Yui Kee Computing Ltd.

Newsletter

March 2001

Contents

Change of Style

We have changed the style of the newsletter slightly this month. As we expect most people to be reading this on screen, a single column and a slightly larger font should be more readable. Please let us know which you prefer.

Who Loves Anna Kournikova?

Last month we suggested there could be an outbreak of an email virus on 14 February, we were wrong, VBS/SST-A (the Kournikova worm) struck on 13 February. Initial statistics from MessageLabs (http://www.messagelabs.com/) indicated it was spreading twice as fast as VBS/LoveLetter did in May 2000. However, reports made to Yui Kee suggest that it hit far fewer companies in Hong Kong. This was probably related to timezone differences of the source, Philippines for VBS/LoveLetter, Netherlands for VBS/SST-A.

The creator of VBS/SST-A apparently posted an apology on the Internet and turned himself in to the police (see http://www.sophos.com/virusinfo/articles/kourarrest.html). We welcome his arrest. Although his intention might have been a joke or a demonstration of insecurity, the fact is he disrupted thousands of users around the world.

We do not need another demonstration of this vulnerability; Melissa and LoveLetter have already proved the point. In this context, the comments of the Major of his town (see http://www.sophos.com/virusinfo/articles/kournoreward.html) suggesting he should be rewarded with a job offer, are deplorable. Before we laugh at foreign politicians demonstrating their ignorance of technical subjects, we should remember that some of our own politicians also sometimes show their ignorance. However, the politicians who preface their remarks with how little they know of technical subjects tend to show the deepest grasp of the issues involved.

Too Many Alerts

Sometimes, anti-virus vendors are accused of crying wolf, they rush out with press releases about the latest highly destructive virus which quickly turns out to have affected almost no-one. The recent VBS/SST-B (a minor variant of VBS/SST-A, with a German message) and W32.Naked@mm (the "Naked Wife Trojan") are examples of this. The press are quick to follow-up on such releases; massive virus outbreaks bringing businesses and countries to their knees are good copy. Users get tired of the repetitious warnings, until they fall victim to a real epidemic, such as Melissa or LoveLetter.

As an Anti-Virus distributor and consultant in Hong Kong it would be unfair for us to point an accusing finger. We try to judge each case and provide timely, accurate and balanced information on virus emergencies. We will not be naming companies in these examples, you should judge your suppliers actions yourself.

Anti-virus developers have, to some extent, a split personality. There are the techies, who analyse and deal with the new viruses – their concern is to serve the company by giving the customers the protection they paid for. Then there are the marketers – their concern is to serve the company by getting the maximum favourable publicity. When a new threat is discovered, particularly if it has the capability to spread very fast, they both want to get a warning press release out as quickly as possible.

However, in some companies, the marketers appear to have a bit too much influence. If things are quiet, they will release a warning about a months-old virus that is no longer causing problems. Or they release a warning about a virus that, for technical or social reasons, it is clear will not spread very far or fast. Even worse, some have issued warnings about viruses that no one else could confirm even existed.

Some cases are less clear – at one point, reliable statistics showed that VBS/SST-A was spreading twice as fast as LoveLetter, so a major alert was justified. Only hindsight could show us it would be less successful overall. However, some companies also made a worldwide press release for VBS/SST-B, even though its German message made it unlikely to spread outside of German-speaking countries.

Good Security is Boring

System administrators and information security staff have a similar problem to anti-virus vendors when trying to get the message out to users. So much of computer security depends on users, from choosing good passwords to not indiscriminately clicking on email attachments, but the message is not exciting. There are any number of films where breaking a security system or a security system failing has been a central feature of the plot, but none which prominently feature a successful security system. The reason is obvious, successful security is boring – you take care of all the tedious details, and nothing happens, no dramatic break-ins, no chases, no explosions.

Therefore, the big security failure is often the only chance we have to get the message to users and managers. Managers are the more important target: to be effective, the security culture of an organisation has to come from the top. Use the statistics from vendor press releases and internal organisation data to present how much money good security is, or could be, saving. But avoid the hype which can undermine your case – LoveLetter was certainly a major, worldwide incident, but the figure of US$10 billion for damages is highly speculative.

YKScan Service

Last month we introduced MessageLabs (http://www.messagelabs.com/) and their managed service scanning Internet email for viruses. Yui Kee is now providing local, Chinese technical support and re-badging the service as YKScan. The pricing starts at HK$17 per user, per month. This is an excellent solution for organisations with their own domain name that have had trouble with email-borne viruses.

Recently, the virus-writer known as Kalamar (who previously created the kit used to make VBS/SST) has released a new version of his virus-generation kit. It has already been confirmed that YKScan, utilising the Skeptic heuristic scanner, will detect and stop all possible variants generated by the new kit.

Contact us for further details, subscription forms or to ask any questions: cdsales@yuikee.com.hk .

HKCERT

The Hong Kong Computer Emergency Response Team (http://www.hongkongcert.org) was launched at the end of February with HK$10.7 million from the government's Innovation and Technology Fund and will be operated by the Hong Kong Productivity Council. Similar to CERTs in other countries, the organization's mission is to collect information relating to computer security such as the latest viruses, security weaknesses and counter-measures, and disseminate them to the public. It will focus on the needs of the small and medium-sized enterprises (SMEs).

It is absolutely necessary to have a CERT in major IT centres; it provides a vital coordination role and will act as a trusted source of information and alerts for the Internet using public and organizations. This move fits well with the Governments plans to make Hong Kong a regional IT hub. Large organizations can also form CERTs for their internal needs.

Evaluating eSafe

Yui Kee staff have been certified on Aladdin's eSafe Gateway and Yui Kee has been appointed as a distributor. eSafe Gateway works independently of your firewall, and examines ftp, http (web) and smtp (email) traffic. Going beyond traditional anti-virus protection, it can be used to enforce an organisation's Internet usage and security policy with great flexibility. For example, it can strip all JavaScript or VBScript from incoming HTML, or just scripts that contain forbidden functions, or only those from, or not from, specific sites. It can greatly cut down on non-productive use of your Internet connection by anti-spam measures based on message source and destination (anti-spoofing, anti-relay and anti-bombing) or content (blocking by keyword), and blocking of non-productive ftp or web sites (by keyword or an optional URL list subscription).

Existing users of eSafe Gateway in Hong Kong include the Government (SCIGS, ESD Life, Electronic Tendering Systems) and Star TV.

Organisations wishing to evaluate eSafe Gateway should contact us for an evaluation CD-ROM: cdsales@yuikee.com.hk .

Port Scanning

Personal Opinion by Allan Dyer

Anyone who runs a firewall, or personal firewall software, will be familiar with port scanning: crackers using programs to attempt to connect to many services on a computer, or a service on many computers. We can compare this to a criminal who

walks down a line of parked cars, trying every door-handle – he's looking for one that is open and can be robbed. The problem on the Internet is, even though legislation in many countries makes unauthorized access to a computer a crime, attempting to connect and failing, or "casing the joint" is not. We see the firewall logs where he fails, but we do not see where he succeeds. Even though the attempts are failing, a cleverer cracker can use the sheer volume of the log files to try to hide the successful attacks.

I think it would be useful to make port and host scanning a minor crime, so that the perpetrator's computer can be searched for further evidence, and so that the Police can use their discretion to impress on "script-kiddies", and their parents, that they are doing something wrong before they get too deeply involved. Unfortunately, the Government Interdepartmental Report on Computer Related Crime did not address this. I would be interested to hear of attempts to address this in other jurisdictions, or opinion on if it could work. adyer@yuikee.com.hk

Sophos Anti-Virus and MIMEsweeper

Sophos Anti-Virus is a popular choice for use with Baltimore's MIMEsweeper and Mailsweeper products because the Sophos Anti-Virus Interface (SAVI) allows an efficient interface and fast performance.

See http://www.mimesweeper.com/support/technotes/av/savi_technote.asp on integrating Sophos and MIMEsweeper.

Yui Kee is the authorised distributor of Sophos in Hong Kong, please contact us for any queries: cdsales@yuikee.com.hk .

Sophos to protect WWF networks from extinction

On 12 March 2001, Sophos announced that the World Wildlife Fund (WWF) selected SAV to protect their UK networks.

Sophos, was chosen by WWF, the world's largest and most respected independent conservation organisation, to provide protection against computer viruses. WWF will install Sophos Anti-Virus protection in 16 offices across the UK; including its UK headquarters in Godalming and national offices in Scotland, Wales and Northern Ireland.

See http://www.sophos.com/pressoffice/pressrel/uk/20010312wwf.html for full details.

F-Secure Anti-Virus Updates

F-Secure has been providing direct updates and technical support since July 2000. If you have not been receiving updates, please contact the F-Secure Technical Hotline: 22384639.

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/