Yui Kee Computing Ltd.

Newsletter

February 2001

Contents

The Return of Melissa and Navidad

22 January 2001, Hong Kong: Yui Kee warns that two old viruses, Melissa and Navidad, are now spreading again as new variants around the world and in Hong Kong. Users practicing "Safe Hex" will not be at risk.

Several anti-virus developers and security companies have issued

warnings about the new Melissa variant. Variously called W2001MAC/Melissa.W-mm, Melissa-X, W97M_ASSILEM.B, Melissa.W, it is in a document saved using Microsoft Word 2001 for Macintosh.

This is problematic, as some anti-virus programs are still unable to handle this new file format but the virus is fully functional under both Macintosh and Windows versions of Microsoft Office.

Opinion on the threat represented by Melissa.W varies:

Trend Micro has reported, "Reports of infection have come from Europe, North America, and South Africa. We've assigned the virus a 'low risk' ranking as the virus has not had a significant impact or spread very far at this point." See: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=W97M_ASSILEM.B

TrueSecure has assigned a Medium risk, saying, "We currently recommend aggressive efforts to make sure your site is not affected by this virus including, potentially, shutting down your Internet email gateway." See: http://www.trusecure.com/html/tspub/hypeorhot/alerts/w2001mac.shtml

"This is a wake-up call for anyone who thinks viruses happen to other people," said Graham Cluley, senior technology consultant at Sophos Anti-Virus . "Everyone should be employing safe computing practices. My message is simple - stop opening unsolicited attachments; start treating your computer with the respect it deserves." Sophos has already released an update for the virus. See: http://www.sophos.com/virusinfo/articles/melissax.html

F-Secure warned: "Melissa.W has been spreading for two days now and is getting very widespread. This is serious as many av programs can't handle its file format." See: http://www.f-secure.com/v-descs/melissaw.shtml

Yui Kee has received no reports of Melissa.W in Hong Kong. Allan Dyer, Chief Consultant at Yui Kee, said, "We cannot predict at this stage whether this will become prevalent in Hong Kong." However, W32/Navidad-B has been confirmed in Hong Kong.

W32/Navidad-B also travels as an email attachment, but as an executable file rather than a document. When it has infected a victim's computer, it will search the users' Inbox and reply to messages that have one attachment. The subject and the body of the reply will be the same as the original message, but the attachment will be a copy of the virus. "This is particularly well suited to spreading at Chinese New Year, we have seen people sending out their new year greetings to a large group of friends with an animation attached, Navidad will react to these messages by replying to all the recipients, with itself attached.

The recipients can easily mistake this for another fun greeting." said Allan Dyer, "We have already seen two infected individuals who sent out the virus to a total of ninety-six contacts. This clearly shows the potential for epidemic spread, and the importance of Safe Hex. I do not want to sound like a grinch, but are your greetings any less heart-felt if you do not send that attachment?"

Further information on W32/Navidad-B is at:
http://www.sophos.com/virusinfo/analyses/w32navidadb.html
http://service1.symantec.com/sarc/sarc.nsf/html/W32.Navidad.html
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_NAVIDAD.E
http://www.f-secure.com/v-descs/navidad.shtml

Guidelines for Safe Hex are at:

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

Which Solution?

In this issue we introduce two products that both have the capability of scanning Internet email for viruses, but they are very different solutions. Why are we carrying both, and which should you choose?

In security, one size does not fit all. Each organisation has its' own concerns and requirements. Our consultants will discuss your situation and help you to choose the best solution for your concerns, requirements and budget.

MessageLabs is a Managed Service Provider, they take away the concerns about malicious code in Internet email by scanning your email at their Virus Control Centre at data centres on the Internet. You (or your ISP) just redirect your incoming and outgoing email via the Virus Control Centre and MessageLabs does the rest. They use three industry-leading anti-virus scanners updated every 10 minutes, and their own heuristic scanner, called Skeptic™. Easily-accessible statistical reports are provided, so you can see how much work they are saving you. MessageLabs service is ideal for organisations that want to outsource the hassle of email virus protection.

eSafe Gateway is best described as Content Security – it does a lot more than anti-virus in email. It inspects email (SMTP) web (HTTP) and FTP traffic in various ways. It stops malware: viruses, Trojans, increases productivity by blocking access to objectionable or unproductive sites and greatly reduces spam by anti-spoofing verification, blacklists and other methods. It has a host of useful features, such as adding standard company disclaimers to outgoing email. ESafe Gateway is ideal for organisations that want to take control of their Internet content.

Valentines' Day Massacre

Not long after Chinese New Year we have St Valentines' Day when people may also send each other greetings. A recent survey by IDC/MessageLabs indicated that more than a third (37%) of business email users across the UK would still open a message saying I LOVE YOU, if it arrives on 14 February. Therefore, there is a renewed change of spread for VBS/LoveLetter. More details at:
http://www.messagelabs.com/viewNewsPR.asp?id=61&cmd=PR

Email Tracking

Content Security Resource Center (CSRT) Alert (see: http://www.ealaddin.com/home/alert.asp)

A JavaScript security flaw exists in several email client programs. The exploit makes it possible to track down forwarded email without the forwarding senders' awareness. An attacker could create an email containing an embedded script, the email could be sent to victims, if the victim will forward the email, a copy of the forwarded email text will be sent back to the attacker, without the victims' knowledge.

This security hole exists in HTML\Java enabled email readers. That makes most Outlook\Outlook Express and Netscape Communicator users vulnerable.

The exploit has been known since 1998 but only now created a media concern.

You can read about it here:
http://www.wired.com/news/business/0,1367,41639,00.html

eSafe Gateway and Mail provide a solution to this exploit. eSafe Gateway 3 and eSafe Mail clients are advised to block the string "document.body.innerText" in scripts within HTML email.

Here are the instructions:

1. Open eConsole

2. In Rules=>SMTP=>Incoming=>Scan - make sure the "Scan body for HTML vandals..." check-box is checked.

3. In Content Filters=>HTML=>SmartScript Filters=>JavaScript - make sure either the "Strip w/forbidden functions" check-box is checked.

4. Add the function document.body.innerText

5. Repeat for the other script types.

Introducing Aladdin's eSafe Gateway

Yui Kee will distribute Aladdin's eSafe Internet Content Security Solutions in Hong Kong, see: http://www.ealaddin.com/news/2001/esafe/yuikee.asp for full details. eSafe Gateway sets the standard for content security, protecting networks from vandals, viruses, inappropriate content, and data exposure. Built in a scalable, high-availability architecture to provide superior load-balancing. eSafe Gateway can be configured to operate in any network with or without a firewall.

Gateway vandal protection inspects all traffic passing through FTP, HTTP, and SMTP in real time. eSafe Gateway finds and cleans Java, ActiveX, and script vandals. Gateway virus protection by a full 32-bit, ICSA and Checkmark certified anti-virus engine. It removes viruses from files and emails, attachments, Microsoft Office documents, all MIME types, and all compressed file formats.

Scalable, load-sharing architecture allows you to add more Content Inspector machines according to network needs.

Spam is reduced to a minimum using anti-spoofing verification, an updateable blacklist of spammers, and rule-based keyword filtering.

Block access to objectionable and unproductive sites using advanced technology that analyzes sites' content with more than 40 categories and one million URLs. Please contact us for pricing information and more details.

Introducing MessageLabs and its 100% Record

MessageLabs is a Managed Service Provider (MSP) specialising in Internet-level email content filtering and has the unique claim to having stopped every email virus since its service started in 1999. While the world watched helplessly last year as the I LOVE YOU (VBS/LoveLetter) virus caused damage estimated at US$7 billion (according to some sources), MessageLabs was the first company to identify and intercept the "Love Bug". Not a single one of its customers was affected.

Its SkyScan AV is the world's first Internet-resident antivirus service and the only virus protection solution that does not rely on knowing virus signatures in advance. SkyScan AV comprises three layers of scanning software from leading anti-virus vendors and a proprietary fourth layer called Skeptic. Skeptic is a unique, patented and revolutionary malicious code scanner combining artificial intelligence and a heuristics to sniff-out and stop anything suspicious.

MessageLabs' technology is continually updated with emails scanned in real-time so there is no impact on delivery times. Users simply sign up for the service so that all their email traffic is directed through the company's Control Towers strategically placed at major Internet exchange points.

Currently, MessageLabs scans email for more than 300,000 users worldwide, and major customers include Air Products, Fujitsu, The Bank Of England and Vodaphone. Yui Kee Computing has already started selling the SkyScan AV service prior to MessageLabs' official launch in Hong Kong, planned for March. Please contact us for pricing information and more details.

Authentication Pitfalls

By Allan Dyer (based on an article for the IMIS Journal)

Strong authentication is important for securing our networks, but people often make mistakes resulting in inappropriate application of the methods. The mistakes can be characterized as failing to (correctly) answer the questions, "What should we authenticate?" and "What is doing the authentication, and do we trust it?".

Biometrics

Sometimes I have heard (usually from biometric vendors) that biometrics will be the great enabler for e-Commerce. We imagine customers shopping online, and, at the "checkout", they place their finger (or hand, or eyeball) on the reader attached to their PC, authenticating their authority to transfer the funds and complete the purchase. The first question, "What should we authenticate?" is correctly answered. It is the customer who is making the purchase, and e-Commerce is still between people. The second question, "What is doing the authentication, and do we trust it?" is more complex, but an essential component is the reader on the customer's PC. That is responsible for reading the finger and checking it has a pulse (unless you want to do business with corpses). A thief could copy someone's fingerprint data and use a modified reader (which falsely reported a pulse) to introduce the data to the system. Essentially, the fingerprint data is a unique identifier, but it is not

useful for authentication until we also have trusted information that the finger is there now, and alive.

Can e-Commerce get around this problem? A tamper-proof fingerprint reader with a secure communications protocol could be built, but then an e-Commerce site will have to provide these for its customers. Inter-operability between sites and vendors will become an issue and this becomes not an enabler, but a recipe for complexity and confusion.

Machine and Software Identifiers

Another case where authentication requirements have been confused is with the Pentium III serial number. It has been suggested that this will be useful for e-Commerce, for example, from Intel's website, "System identification can enable certain benefits, such as authenticating participants in a secure chat room or enhanced security in e-commerce situations" (see http://support.intel.com/support/processors/pentiumiii/psu.htm).

This fails both of the questions: The processor is identified, but we chat and do e-Commerce with people. Commerce is about people, not processors, making agreements. This will cease to be a problem when we get chips implanted directly into our brains, but until then, processors are used by different people and people use different processors at different times.

For the second question, Intel's Pentium III serial number is not an authentication method it is an identification method. The example of a passport illustrates the difference: I can authenticate my identity using my passport. I present myself at the border with my passport, and the official can verify that the passport is real, and it has my photo in it. No border would accept me without a passport if I said, "My passport number is...". In computing terms, the serial number verification program could be executed in a virtual machine that can be configured to report any desired serial number. Strong authentication must assume a hostile environment.

Is the serial number totally useless? No, if you assume a non-hostile environment, it is a useful identifier, for example for asset tracking and management.

An example of software identification is the Microsoft Office GUID. This is also not an authentication mechanism. The GUID identifies the installation of Office the document was originally created on. Also, it does not fulfil another important function required for verifying a document: integrity. It does not guarantee that the document has not been modified since leaving that Office installation (for example, by the addition of a virus).

Privacy

The last two examples have been used to illustrate how privacy advocates were obstructing strong authentication. I disagree - these identifiers cannot be used for strong authentication, but they can erode privacy and anonymity. In order to achieve anonymity, the communication must have no identification of its source. Therefore, an identifier like the PIII serial number or Office GUID is sufficient to destroy anonymity but they are insufficient for the non-repudiation required of authentication.

The situation was particularly bad for the Pentium III serial number in its' original form, because it could not be disabled. Users, therefore, could not choose whether their processor was identified.

These are both cases where the inclusion of an identifier without the user's consent makes it more difficult for people to choose anonymity. Anonymity does have an important role in a free society - Watergate is just one example where the whistle-blower required anonymity, and just the same newspaper that would refuse to publish an unsigned letter published a properly investigated story that came from an anonymous tip-off.

We need an infrastructure that allows us to choose between authentication and anonymity. The examples of the Pentium III serial number and the Office GUID are not examples of authentication or of governments seeking to suppress authentication. They are certainly not a worrying trend for those who hope to see smartcards employed as a universal authentication feature because smartcards are fundamentally different from these examples.

Smartcards and similar tokens do not have this flaw of enforced identification or authentication. In the best implementations, the private key never leaves the card. The user therefore has a simple, physical method to prevent unwanted authentication: remove the card from the reader, or better, only insert it when authentication is desired. Of course these implementations involve the use of strong public key cryptography, which is the technology the US Government has been trying to restrict.

This does not imply that smartcards and tokens are a perfect solution for authentication. One vulnerability is that, when the user reads the agreement on screen, enters the card password and clicks "sign", they trust the software to present the same agreement to the card as they saw on screen. Nevertheless, smartcards and tokens do solve several problems and I expect them to become more common.

Total online anonymity is like a city of masked people; the opposite extreme is a city of people with their names tattooed on their foreheads. The

reality is somewhere in-between, and much more complex: we have no way of identifying the vast majority of people we pass on the street, but in some situations we identify and authenticate ourselves by much stronger methods. We need the same choice in cyberspace.

Smart HKID

Personal Opinion by Allan Dyer

I would like to congratulate the organizers of the Smart HKID Forum, held on 6 January 2001, for arranging an excellent event. I was particularly struck by the quality of the questions from the floor. The audience obviously included people with practical experience and even expertise in many of the key technologies for the project: smartcards, encryption, biometrics and security planning.

It is because of this observed knowledge that I would like to repeat a request I made at the forum: that the Government should publish the security details throughout the project. The smooth response was that openness and transparency were good, but had to be balanced against the greater chance of "hackers" attacking if details were revealed.

However, I think that full publication will increase public confidence in the project and, ultimately, make it more secure. Security through obscurity is often flawed and fails; the DVD CSS protection scheme and the GSM encryption are just two examples of this. Just because the information is not published does not prevent criminals trying to obtain it by illegal methods, or reverse-engineering the systems. If a criminal discovers a flaw, s/he will exploit it for his/her own gain silently.

Conversely, if the details are published, there are two benefits. More knowledgeable people will look at them, giving a greater chance of finding flaws at an early stage when they can be fixed more cheaply. Secondly, those knowledgeable people will be able to assure their friends, "this is a good project, and it will work securely". Without the published details, those knowledgeable people can only say, "I don't know, there are so many things that could be done wrong". This works for the privacy concerns too: if enough details are known, we can see the privacy protections are working correctly.

Seminar: Cyber Crime and New Laws

This seminar, co-organized by 19 IT professional bodies, is a very good opportunity for the IT counterparts to communicate concerns and opinions on cyber crime and new laws which are proposed by the Security Bureau (Report of the Inter-departmental Working Group on Computer Related Crime) in the early December 2000. Details of this seminar are:

Date: February 17, 2001 (Saturday)

Time: 2:30pm to 5:30pm

Venue: Chiang Chen Studio Theatre, Hong Kong Polytechnic University, Hung Hom, Kowloon

Speakers:

Miss Siu-hing CHEUNG, Deputy Secretary for Security (Special Duty), Security Bureau

Professor Samuel CHANSON, Chairman of the Information Security and Forensics Society

Mr. Tom ROBERTSON, Vice-President of Business Software Alliance

Language: English and Chinese

Fee: Free

Inquiry: For further information, please call Miss Michelle Ho at 2509 3211 or visit http://www.sinchungkai.org.hk/ .

Registration: Online registration is available at http://www.sinchungkai.org.hk/.