Executable instead of W32), second, instead of the platform they might use the type of malware: TROJAN or WORM. Understanding the company's naming conventions, we can realise that WORM_FBOUND.C and W32/Fbound.C both refer to the third variant in the Fbound family.

What happened with FBound? At the beginning of March, two viruses were discovered and Trend Micro initially called then FIDAO.A and JAPANIZE.A. Other companies realised that they were variants in the same family, and called them Fbound.A and B. Trend changed their naming to follow the consensus.

On 14th March, a minor variant of FBound, very similar to FBound.B, started spreading rapidly. I cannot be certain who saw it first; certainly the first alert I saw was from Trend Micro, calling it WORM_FBOUND.B. Network Associates soon warned about W32/Fbound.c@MM, and MessageLabs about W32/Impat.A-mm. Symantec warned about W32.Dotjaypee@mm. So, initially MessageLabs and Symantec thought they had isolated a new family, and Trend Micro considered the virus to be the same as one they already identified. After further investigation, the relationships became clearer, however, Symantec was already using the name Impo for this family, and Kaspersky uses Zircon. Then, it was realised that Impo has rude connotations in Japanese, as an abbreviation for Impotent, so Symantec changed their name again to FBound.

A further complication is the use of generic identification. Symantec actually reports W32.FBound.gen@mm, the gen stands for "generic", and it will give the same name for the A, B and C variants. Generic detection is good - designing a product so that it can detect variants of known viruses makes sense. Researchers disagree on whether generic identification is good - once the virus has been detected, is it necessary to test further until the exact variant has been identified, or is it OK to report "Family.gen"? I will not cover the full arguments on both sides here. The result in this case is that Symantec's use of generic detection and reporting of aliases used by other companies makes it appear that Trend Micro used three different names for one virus: FIDAO, JAPANIZE and FBOUND. In reality, they used different names for two variants, and later standardised them.

Who is right? Well, today almost all companies agree that Fbound.C was the virus that spread rapidly on 14th March 2002, just Kaspersky prefers the family name Zircon. Most of the confusion happened in the first day and at that point the important task was to get the thing detected. Anti-virus products have to give *some* name when the virus is found, it would make no sense to wait four days, until the naming was sorted out, before releasing the updates! Some things could have been done better: Trend Micro should have known not to use the author's suggestion. In this case, the problem originated at the beginning of March, when companies started using Fbound, Impo and Zircon as names for uncommon viruses, but it only became an issue when the fast-spreading third variant appeared, there are probably many other cases where there are unrecognised differences in naming.

I hope this illustrates that the anti-virus companies are not making the names different to be difficult, there are real constraints that cause the complexity and confusion. There are disagreements about the naming of species in biology, but there the issues can be worked out over months or years.

Finally, this is just one recent example and specific details, such as which company sent the first warning, or did not immediately recognise the relationship between variants are not general indicators of that company's performance on other occasions.

Club eBiz Conference

Our Chief Consultant, Allan Dyer, spoke on "Malicious Code and Mobile Devices" at the Club eBiz Wireless Security Conference on 20th March. Viruses and Worms are currently the commonest type of security incident for desktop computers, but they have yet to make an impact on mobile devices, Mr. Dyer discussed how and when this will change.

Professor Doug Vogel (left) presents a souvenir to Mr. Allan Dver

Also speaking the same evening was Dr. Joseph Williams, Chief Architect of Sun Microsystems - he gave an overview of wireless security, and then concentrated on the vulnerabilities of IEEE 802.11 networks, "wireless Ethernet", including War Driving and WEP shortcomings.

An interested audience

Club eBiz (http://www.club-ebiz.com/) is an initiative from the Department of Information Systems at City University to bring together business professionals and executives who share similar interests in electronic business. The presentation slides are available on request.

Networking and discussion after the speeches

SSH - Securing Connections

Last month, F-Secure SSH was our top-grossing product, so we take a look at the reasons for the success of this quiet-but-effective utility. SSH is a published protocol for secure remote login and other secure network services over an insecure network. It is widely used and recommended, for example, in RFC2010, Operational Criteria for Root Name Servers, it is recommended for remote login to root name servers. An increasing number of network devices are shipping with SSH, such as Cisco Routers and Nokia Security Appliances.

In it's simplest use, SSH is a "drop-in" replacement for insecure protocols including telnet, rlogin, rsh and rcp. That is pretty useful for the hard-working Unix administrator who wants protection without inconvenience, but F-Secure SSH also provides tunnelling (X11 connections are provided by default), servers for all major Unix platforms (including Linux) and Windows 2000/NT4, and clients for those plus Windows 95/98/Me and MacOS. F-Secure SSH provides a secure variant of FTP for file transfer; called SFTP, this can be used through a standard GUI. A choice of algorithms is provided, including Triple-DES, DSA, RSA, IDEA, Blowfish, AES and others, so conformance with existing security policies is easy. F-Secure SSH also supports public key infrastructure, and smartcards.

Although the obvious applications for F-Secure SSH are remote systems administration, web-site update and maintenance, it is very flexible. It may be used in some circumstances instead of a full IPSec VPN: any simple TCP-based protocol can be tunnelled over it, and, as it is application layer, it does not require special configuration for NAT, unlike transport layer-based IPSec.

An example of this is secure, remote email pick-up. POP and SMTP are insecure protocols, and we accept that external email is vulnerable. However, our internal email may be more sensitive, and the password that users use to access their mailbox is probably the same as they use to login to the network. How do you provide your home / mobile workers with the ability to pick up their email without exposing company internal email and, more importantly, their password on the internet? One method would be a host-to-gateway IPSec VPN for each home / mobile worker. Simpler and cheaper is F-Secure SSH - the client would be configured to tunnel POP and SMTP to an SSH server inside the company (either on the mail server, or as convenient). The user can be provided with an icon that starts F-Secure SSH, establishes the connections and then starts their favourite email client configured to use the tunnels.

F-Secure SSH contains components certified by NIST (National Institute of Standards and Technology) to FIPS 140-1. SC Magazine gave F-Secure SSH Client and Server five stars as an overall rating in its January 2002 review. The review praises the ease-of-installation with no noticeable overheads and the secure tunnelling of F-Secure SSH therefore giving peace of mind to any e-business company relying on its web sites. For more information, please contact our Sales Dept at Tel. 25550209, Fax. 28736164 or E-mail: info@yuikee.com.hk

Special Offer: Stop Viruses at the Gateway

Do you want to save more than **HK$10, 000**?

Yui Kee Computing Ltd is honoured to offer a bundle program of HP server and email security products: either Sophos MailMonitor (Anti-Virus) or e-Safe Gateway (content security). Installation, Configuration and Operating System are included. Your total saving may be over HK$10,000.00.

For more information, please contact our Sales Dept at Tel. 25550209, Fax. 28736164 or E-mail: info@yuikee.com.hk

Includes:

ONE YEAR software update & upgrade

ONE YEAR Office Hours Technical Support

ONE YEAR Virus News

Training, Installation & Configuration

Valid until 7th April 2002

Bundle	SMTP Anti-Virus Gateway	Original Price	Now
A	HP server tc2100 PIII-1.13 (128MB)/Sophos MailMonitor for 50-users/Red Hat Linux 7.2	HK$ 22888.00	**HK$ 18237.00**
B	HP server tc2100 PIII-1.1 (128MB)/Sophos MailMonitor for 100-users/ Red Hat Linux 7.2	HK$ 28728.00	**HK$ 22909.00**
C	HP server tc2100 PIII-1.26 (128MB) /Sophos MailMonitor for 200-user/ Red Hat Linux 7.2	HK$ 39528.00	**HK$ 31637.00**
Bundle	**Internet Content Gateway**	**Original Price**	**Now**
D	HP server tc2100 PIII-1.13 (256MB) / and eSafe Gateway for 50-users/OEM Win 2k server + 5 cal	HK$ 42093.00	**HK$ 35518.00**
E	HP server tc2100 PIII-1.26 (256MB) / eSafe Gateway for 100-user/ OEM Win 2k server + 5 cal	HK$ 51893.00	**HK$ 43914.00**
F	HP server tc2100 PIII-1.26 (256MB) / eSafe Gateway for 200-user/ OEM Win 2k server + 5 cal	HK$ 68741.00	**HK$ 58234.80**

Description
HP Server tc2100 PIII-1.13 (128MB) SCSI Mod 18 includes one PIII-1.13GHz CPU, NIC, single channel SCSI controller, CD-ROM, floppy, 18.2GB HOD, tc2100 startup CD
HP Server tc2100 PIII-1.13 (256MB) SCSI Mod 18 includes one PIII-1.13GHz CPU, NIC, single channel SCSI controller, CD-ROM, floppy, 18.2GB HOD, tc2100 startup CD
HP Server tc2100 PIII-1.26 (128MB) SCSI Mod 18 includes one PIII-1.26GHz processor, SDRAM, 18 GB SCSI HOD, NIC, single channel SCSI controller, CD-ROM, floppy, installation CD
HP Server tc2100 PIII-1.26 (256MB) SCSI Mod 18 includes one PIII-1.26GHz processor, 18 GB SCSI HOD, NIC, single channel SCSI controller, CD-ROM, floppy, installation CD

Product News: eSafe Appliance

Staying ahead of Internet malware

You've taken a multilayer approach to security and you've got antivirus gateway software. You use the latest virus signature updates. You spend considerable time to patch your operational system regularly. If you presume that all this qualifies for a reasonable protection against content security threats, you may be wrong.

The reactive approach: just waiting for new virus updates and security patches to come up is not enough to counter the rising tide of malicious mobile code. What you need is a solution that keeps your Internet traffic protected even during a several-hour window until the next patch comes up. Aladdin's eSafe Appliance can do just that to insure clean information flow in your organization.

Introducing eSafe Appliance

Aladdin offers industry's first OPSEC compliant Content Security appliance designed to defend your organization against fast-spreading Internet threats. Under the hood, you will find top-performance hardware, hardened OS and award-winning eSafe technology. All its components are fully integrated and optimised to eliminate viruses, worms and trojans. Installable in less than 15 minutes and manageable via user-friendly GUI, eSafe Appliance protects straight out of box, thanks to smart initial settings. What make it cost effective are everything-included approach, self-update capability, secure remote management and performance-oriented architecture.

Proactive Content Security software and hardened Operational System combined in eSafe Appliance are capable of recognizing and countering many classes of unknown threats. It is backed by sophisticated auto-update mechanism designed to keep the stress out of the IT staff.

The challenge

Many companies are using multipurpose server platforms with anti-virus and content security software. The integration and support of software, hardware and OS coming from different vendors is always time and resources consuming operation. Moreover, with a general purpose operational system it is necessary to make frequent checks for bug patches and other security holes. Installation of patches and hot fixes to deal with the vulnerability to hacker attacks as well as hardware maintenance and upgrades are not coming cheap either.

It's always matter how up to date your anti-virus software is. However, the signature updates alone do not allow you to stay ahead of the new threats. There always is a several-hour gap between the detection of new malware and the release of a signature. A solution that gives that extra cover to your Internet traffic during the exposure period can be literally a lifesaver.

Nowadays, IT managers have to fight for every penny for a security budget and the MIS personal is shrinking. Therefore one have to make sure that the initial investment in the security solution does no become a money pit. What makes it for a cost effective solution is a device that is easy to install, remotely manageable, self-updating and that can easily compliment the existing security infrastructure such as firewall, anti-virus and content security tools.

The solution

The eSafe appliance is a fully integrated hardware product that ships complete with 24x22x5.5 cm hardware box, cables, Quick Start Guides, Administration Manual and a CD with eConsole management software and additional documentation in electronic form. One can have it up and running in less than 15 minutes. All it takes is to get the Appliance out of box, plug it to the power grid, to the network and connect to the eSafe Manager Web administration interface via the default IP address. The instant that the box has been configured with the proper IP, it becomes fully functional. All further configuration is performed centrally via eConsole management software that immediately discovers the newly installed eSafe Appliance.

eSafe Appliance can be configured either in CVP mode for joint work with Check Point Firewall-1 or as a standalone SMTP gateway.

Many organizations leverage existing Firewall-1 software or brand new firewall appliances for proactive content security with eSafe Appliance working as CVP scanner. All it takes is to make a few software definitions according to detailed, easy to follow procedures from the eSafe manual. The eSafe Appliance in CVP mode of operation provides with a full protection against threats coming from Internet via popular HTTP, FTP and SMTP protocols.

eSafe Appliance with eSafe Mail SMTP license is a completely standalone solution and works transparently with any firewall, mail-relay or SMTP mail server. For a seamless integration with your MTA of choice, sitting in DMZ or for that internal mail server taking a heat from the Internet all you have to adjust is a few configuration parameters. Again it is done via the intuitive GUI.

With eSafe Appliance, the network's anti-virus protection and content security needs are served without any unexpected maintenance. The eSafe Appliance is a cute little box. It just sits where you plug it in and does its job without a problem. Service providers love the fact, that it can be managed remotely via secured interface, while the end user gets all the security information and statistics on the desktop via eConsole.

The Proactive Security capability of eSafe Appliance is baked by built-in automatic update mechanism that keeps its system software, content security engine and virus definitions up to date. Now, that the routine maintenance tasks and hardware integration headaches are gone, your MIS and Service Provider's staff can focus on other things.

Under the Hood

The eSafe Appliance is an embedded system sporting a 700 MHz CPU, 256 MB RAM, 10 GB internal storage and 10/100 Mbps network interface. It features a hardened Linux operational system that is governed by eSafe Manager administration tool. The eSafe Manager is a Web GUI that is secured via SSL. The centrepiece of the Appliance is award-winning eSafe content security technology. This technology goes far beyond just an anti-virus an order to protect the users against viruses, trojans, worms and other content security threats. All the configuration, monitoring and statistics gathering concerning the state of content security policy are centrally managed via eConsole. This user-friendly yet sophisticated GUI is capable of running on a Windows workstation. The eSafe Appliance comes preinstalled and preconfigured, together with 30-days evaluation license.

The eSafe Appliance is a server dedicated to a single function, therefore it offers unprecedented level of timesavings and reliability. That makes for a cost effective solution for enterprise protection against viruses and malicious mobile code. eSafe Appliance is a Proactive Content Security solution. It compliments and integrates with many elements of existing security infrastructure. For more information, please contact our Sales Dept at Tel. 25550209, Fax. 28736164 or E-mail: info@yuikee.com.hk

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/

Subscription Renewal

If you do not send this back by 20th April, 2002, you might not receive the next issue.

Please fill in this survey and click on the Submit button to send the data via our website, or fax back to: +852 28736164 as soon as possible.

A. Your email address (as used for subscription):

B. Have you found this newsletter useful to you in the following area?

(1 = not useful; 5 = very useful)

i. Providing products and services update in the Anti-virus and Information Security area?

1 ○ 2 ○ 3 ○ 4 ○ 5 ○

ii. Providing advice on good practices and warning of bad practices in the area.

1 ○ 2 ○ 3 ○ 4 ○ 5 ○

iii. Providing latest news and information that concerns Anti-Virus and Information Security users and about Yui Kee Computing Ltd's offers and activities.

1 ○ 2 ○ 3 ○ 4 ○ 5 ○

iv. Providing communication channel between us.

1 ○ 2 ○ 3 ○ 4 ○ 5 ○

C. In order to continue getting increased benefit from the content:

We are considering launching a Chinese version of this Newsletter, and options for charging subscribers:

i. Do you read Chinese? Yes ○ No ○

ii. Would you pay HK$180 for 12 issues of the English edition? Yes ○ No ○

iii. Would you pay HK$180 for 12 issues of the Chinese edition? Yes ○ No ○

iv. If not, please suggest an acceptable amount here: HK$

v. Would you like to receive one free issue of the Chinese version? Yes ○ No ○

D. Topics

Please suggest topics that would be useful to you, we'll do our best on researching and inviting suitable writers.

E. Other Comments

Please make any other suggestions to improve this newsletter:

Reset

Submit


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