Yui Kee Computing Ltd.

Newsletter

January 2003

Contents

Editors Notes

We have a letter this month, commenting on last month's article, "Good Advice?". We do welcome any kind of feedback on this newsletter, not just from suppliers. Send them to me: adyer@yuikee.com.hk. Messages will normally be regarded as private, if you do not mind them being published mark them "for publication".

Incident Update

A new variant of a mass-mailer that forges the senders' address, called W32/Yaha.K@mm, became prominent on 30 December. MessageLabs first stopped a copy of this on 21 December, and they saw a slow exponential increase until it was in second place (to Klez.H) at the end of the year. However, there was more than the usual confusion about naming of the virus. MessageLabs commented, "By releasing a number of variants over a short time period, the authors either accidentally or intentionally caused chaos with the usual processes of virus naming, and so currently we have three variants of Yaha spanning the letters J to M, but very little agreement between the different vendors as to which is which." Sophos was able to detect the later variants through their detection of the December 24 variant.

The New Year has begun with a bang, with four new worms becoming widespread in just two days. "Several new viruses are found every day, there's nothing special with that", says Mikko Hypponen, Manager of Anti-Virus Research at F-Secure. "But it is not normal to find four new viruses which are all successfully spreading in the wild within two days." Mr. Hypponen went on to say this does not appear to be a coordinated attack.

Two of the worms, W32/Lirva.A and W32/Lirva.B (also called W32/Naith and W32/Avril) are closely related and hit on the 8th and 9th of January, respectively. They spread by sending themselves to email addresses harvested from various files. The emails can have various subjects and body texts, mostly business or security related, but some refer to teen skater-punk Avril Lavigne. They also open Avril Lavigne's website and display geometric figures on the 7th, 11th or 24th of any month. Rather predictably, press and commentators have focussed on the connection with a young, female super-star, and the worm is commonly called "the Avril

Lavigne Worm". Much has written about virus writers having a male teenager's obsession with sex, but we should remember that the victims are showing the same obsession. The virus writers just seem to have recognised that such a link attracts many people, which makes them no different to newspapers and anti-virus websites that choose to illustrate an article about a self-replicating program with a picture of a skater.

The third worm is a new variant of ExploreZip, found on the 8th. ExploreZip was originally found in June 1999, and it quickly became widespread. W32/ExploreZip.E was compressed to make it undetectable by current anti-virus software at the time it was released, but it is functionally the same. It spreads by replying to unread emails, and also by copying itself to Windows shares across the network.

The fourth worm W32/Sobig.A, was found on the 9th, also spreads by email and network shared drives. It also tries to download extra components from a website, but the website is currently inactive.

Letter

Thought I would ask you a question, to the last comment in your comments to the ISPs recommendations:

'DO update anti-virus applications from time to time

Yes, good, except, lets make that "as often as your anti-virus developer provides updates" - in many cases, this now means daily, or more frequently. OK, ISP, nice to see you making an effort. Try harder next year.'

What do you recommend to your customers if during the period they do not have the new signature available?

Nick Hawkings
MessageLabs

Thanks for the question, Nick - of course, when I'm contacted by a customer in an emergency, I respond with practical advice and help related to the specific virus: any tricks they can use to stop it spreading, what other dangers it presents that they need to protect against (e.g. if it opens a backdoor, which firewall ports should they block?), I might be able to get a virus definition file from the developer more quickly, and send it to them. When an incident happens, the first priority is to deal with it.

However, what can companies do in the planning of their information security? Anti-virus software is not guaranteed to detect all new viruses, and it may take hours or even days for new virus definitions to reach customers - how can companies reduce or eliminate this "detection gap"? Good general security, and good user education will help make the organisation less vulnerable to the latest virus. Outsourcing the problem can provide effective coverage - the large virus outbreaks in recent years have all been caused by email viruses, so getting an expert service to check all your email before it reaches you makes a lot of sense. Of course, Nick, your company provides the most experienced and effective of such services. When email arrives at MessageLabs' Virus Control Centre, it is recursively unpacked and all executable content is scanned using three commercial anti-virus scanners (currently McAfee, F-Secure and VFind, but this is constantly evaluated to ensure the best detection). The centre checks the developer's sites for updates to the scanners every ten minutes. Additionally, the messages are checked by Skeptic, MessageLabs own heuristic (rule-based) scanner, which is optimised for email. Skeptic successfully stopped fast-spreading email viruses, including VBS/LoveLetter and more recently W32/Yaha.K@mm and the Avril Lavigne worm, W32/Lirva.a@MM, in some

cases hours before the traditional anti-virus developers had detection ready. The key is to implement defence in depth.

Allan Dyer

Is Grid Computing Secure?

Grid computing and related distributed computing technologies, are moving into the commercial sector. They offer the ability to tackle extremely complex problems by utilising processing power from multiple, geographically distributed machines. The special features of Grids include their aggregation of resources across multiple administrative domains, and resource management that offers specified performance, cost and quality of service. However, these features also create possible security risks.

Gateway Inc. has set up a grid of its approximately 8,000 display PCs in showrooms around the USA and it intends to offer a grid-computing service to businesses interested in processing computing jobs that would ordinarily require the power of an expensive supercomputer. This appears to be a perfect example of a company utilising an otherwise wasted resource - for the vast majority of the time, the display PCs are required to look attractive to potential customers, but not actually do any processing. Security was also considered in building the grid: the central server controlling it is physically secure and encryption technologies are used to protect data in transit. Data confidentiality is also protected by the nature of the grid - stealing useful data involves infiltrating many machines.

A rather different distributed computing project is SETI@Home, where people can assist in analysing radio telescope data in the search for extra-terrestrial intelligence by running a screensaver. The SETI@Home FAQ does have some information about security. They protect the participants from malicious data and Trojans by ensuring the screensaver will only download data from their data server, and only allowing screensavers that have been downloaded from their webpage to participate. To protect the project, they do not make the source code of the screensaver available, and there is a mechanism to detect forged results, which they do not describe for security reasons.

The security issues can be divided into problems for the computing power providers, and problems for the computing power users. The providers will be concerned that the software is not a Trojan, that it will only act as specified and not steal data, or open new security holes, or consume too much processor time. This is no different from the concerns of using any other software, and can be addressed in the same way: only use software from trusted suppliers. The users have different problems: their data might be stolen, or wrong results returned. This is similar to outsourcing processing to a traditional data centre, but addressing it in the same way, by only using trusted providers, fails because there are multiple providers in multiple administrative domains.

In the case of Gateway, the computers are all under Gateway's administration, but they are in insecure locations - members of the public enter the showrooms and try out the machines. A determined attacker has the opportunity to take away a copy of the software, reverse engineer and modify it for the desired result, and then re-introduce it to the showroom computers. The attacker could package the modification as a worm that could infect the other showroom PCs on the network, changing their software in the same way - there is then no difficulty in infiltrating enough machines to be able to steal a useful amount of data.

In the case of SETI@Home, the FAQ reveals the vulnerability - they admit to being concerned about falsified results. Their protection is to not release the source code, and to have an unspecified method to detect forged results. This is "security through obscurity" and detailed reverse engineering of the screensaver would reveal the tricks used.

However, I am not concerned about an attack on SETI@Home because there is no payoff to falsifying results. The owner of the computer where the data demonstrating the existence of aliens was processed would get a special place in world history, but a positive result will be carefully checked so the lie will be quickly revealed. Most results will be negative, and the only benefit for a cheater reporting another negative might be that they could "process" more blocks of data, as they are not actually doing the work. The security through obscurity of the project makes cheating difficult enough that no one will bother. Actually, a false negative result would benefit an attacker who wanted to conceal the existence of ETI, but the concept of a worldwide conspiracy of aliens sabotaging SET@Home is probably best left as a plot for an X-files episode. So we assume that the data is being processed correctly, and, as it is data that would probably never be processed otherwise, there is a significant benefit in the project.

The situation changes when Grid computing becomes commercial because there could be a significant payoff. If providers are paid for the processing power they supply, then not processing the data and returning a "normal" result would allow a cheater to "process" more data, and be paid more. False results may also give an advantage to a competitor, for example, if Grid computing is used for molecular modelling for drug design, a rival drug company could benefit by disrupting your research programme. In general, falsified results are not a security risk for grid computing if results that give a benefit to an attacker can and will be easily checked. That can be restated, results that will not be checked give no benefit to an attacker. However, the attacker's objective might be to steal the data being processed - this vulnerability can be fixed if the data can be effectively "anonymised".

So Grid computing has great potential for making massive or special computing power available to customers that could not otherwise afford it, but its nature, in particular, the fact that it involves machines across multiple administrative domains (and, therefore, under different security policies) create special security vulnerabilities. Potential users should evaluate the risks carefully.

Graham Cluley Speaks in Hong Kong

On 7th January, Mr. Graham Cluley, Senior Technology Consultant at Sophos Plc and one of the world's leading anti-virus experts, spoke to a select audience, including some of Yui Kee's most important customers.

Graham's topic was, "Computer viruses: 2002 in review and predictions for the future" and he was in typical, entertaining form. Talking about the major incidents last year, he described information security managers who go "smug mode on" in response to typical outbreaks. Over 90% of outbreaks are currently caused by mass mailing email worms that can be stopped by very simple and inexpensive techniques. When managers who have implemented these techniques are asked about the latest, high profile worm they will look smug and airily reply, "Oh, we never saw that".

Is Someone Selling Your Mailserver?

Spam selling lists of millions of email addresses is very common, now we seeing spam selling lists of open relays. The message in question started its sales-pitch, "Sick and tired of always looking for good open relay mail servers?" and offered, "thousands of good ones", "checked every hour" to be "delivered to your inbox every day for only $25 /mnth".

What does this mean? Those familiar with email systems and open relay blacklists can skip to the next paragraph. Normally, when you send email, your computer connects to your local mail server (in your office, or at your ISP) and gives it the message, with the destination address. That mail server looks up the location of the destination mail server, connects to it and delivers the message. When email is sent to you, your local mail server receives the message and puts it in your mailbox, ready for you to read when convenient. So, normally, your local mail server will be handling messages that either originate from or are addressed to your organisation (or both). What happens when your mail server receives a message that neither originates from or is addressed to your organisation? Many mail servers are configured to refuse the message, a mail server that accepts and delivers the message is called an Open Relay. Spammers love Open Relays, they can send an open relay one message, with hundreds or thousands of destination addresses, and it will happily deliver their spam. The bandwidth of the owner of the open relay gets used, not the spammers, and it helps the spammer conceal the source. Because of this, there are blacklists of open relays published, and some organisations (Yui Kee included), refuses connections from mail systems on those lists - this might be expressed as a policy, like: "You must secure your mail server against abuse by spammers before attempting to send us email".

Sometimes, the legitimate users of open relay mail systems complain about their email being blocked ("Why have you blocked my message?, This is against Free Speech!"). Explaining what the spammers are doing, stealing their bandwidth, and how they can fix it, does not always help, ("I cannot be expected to understand these obscure technical details!"). Now we can give these confused victims a message with a dollar sign: Spammers are **selling** other spammers the address of your mail server, so that they can abuse it too. Wake up - someone is making money from your mail server, and it is not you!

eToken Now Entrust Ready

Aladdin's eToken Pro, a USB authentication system, has achieved the Entrust Ready designation. The interoperability allows storage of a user's Entrust digital ID on a secure, personal eToken.

Entrust's vice president and chief marketing officer, Ian Curry, said, "Our Internet security solutions are key to creating a flexible and extensible secure network and e-commerce environment for our customers. Our customers need reliable and easy-to-implement technologies for strong, two-factor authentication-combining our Digital IDs with eToken provides an excellent authentication solution for customers."

Aladdin's vice president eToken solutions, Leedor Agam, said, "Ease of use and mobility are the main benefits provided by using eToken with the Entrust solution. Entrust users can now take full control of their identification credentials, making their use simple and fully mobile."

More information:
http://www.ealaddin.com/news/2003/etoken/entrust.asp
http://www.yuikee.com.hk/computer/token/eToken/

Fight Back Debate

Allan Dyer

In the November 2002 newsletter I reported on Jimmy Kuo's suggestion at AVAR 2002 that legislation was needed to allow individuals or the authorities to counter strike against machines that are infected and attacking others. The debate on this idea continues, Timothy M. Mullen, who proposed the idea last July, has defended it on Security Focus, see: http://online.securityfocus.com/columnists/134.

Mr. Mullen seems firmly in favour of empowering individuals to take action. Personally, I fear that this would lead to over-enthusiastic vigilantism, so the power should be in the hands of a competent authority. Such an authority would have to be established to react quickly - this may prove difficult for the USA justice system, which took two years to sentence David L. Smith, the author of the Melissa virus. Interestingly, Mr. Mullen presents some examples of comparable cases where an individual is targeted for the good of society, "If parents don't vaccinate their children, the state takes them out of school. If a dog consistently attacks people, the authorities put it down", these show we rely on a competent authority, not individuals, to take action in such cases.

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