Yui Kee Computing Ltd.

Newsletter

October 2001

Contents

AVAR 2001 Conference

AVAR 2001 is a rare opportunity to meet and hear the industry's top anti-virus experts. The line-up is headed by Dr. Vesselin Bontchev, voted the individual who contributed the most to the anti-virus industry at the Virus Bulletin Conference 2000, as the Day 1 Keynote Speaker; and Ms Eva Chiang, who received the Secure Computing Lifetime Achievement Award in April 2001, as the Day 2 Keynote Speaker.

The Fourth annual Anti-Virus Asia Researcher's Conference will be held 4-5 December in Hong Kong. Full registration details at the website:

http://www.aavar.org/avar2001/home.html

11th September 2001

After the loss of so many lives, it seems inappropriate to talk about anything other than the human tragedy, but this newsletter is about Information Security and there are lessons to be learned. Yui Kee offers it's condolences to those affected.

Business Continuity planners need to "think the unthinkable" and prepare for it because sometimes, the "unthinkable" happens. After the catastrophe, when the emergency services have finished, the survivors and others affected must get on with their lives. They depend on businesses as employees or as customers, and it is only handing the terrorists another victory if the businesses fail. Major disasters are, thankfully, rare, but a minor disaster, such as a building power failure can shut down an office almost as effectively.

Good backups are a boring but essential component of Information Security. They allow recovery from so many situations - the tapes sitting next to your server can restore the

accidentally-, or virus-deleted files. The fireproof safe in the basement can contain enough to rebuild the server after an office fire, but only off-site backups can get you running again in a reasonable time after a massive building collapse. This need not be expensive or complicated for an SME - the Managing Director can store the weekly or monthly tapes at home.

Incident Update: Nimda

Last month, a worm called "Nimda" was spreading rapidly. Its' initial speed of spread was even faster than CodeRed's. This worm consists of a mass mailer and a web worm. It can propagate via infecting files, mass mailing, vulnerable IIS servers and file sharing. Also, a non-IIS web server (such as Apache), could act as a passive carrier of Nimda if infected HTML files were uploaded to it - this will help the worm to spread further. Therefore, non-IIS web servers cannot be considered as 100% safe. Browsing the infected web servers with vulnerable IE might get infected transparently. On the other hand, we have not seen any email propagation cases so email gateway AV solutions will not reduce the spread very much. That is why MessagesLabs, an Internet level email AV service provider, only rates it as low risk but other AV developers rate it as Medium to High risk.

Once the system gets infected, removal is not easy. Fortunately, most of the AV developers have released auto-removal tools. However, the key disinfection step is disabling all network shares or temporarily disconnecting hosts from the network until all machines are cleaned. Therefore the tools cannot prevent business loss in corporate environment. Again, keeping software up-to-date and patched is the easiest way to minimize the recovery cost. Also, installing content security products like eSafe Gateway can also prevent users from downloading dangerous file types from the Internet.

A new variant "Nimda.B" was discovered on 9th October. The only difference is that it uses PUTA!!.SCR and PUTA!!.EML as the file names. According to the AV developers, it is not widely spread.

Loosing Support

Some anti-virus companies are announcing timetables for the death of their older products, such as those for Windows 3.1, NT 3.51 and, in some cases OS/2. This raises some issues about the nature of anti-virus software:

Anti-virus software is different because it is essential utility software that becomes less effective as time passes. If you created AV software that caught 100% of known viruses in 1987, today that same software would detect about 0.002% of known viruses. Another way of describing this is that AV software has become 60,000 times more powerful since 1987 - which is probably unique among software packages (I would certainly appreciate a word processor that would help me work 60,000 times faster...). The truth is, that is how fast the virus problem is growing and, to be useful, AV software must keep pace.

This leads to the second difference - AV developers keep releasing updates and upgrades for old platforms, far longer than for other types of software. How long ago did you last hear of anything else new for Windows 3.1? However, there still comes a point when further support is not justified, and each developer has their own criteria for that.

What if you must use the old platform? There may be solid reasons why the old platform must be used, in which case the full situation and all associated risks should be examined. Switching to a solution from another vendor might be an option - developers' criteria do differ. There are also several reasons why the risks may be lower: Many newer viruses will not work on the old platforms (however, if the system is a server with newer clients, it could still store and allow exchange of infected files, even though they could not execute on the server itself).

The system is probably not having new programs installed and run, meaning less chance of infected software being introduced. Indeed, the installed software is probably very stable (that is one reason it is still being used) and has not changed in years. Together, this might mean that a combination of the last release and update of the AV software (to catch the old viruses that might still be on old media), plus good backups and change control procedures will give an adequate level of protection for some time to come. Ultimately, it depends on the circumstances.

If you are using Windows 3.1, NT 3.51 or OS/2, please contact us to discuss your particular requirements.

About CodeRed

A user asked: "I use Cable modem and my cable modem lights has been on constantly from pings of machines infected with Code Red. Will YKScan get rid of this virus?"

No, YKScan protects against viruses in email, CodeRed does not use email to spread. If you are not using Microsoft's IIS then your machine will not get infected with CodeRed. If you are, then installing the security patch protects your machine from infection.

If you are not charged by the bandwidth you use, the constant flashing is not a concern to you - it represents bandwidth used by Code Red, but you were not using that anyway. It might be a concern for your upstream ISP, who may be overloaded by the traffic on everyone's line...

There aren't any good ways of dealing with the CodeRed traffic at the moment. When worms like this become common, we might see a big shift in the culture and management of the Internet in order to cope.

Personal Computer Security

A very effective method of personal computer security:

http://www.uoe.dk/csworld/security.html

F-Secure's security solutions to support Microsoft Windows Powered Pocket PC 2002 Software

F-Secure Corporation today introduced F-Secure FileCrypto for Pocket PC Enterprise Edition, a full-featured file encryption application that provides strong protection for Microsoft Pocket PC 2002 devices against unwanted data disclosure.

Pocket PC 2002 is the next generation software for personal digital assistants from Microsoft Corp. F-Secure introduces F-Secure FileCrypto for Pocket PC Enterprise Edition as a partner in the launch activities for Pocket PC 2002. The new encryption application will provide Pocket PC 2002 users with a premier product that utilizes the benefits of the new enhanced platform.

"Corporations view data security as a key element in their mobile computing standard," said Andy Haon, Director of Product Planning for the Mobility Division at Microsoft Corp. "F-Secure FileCrypto for Pocket PC Enterprise Edition helps to address this key enterprise need, which will benefit users with enhanced security options for the Pocket PC 2002 Software."

F-Secure FileCrypto for Pocket PC Enterprise Edition has been designed to protect devices in demanding personal use and corporate environments, where fully automatic data protection and strong user authentication is required. It automatically encrypts sensitive data before storing and decrypts it again when it is needed, without any user intervention. Confidential documents and personal files in the encrypted folders remain always safe.

"Handheld devices can be very productive in enterprise use, provided that corporate information in the device memory is protected against unauthorized access in all situations. The combination of Pocket PC 2002 and F-Secure FileCrypto for Pocket PC Enterprise Edition offers best available security to corporations deploying PDA devices. Working together with Microsoft has been an important part of our product development for this new platform", said Ilkka Starck, Vice President, Wireless Security Solutions from F-Secure Corporation.

F-Secure FileCrypto for Pocket PC Enterprise Edition is available immediately and the Pocket PC 2002 version of the product will be released in October. Contact cdsales@yuikee.com.hk for details.

Sentencing the Author of the 'Anna Kournikova Worm'

On the 27 September 2001, Jan de Wit (the author of VBS/VBSWG.J@mm, better known as the 'Anna Kournikova Worm') was sentenced to 150 hours community service, or, if he prefers, 75 days in jail. When this worm appeared, it spread rapidly worldwide and quickly reached the top of the lists of most anti-virus developers. It caused widespread disruption, so many say that the sentence is too lenient:

Graham Cluely of Sophos said, "Considering that Anna K. was one of the top five viruses of all time and was as big as Melissa, the prosecutor's request sends out all the wrong signals to the industry."

Jason Holloway, U.K. general manager with F-Secure, said he was disappointed with the light sentence; "It may be due to the FBI's lack of specimen charges against de Wit, but it does not send the right message to the industry."

Opinion at the Virus Bulletin Conference generally agreed that 150 hours of community service was too lenient, but the 18-month jail time that Christopher Pile was given by British courts in 1995 was too harsh.

The major problem does seem to have been with evidence of damage: the FBI was only able to list 55 incidents of infection, causing just US$166,827 worth of damage. In the July issue of this Newsletter, I talked about the importance of reporting - this case reiterates the lesson of the CIH case, without reports, there is nothing to charge the criminals with if they are caught.

However, there are some positive aspects to the case: The judge rejected de Wit's plea that he did not understand the consequences of posting the worm to a newsgroup. Additionally, de Wit's computer and collection of viruses (reported as over 7000) has been confiscated. Realistically, both can be replaced, but replacing the virus collection in particular will be time-consuming, hopefully, he simply will not bother. Also, the case has been dealt with relatively quickly - the worm started spreading on 12 February 2001, and we have a sentence on 27 September 2001. In contrast, Melissa started spreading 26 March 1999 and it's author, David Smith, has yet to be sentenced in the USA. Justice should be swift and accurate.

Virus Bulletin 2001 Report

by Allan G. Dyer

This is a personal look at some of the papers at the Virus Bulletin Conference, held last month in Prague.

Of great relevance to Asian computer users, Costin Raiu explored the complexities of the Multi-Byte Character Sets, and how they affect macro viruses in Microsoft Office. When infected documents are moved between different language versions of Office, some double-byte characters in comments are replaced. Depending on the identification method used

in anti-virus software, this may result in the modified virus going undetected. Also, as some viruses store parts of their code, or other data, in comments, the behaviour of the virus might change. Costin's work will be a useful reference for developers improving their detection of macro viruses in double-byte versions of Office.

Aleksander Czarnowski discussed new types of Distributed Denial of Service (DDoS) attack: Pulsing Zombies, Stick (an anti-NIDS) and 4to6ddos (attacks IPv6 networks from non-IPv6 hosts). He also covered some solutions to DDoS problems (mostly using NIDS) and the involvement of viruses and worms in DDoS attacks. He concluded that the only solution currently really working was detection of DDoS components at a host level, which anti-virus software is ideally suited for performing, and the ultimate protection will involve linking multiple layers of anti-virus and network security protection.

Peter Morley explained the issues around processing of virus collections by anti-virus developers. He had an interesting take in the strategy of prioritising the processing of samples from different sources: in-the-wild samples, monthly collections from other developers and backlog. Peter prompted some discussion by raising the question of advertising the count of viruses detected. The counting of viruses is not simple because some products detect groups of similar viruses generically while others identify exactly. However, Peter's point was that, of the approximately 50,000 known viruses, over half were 'legacy' DOS viruses that are no longer a threat in modern networks. Because these legacy viruses are still included in the totals, they are still usually included in the test sets used in comparisons of anti-virus software. Therefore, the results of the tests are that all products score in the high 90's percent, giving the impression that all products are about as good as each other. In reality, there are often significant differences between products in detection of viruses that are a credible threat in today's networks. Peter wanted to list a lower total of current viruses, with a note: (also detects XX,000 legacy viruses). In my opinion, the number of viruses is essentially irrelevant, what matters is cost-effective protection against the malware that is a real threat to your organisation. Marketing departments that quote larger and larger numbers in their advertising and customers that use those numbers to make purchase decisions are getting it wrong. The issue is more complex than that, and the evaluation should reflect the situation.

John Stojanovski explained anti-virus problems and potential solutions for the Palm OS. The current threat for Palm OS devices is minimal - one virus and a few Trojans, but future developments are likely to change this. Already, Palm OS 4 has an ‘Autorun’-style feature for secondary storage devices which could easily be exploited by viruses. Improvements in connectivity through Bluetooth and the Telephony manager will both increase the potential for spread and the possibilities for damage. John called for the AV industry to be ready for these developments.

Meiring de Villiers explained the legal issues of *res ipsa loquitur* and concluded that a software developer would be liable if they shipped infected software. This, at least, reassures us that the law is not a total ass, but I was disappointed that the much more interesting and complex issues around ordinary businesses accidentally or negligently distributing viruses was not addressed.

Jeannette Jarvis described a Successful Anti-Virus Strategy from the perspective of a major corporation (Boeing). She identified four ‘P’s: Products, Processes, Policies and People; and detailed their use in combination.

A panel from AVIEN (Anti-Virus Information Exchange Network) led by David Phillips explained who they are, and what they do. AVIEN exchanges information about viruses between large corporate users, without Anti-Virus vendors. They have found this to be effective in allowing them to respond to a major outbreak hours before anti-virus developers have released updates. However, in the discussion, Vesselin Bontchev raised the point that if they acted before a sample has been analysed by a Researcher they could be taking actions that will worsen the situation and that any delay in getting a sample to the Researchers is damaging.

I think there is merit on both sides of the discussion - communications in an emergency, including sample delivery, should be streamlined and efficient, but large organisations must also be prepared to act on 'Best Available Data' to minimise the impact, even if the methods chosen are shown to be less than optimal in the long run.

Vesselin Bontchev dissected a virus epidemic. In most cases, we have very little idea about the spread of viruses. However, some viruses take action in a way that can be monitored. W97M/Groov.A is one such virus - it sends a file to Vesselin's AV company's ftp site (perhaps the virus writer wished to inconvenience the company, other AV researchers have also been the target of such tricks) - since 1998 they have received an average of 1800 uploads every day. By analysing the statistics and follow-up, Vesselin showed that there was a delay of several months before the population really started growing, a period of exponential growth, then linear growth and a plateau showing annual variation. Christmas was a definite trough, and April a high-point (perhaps when many SOHO users switch on their computer for the first time in the year to complete their US tax return). W97M/Groov.A has not been near the top of the lists of viruses reported to vendors or researchers, but this self-reporting mechanism clearly shows it is more prevalent. What other viruses are also prevalent, but do not have a self-reporting mechanism? Attempts to contact the infected users showed that the vast majority (97%) were complacent and did not care about virus infections - this is the real reason that the computer virus problem is still increasing.

Jessica Johnston took an outsider's look at trust in the anti-virus industry and found a complex web of different perceptions. The Computer Anti-virus Research Organisation (CARO) is made up of some of the top experts in the AV industry, mostly from competing companies, but they cooperate on resolving virus threats and pooling their knowledge. Trust between members is very important in CARO, but Product Managers may perceive them as sharing more between themselves than they communicate with their own management. CARO has power and influence within the industry, but is virtually unknown to customers and Jessica concluded that CARO must listen to the critiques to survive.

I have touched on less than half the papers presented, but limitations of time and space prevent a more complete report. Overall, the conference was very good, and the city of Prague an excellent location. This newsletter will probably return to some of the issues raised in future editions.

Two Possibly Good Ideas

One problem with defending our networks against hackers is that we do not take action against the hackers. For example, suppose a machine attempts to use an IIS buffer overflow exploit against one of our IP addresses. There are several possible results:

i) The target has an unpatched IIS server, and the attack succeeds. By the time we find out, we probably have no way of identifying the attacker.

ii) The target has a patched IIS server or another webserver entirely, and the attack fails.

iii) Our firewall blocks port 80 for the target, and the attack fails.

iv) The target IP address is unused, or has no webserver, and the attack fails.

For cases (ii) and (iii) we might have log entries that show the source of the attack, but no damage was done and no crime was committed so there is nothing to report to the Police. An enthusiastic Administrator might identify the responsible ISP and report to their 'abuse' or 'postmaster' addresses, but the lack of response quickly becomes discouraging. Any kind of retaliation at the source would be illegal, and, as a worm like CodeRed might be involved, it could be targeting another innocent victim.

DShield.org (http://www.dshield.org/) is a reporting experiment (or a Distributed Intrusion Detection System) operated by Euclidian Consulting. Organisations send their packet filter logs, and DShield analyses them, extracting statistics. Importantly, there are tools to automate the log submission. DShield also picks strong cases of abuse (from reports where the organisation has agreed to this use of the data) and contacts the relevant ISP. Hopefully, the ISP is more likely to take action because a pattern of abuse can be shown. The danger with this is that organisations are revealing their packet filter logs, which could give useful information to an attacker. DShield has a privacy policy on their site, but many organisations would find it difficult to trust an unknown company. It would be good to see this idea adopted by publicly accountable organisations, such as CERTs.

The second idea is from HackBusters (http://www.hackbusters.net/) who have a more controversial approach. In their own words, "Here at HackBusters, we believe that an active defense is equal to a good offense. That's why we've developed LaBrea." Simply, their software allows a machine to be set up to respond to all attempts to connect to unused IP addresses on a network, establishing connections and then allowing them to timeout. A more aggressive mode puts the client into the persist state indefinitely. Thus, any attacker port scanning will spend a long time on each of the unused IP addresses. This can reduce the bandwidth wasted by the attacks, and permit more time for compromised machine's administrators to be contacted before further damage is done. However, this does break the TCP specifications, so it should be studied very carefully before introduction. It assumes that any attempt to connect to an unused IP address is a hacking attempt. Largely, this is true - port scanning is very common, but mistakes, perhaps in updating DNS records, do happen and this "tarpit" will also trap innocent mistakes, and perhaps make recognising and correcting them more difficult.

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/