YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

February 2003

Contents

Incident Update

Last month we said that the New Year had begun with a bang, it is not getting quieter, with the appearance of the Slammer Worm on 25 January, read more about this below.

W32/Igloo-15 was reported on 13 February, the latest in the long tradition of viruses using the promise of star's pictures to encourage users to launch them. This promised pictures of Catherine Zeta-Jones.

W32/Lovgate.B (also called W32/Lovgate.C) got press coverage on 24 February, but also seems to have been over-hyped.

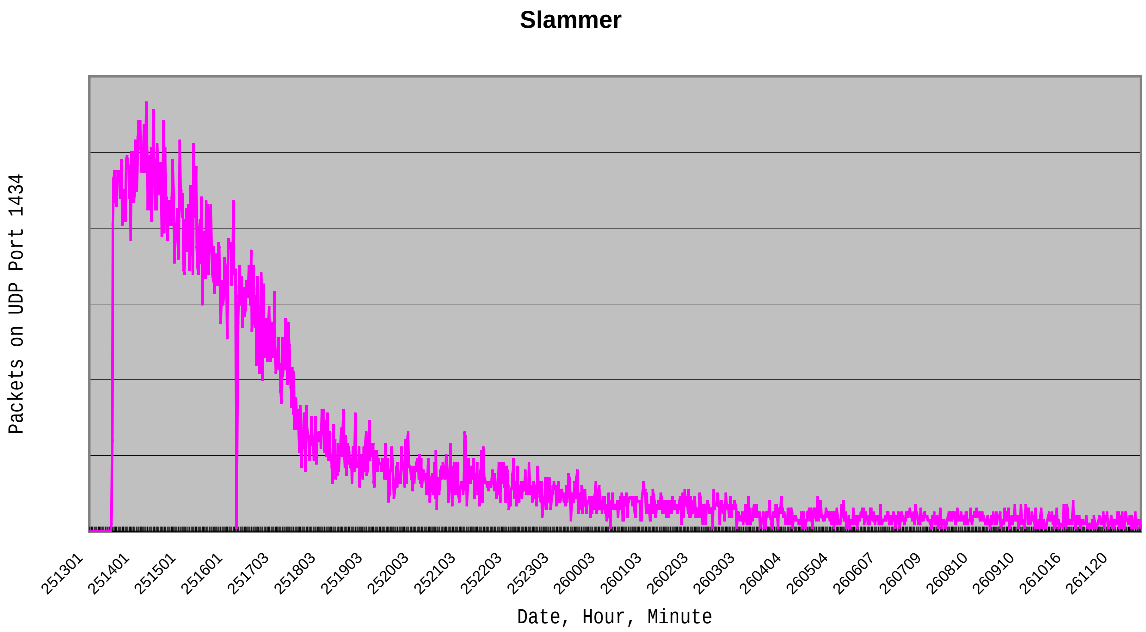
W32/Klez.H-mm remains the most prevalent virus in MessageLabs' statistics.

Thoughts About Slammer

The Slammer worm (also called W32/SQLSlam-A, W32/SQLSlammer, W32.SQLExp.Worm, DDOS_SQLP1434.A, and Sapphire) hit the Internet about 13:30 Hong Kong time on 25th January 2003. Within three minutes it had infected most vulnerable hosts on the Internet. It attacks Microsoft SQL servers, infecting them by sending a specially-crafted packet to UDP port 1434. The graph shows the Slammer packets stopped at Yui Kee's firewall.

The rapid rise seen in the graph is interesting. Last year, a theoretical paper "How to 0wn the Internet in Your Spare Time" described the Warhol Worm - a worm capable of attacking most vulnerable hosts on the Internet in under 15 minutes by utilising a "hit list" of vulnerable hosts with good connections. Slammer achieved the same in less than three minutes by being small and efficient. The choice of a single UDP packet was particularly interesting - this eliminated the latency involved with creating a TCP connection.

Slammer basically did nothing but spread, so the damage was the consumption of bandwidth and CPU time. The SQL servers that were infected essentially stopped being database servers until they were rebooted and patched. Many Internet users saw a slowdown, and some sites lost



contact with the Internet for several hours. This mainly affected sites with an infected SQL server, but some sites with no Microsoft SQL servers were also affected. This appears to be because their ISP's router also served one or more infected sites, and was unable to cope.

Another interesting feature is the fall in the graph. Code Red and Nimda stayed with us for months, but Slammer was 90% gone by the end of the day. Partly, this was because it utilised all available bandwidth on the infected machines - if you are using a database for something important, and it stops working, you take action immediately. In contrast, Code Red did not take all the bandwidth, and it infected Microsoft's webserver, which many people used because it was there, and which is installed by default in some circumstances. However, it seems the ISPs should take the main credit: some companies did not fix their servers until after the weekend, but many ISPs took action and disconnected the infected sites, allowing the rest of the Internet to resume working. This is not unreserved praise; the confused reaction of some ISPs revealed their staff were poorly-equipped to react to an incident.

Slammer was also easy to deal with because it used an unusual protocol - almost no normal traffic uses UDP port 1434, so a simple filter blocks it with no side-effects. It also makes it easy to identify infected hosts from the traffic.

What lessons should we learn from Slammer?

- Defence in depth. Do not expose systems on the Internet unnecessarily. There are very few (no?) reasons why you need a SQL server accessible to the world.
- Apply security patches. The patch for the vulnerability that Slammer utilised was available last year from Microsoft.
- Warhol Worms are no longer "just theoretical". There will be more; they may be even faster (although that does not matter much - 3 minutes is already too fast for a human to analyse and decide on a response).
- You need good neighbours. The availability of your connection depends on the security of networks "close" to you.
- Good incident response at ISPs can make a big difference.

Further information:
Warhol Worm: http://www.icir.org/vern/papers/cdc-usenix-sec02/index.html
Flash Worm: http://www.silicondefense.com/flash/

http://www.caida.org/analysis/security/sapphire/
http://vmyths.com/rant.cfm?id=560&page=4
http://news.com.com/2100-1001-982955.html
http://www.theregister.co.uk/content/56/29139.html

HKCERT Seminar

Hongkong CERT is planning a seminar titled, "Incident Response on the Hostile Network", keep an eye on their website for details.

Sisyphus was a Systems Administrator

In Greek legend, Sisyphus was renowned for his cunning but his disrespect got him into trouble, he was condemned for eternity to push a heavy rock to the top of a hill, where it would always roll down again. Systems administrators may recognise themselves as they try to keep up with the stream of critical security patches. Commentators are quick to blame them when there are outbreaks because old patches have not been installed. System administrators even blamed each other for Slammer's spread in a Sophos poll.

However, it is apparent that Microsoft was badly hit by Slammer because they had many unpatched systems. If Microsoft can't keep their own systems up-to-date, who else can?

Almost two years ago, Bruce Schneier wrote an article, "The Security Patch Treadmill" pointing out the limitations of patches and advocating monitoring to improve security. This does not mean that you can forget patching, defence in depth is the key.

Further information:
http://www.counterpane.com./crypto-gram-0103.html#1
http://www.sophos.com/virusinfo/articles/slammerpoll.html
http://www.theregister.co.uk/content/56/29073.html

Remote Update from Sophos streamlines anti-virus protection for remote workers

No more headaches for network administrators responsible for remote work force. Sophos Anti-Virus has announced Remote Update, a new application that easily updates remote computers with the latest virus protection and upgrades of Sophos Anti-Virus software.

Designed to integrate with the Sophos Enterprise Manager suite, Remote Update lets IT managers perform hassle-free updates of the latest anti-virus protection on all their remote computers, such as laptops and desktops outside the network.

Historically, network administrators have had difficulty ensuring the security of remote computers used by employees, leaving the corporate network vulnerable to infection. Remote Update ensures that all computers, regardless of whether they are permanently connected to the company network or not, are still protected against the very latest virus threats.

"With the number of viruses in the wild increasing every day, organisations need to take proactive steps to protect themselves," said Brian Burke, senior research analyst of Internet security software at IDC. "Telecommuters and 'road warriors' are one of the most vulnerable points in an organisation's security network, and administrators have had a traditionally difficult time enforcing strict security measures. Sophos's Remote Update application combats one of the biggest security concerns of this vulnerable population."

Remote Update installs Sophos Anti-Virus on company computers outside the network, monitors for new virus protection, and updates as required. It ensures that employees working from home or on the road are able to remotely access a central installation directory on their company's website or network via the internet, their wide area networks (WANs) or their local area networks (LANs).

Remote Update can be configured to limit the amount of bandwidth it uses to ensure that other applications are not hindered by virus updates. To keep bandwidth requirements to a minimum, Sophos virus protection updates are typically only 1-2 KB in size, while the monthly product update or upgrade is as small as 250 KB. This compares favourably to rival products, which are typically 50-100 times larger. Sophos already has a number of customers taking advantage of this product, including Provident, the international financial services group specialising in personal credit and motor insurance.

"At Provident, we have around 700 remote users, spread across the entire country. With up to 800 new viruses being discovered each month, keeping these remote users up to date with their virus protection is a priority," said David Hopkins, network systems support analyst at Provident. "Sophos's Remote Update makes updating those working from home or on the road a breeze - allowing us to remain confident that all our computers are running the very latest virus protection."

Keeping systems up to date with the most recent virus protection updates is a key to an effective anti-virus solution. Remote Update transforms what could be a tedious or even difficult task into a straightforward procedure.

As an integral part of Sophos's award-winning Enterprise Manager suite, Remote Update is designed to reduce administrative overheads and ensure that the level of anti-virus protection is consistent throughout the entire organisation.

Secure Computing 2003 Awards

Vote for you favourite security products in Secure Computing Magazine's annual awards:

http://www.westcoast.com/events/awards/voting/index.html

Stupid Security Competition

Another method of expressing your opinion about security, although completely unrelated to the one above:

http://www.privacyinternational.org/activities/stupidsecurity/

F-Secure Takes Linux Security to a New Level

A new email gateway solution for ISPs and IT departments launched together with new Linux based security management solutions.

F-Secure's product portfolio for Linux covers both virus protection and data encryption. These products are optimised for protecting both standalone Linux computers as well as Linux servers and gateways, and to help remotely manage both Windows- and Linux -machines. This portfolio is now expanded with 3 new products: F-Secure Anti-Virus for Firewalls 6.10, F-Secure Anti-Virus for Linux Servers 4.50 and F-Secure Policy Manager for Linux. These new products will introduce superior virus detection for Linux servers and email gateways as well as true cross-platform management capability.

Linux has become one of the central building blocks in our global network infrastructure. Lack of security at this level would not only put the backbone itself in jeopardy, but also leave a majority of the end-users' computers vulnerable to attacks. F-Secure's Linux-products ensure that this backbone can be operated safely and prevent viruses from propagating through it. "We have already seen several fast-spreading worms that use Linux servers to replicate. The Slapper-incident is just one example," says Mr. Mikko Hypponen, the Manager of Antivirus

Research at F-Secure. "The only reliable way to fight this kind of threat is to implement security in the network itself", he continues.

F-Secure Anti-Virus for Firewalls 6.10 enables the customer to use pure Linux/Unix solutions at the gateway level. This product provides the same features as the Windows-version, thus enabling the customer to scan traffic that goes through the firewall. The product is especially important in environments where the critical gateways are based on Unix/Linux to reduce downtime and improve scalability. With multiple scanning engines this product provides reliable protection against all known types of viruses, including macro, script and binary viruses.

F-Secure Anti-Virus for Linux Servers 4.50 provides a new architecture that is optimised for mail scanning and other similar tasks. The product provides a new powerful interface that is optimal for integration in systems like AMaViS that check contents for viruses. The interface allows the user to easily schedule tasks like virus scans and definition file updates. This product is, like the F-Secure Anti-Virus for Firewalls, based on the same industry leading scanning technology as the other products in the F-Secure Anti-Virus family. It uses the same update files and provides the equally high detection rate. One of the most significant new features in F-Secure Anti-Virus for Linux Servers 4.50 is the daemon mode. This mode enables the user to load the scanning engines into memory permanently. A small lightweight module can attach to this daemon and start scanning tasks. This unique architecture ensures extremely fast scanning performance with quick and easy integration to any solution that might want to launch an anti-virus check.

F-Secure Policy Manager is the centralized policy management tool for the entire F-Secure product range. This tool has been available for Windows already for several years, but is now available for Linux as well. The new Linux-version introduces both a console- and sever-component for Linux.

These components are fully compatible with the versions for Windows and mixed systems are supported. The most common installation scenario is a set-up where several Linux servers running F-Secure Policy Manager Server are distributed through an enterprise network. Windows workstations connect to these servers and the administrator can use the Linux- or Windows-based F-Secure Policy Manager Console to manage the system. The benefits are obvious in organizations that use Linux as their server platform. The F-Secure Policy Manager 5.11 for Linux is available for download at:

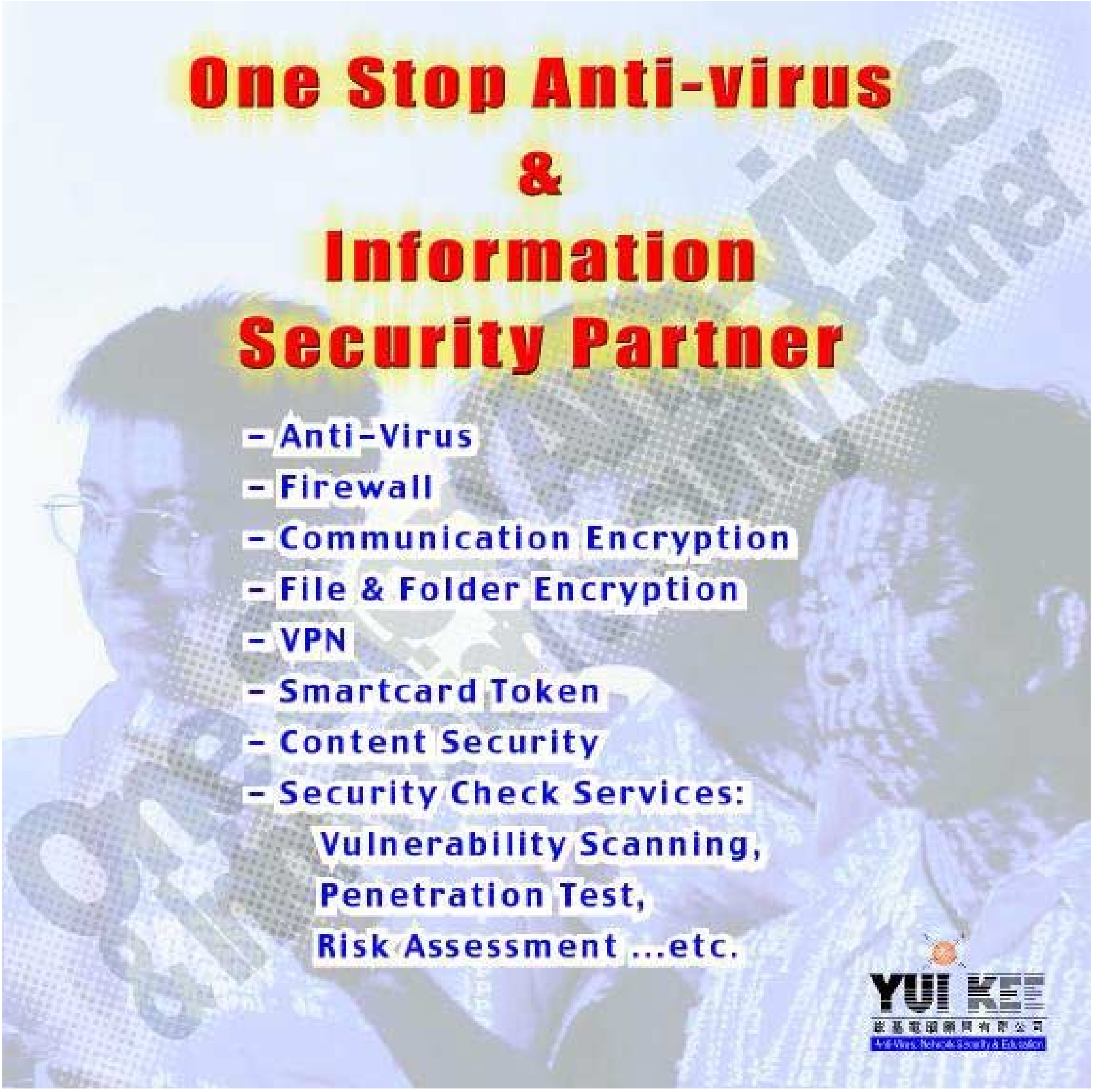
http://www.f-secure.com/products/policy-man/linux/

Are Small Businesses Protecting Themselves Properly?

A survey by Sophos of over 4500 system administrators around the world has discovered many small businesses are not updating their anti-virus software often enough or deploying protection at the email gateway. Don't be caught out - find out more about the survey's findings and how Sophos can help you protect your business.

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

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
銳基電腦網絡有限公司
Anti-Virus, Network Security & Education