Yui Kee Computing Ltd.

Newsletter

October 2002

Contents

Incident Update

W32/Klez.H-mm continues to top the virus lists. The W32/BugBear-mm outbreak peaked around 6th October. The FriendGreetings.com email scam is a new development that emphasises the dangers of trusting code from unverified Internet sources; see "Check Small Print Before Starting E-Card Avalanche" below.

Apology

Recently, subscribers to this mailing list have received unnecessary virus warnings about infected emails from us - this was the result of miss-configuration of our email anti-virus scanner. We apologise for the inconvenience.

How did this occur? All our incoming and outgoing email to yuikee.com.hk gets scanned for viruses (we do have an alternate domain, samples.yuikee.com.hk where incoming email is not scanned, so that we can receive samples for investigation by technical support). When an infected message is identified, a warning message is sent to the sender and recipient. Apparently, someone got infected with the worm W32/Bugbear.A, the worm found the address of our newsletter mailing list, newsletter@yuikee.com.hk, on the machine (this probably means they are a recipient of this newsletter) and sent itself to that address. Newsletter@yuikee.com.hk is a moderated list, so email from anyone except the moderators will be rejected. However, the email is scanned for viruses before the list checks, and the warning message was sent from the address of one of the moderators of the list, so the warning message was accepted for delivery to all the list members. We have now changed the configuration of the virus scanner so that warning messages are not sent from any list moderator's email address. This will prevent a repetition of the problem, as the mailing lists will now reject messages from the virus scanner.

Who Should You Warn?

The above apology does highlight the question, who should you warn about an infected email? The situation is not simple, and recent viruses have made it more difficult. To some extent, it depends on organisation policies, but these suggestions are probably suitable in most cases:

All Messages

The anti-virus administrator should get all warnings - this is useful for statistics to show the severity of the virus problem and diagnostics when tracing problems. Whether this is implemented as messages to the administrator's pager, or a line in a log file the administrator can access will depend on the administrator's preference and the volume of alerts.

Outgoing Messages

The sender should be warned; the recipient should not be warned. Most organisations do not want to advertise that they have a virus incident. When the sender is warned, they should follow the standard procedure for a virus incident (contact technical support, get the infection cleaned), before resending their message.

Incoming Messages

The sender and recipient should be warned. It is polite to warn the sender that their message is being blocked, and why. It is useful for the recipient to receive a warning, so that they can be aware someone is trying to contact them, but is failing (were they waiting for that big P.O.?)

Internal Messages

When the message is to and from the same organisation, then it is really up to internal policy. Probably alerting both sender and recipient is appropriate.

Exceptions

Mailing Lists

As we, inadvertently, demonstrated (sorry!), sending a message to an entire mailing list when just one member is infected is unnecessary. Unfortunately, there is no way for an anti-virus scanner to determine whether a recipient address is a single user or a whole list. Ensuring that warning messages are sent from an address that is not a moderator or member of any list does prevent this on moderated and member-only lists.

Forged Email

An increasing number of email worms, including two of the currently commonest ones: W32/Bugbear.A and W32/Klez.H, forge the sender's address so that there is no reliable way of determining from where they arrived. In this case, warning the apparent sender is worse than useless - at best, it wastes the time of an innocent party; at worst, people take damaging action in a miss-guided attempt to get rid of a non-existent infection, or start ignoring all warnings, even when they have been infected.

One solution would be to stop warning the sender in all cases, but this would make the situation worse for viruses where the sender can be reliably identified. The fact that W32/Klez.H, a virus that forges the sender's address, has persisted at high levels in the wild far longer than similar viruses that do not forge the sender's address strongly suggests that an important factor in eliminating viruses is people (or email scanners) who use updated anti-virus software telling people who do not that they are infected.

A better solution would be an email anti-virus scanner that is aware of the viruses forge the senders address, and which modifies its' alerting behaviour accordingly. Unfortunately, I am not aware of any gateway products that have this sophisticated adaptive capability.

Are You Wasting Money on Security?

Allan Dyer

Recently, I visited a new Network Operations Centre that was promoted as "world class". It is currently undergoing evaluation for BS7799 certification, so, naturally, I looked carefully at their security arrangements. One impressive feature was the physical access control to the control room. To enter, staff use a smart card, type a PIN, and place their finger on a fingerprint

reader. This gets them through the first door and into an anteroom. To open the second door and enter the NOC itself, they present their eye at an iris scanner. As I said, impressive.

Back to some authentication basics: there are three, possibly four, ways of authenticating someone summarised as: Something you know (in this case, the PIN), Something you have (the smart card), Something you are (biometrics, the fingerprint and iris) and Something you do (such as the way you sign your signature - I think this could be classified as a sub-category of biometrics). Using just one of these methods (single factor authentication) provides some assurance that the right person is given access, but it may still fail - a PIN can be guessed, a smart card can be stolen, biometrics have a false positive rate. Using two-factor authentication provides a higher degree of assurance, because two methods must be broken, in quite different ways. Three-factor authentication provides still higher assurance. Using the same factor twice does not increase the security - if we give the staff two, different tokens, they probably keep them in the same pocket, and they get stolen together, or if they choose two, different passwords, they probably find them difficult to remember and write them on the same piece of paper.

So, what does using both fingerprint and iris scanners gain the NOC? We can re-phrase this: under what circumstances would one of the methods fail, but the other work? When control of the fingerprint is separate from control of the iris. Perhaps the attacker cuts off the finger of an authorised member of staff, but an attacker determined enough to do that is certainly determined enough to *threaten* to cut off body parts if the staff does not let them in. Actually, a properly designed fingerprint scanner will check for a pulse, so a severed finger would not work, but that just makes it more likely that the fingerprint and iris stay together, and whoever controls one, controls the other.

The NOC could use just one biometric method, and still get the same level of authentication, by using two methods, it is just wasting its' money. I expect they will pass the BS7799 certification, because that evaluates whether they have effective security. It does not say whether it is cost-effective security. Security will always be an added expense, but there is no reason to make it more expensive than necessary.

Fight with Spam

Everyone with an email address is familiar with spam. “Spam” e-mail is generally defined as unsolicited mailing with many copies flooding the Internet. In most cases, the Spam is some form of commercial advertising as it costs the sender very little compared with a traditional letter. However, the increasing volume of spam is a growing cost for the receiving individuals and companies. As long ago as 1996, a company called Cyber Promotions sent 1.8 million emails to AOL users *per day*. Now, MessageLabs reports than one in seven emails in the U.K. are spam, and some estimates say that that rises to 30% in the US. The problem is also growing in Hong Kong, recently we have observed a growing number of local companies sending unsolicited advertisements.

Supports of spam say that it only takes a moment to delete an unwanted message, but MessageLabs figures suggest that 10 percent of each working day is spent dealing with spam. If only one in ten of Hong Kong's 300,000 companies sent you an unwanted message just once a year, you would receive 82 messages a day. Taking just ten seconds to identify and delete each one would occupy almost two working weeks each year. So spam is a significant burden to the recipient, and ISP and online service companies are also the victims as it occupies their servers and bandwidth.

The spammers mailing lists may be created by searching web-pages, stealing from ISP or Email-provider companies, scanning the Usenet postings or simply guessing at possible addresses, like sales@yourdomain.com. Responding to the "click here to be removed from this

list" may just make the problem worse, as this confirms to the spammer that your address is active.

Spammers may also use underhand methods when sending the spam: They may conceal the real origin by forging the From: address in the message and envelope. They may send the mail directly from a dial-up account, without going through the ISP's mail server. These accounts are known as throwaway accounts because the spammers know they will be shut down within a few days - they may pay for these accounts using stolen credit cards, taking the spammer from antisocial to criminal behaviour. They may send the mail via open mail relays (mail servers that accept mail from anywhere to any destination - this used to be the standard configuration when the Internet was small and friendly, nowadays the normal practice is to only accept mail to is to or from your organisation).

Yui Kee provides a choice of spam-fighting systems to meet different organizations' needs:

To take control of your organisation's email, eSafe Mail (http://www.ealaddin.com/esafe/mail/) provides anti-relay and anti-spoofing controls, keyword blocking, with a preconfigured list of spam keywords and rules-based blocking and management. eSafe Mail can be installed on your mail server, or as an SMTP Gateway.

To outsource the problem, YKScan (http://www.yuikee.com.hk/computer/anti-virus/ykscan/) provides a centrally-managed and hosted anti-spam service using artificial intelligence to create an ever expanding knowledge base for identifying spam. Customers control their own service parameters via a website

Please contact us at info@yuikee.com.hk for more details on how we can help you fight spam.

Further Information:
http://news.independent.co.uk/digital/features/story.jsp?story=319529
http://spam.abuse.net/
http://www.ordb.org/
http://www.hkispa.org.hk/antispam/cop.html

F-Secure Newsletter

F-Secure has launched their new newsletter:

http://www.europe.f-secure.com/news/newsletter/protected/

Check Small Print Before Starting E-Card Avalanche

Sophos is warning PC users against unwittingly sending e-cards to their entire email address books, thanks to FriendGreetings.com. Sophos have received several calls from users concerned they have received or sent a virus disguised as a link to greetings card sent via the website. Sophos is advising users that the the email is not viral, but is in fact the result of an online marketing initiative run by the e-card company. MessageLabs are blocking all emails associated with this program.

Users following the link are invited to install an ActiveX control in order to view their e-card. Two lengthy end user licence agreements (EULAs) are displayed stating that by running the application the user is giving permission for a similar email to be sent to all addresses found in the users's Outlook address book. In many cases, users will not bother to read the EULA and will allow numerous unwanted emails to be sent.

"A flood of unwanted email can be as much of a problem as a genuine virus. This isn't a virus, or a worm - but it could be considered a real nuisance," said Graham Cluley, senior technical consultant at Sophos. "Companies should tell staff that running code from the internet is only allowed if permission has been given by their IT department. Too many people are blindly

believing everything in their inbox when simple safe computing procedures can reduce the risk of spreading a whole range of internet nasties."

MessageLabs commented, "A serious side-effect of this kind of program is that it by allowing it to run, you may potentially breach many laws governing data protection, by allowing the email addresses in your address books to be used for purposes other than that for which they were originally collected and without the consent of the recipient."

Sophos advises practising safe computing to prevent infection by viruses or being targeted by viral campaigns. Specifically, companies could consider blocking employee access to www.friendgreetings.com and block emails containing the words 'you have an E-Card from' in the subject line.

Further details on the FriendGreetings email and how to stop it entering your company can be found at:

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

http://www.messagelabs.com/viruseye/report.asp?id=111

Full details of Sophos's safe computing guidelines can be found at:

http://www.sophos.com/safecomputing

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