Yui Kee Computing Ltd.

Newsletter

September 2004

Contents

Incident Update

Wed Sep 1 05:16:28 2004 Norman: Bagle.AK Medium

Wed Sep 1 06:16:30 2004 Trend Micro: WORM_BAGLE.AI Medium

Wed Sep 15 04:02:13 2004 Trend Micro: MS04-028_JPEG_GDI High

Thu Sep 16 00:16:18 2004 VMyths: JPEG virus (speculation & hysteria, September 2004)

Thu Sep 16 16:16:33 2004 Norman: Netsky.B Medium

Symantec and the Great Firewall Bypass

Symantec has changed its decision to detect Freegate a Trojan. Dynamic Internet Technologies (DIT) produces the Freegate software. DIT provides, "low cost, reliable solutions for customized Internet service needs under challenging environments". Notably, this includes dynamic proxy technology to bypass web-filtering software, such as that used by the Chinese Government. DIT has strong links with the USA Government, collaborating on projects and testifying before the U.S.- China Economic and Security Review Commission

Symantec, which has headquarters in the USA, released definitions for its Norton Anti-Virus product that detected Freegate as a Trojan about 14 September. However, by 16 September, they reversed the decision, releasing a statement, "A number of our customers drew our attention to what they deemed the suspicious nature of the Freegate software. Upon investigation by our researchers, similarities were noted between how the software operated and how various Trojan horses operated, based on the use of open proxies to penetrate firewalls used to block web sites. As a result, it was deemed a cyber threat and blocked by our software. Since that time, further investigation indicates that Freegate is in fact not a Trojan horse and detection for this program has therefore been removed from Symantec's virus definitions."

The speed at which detection was removed seems to indicate this was a genuine mistake, despite the political overtones. However, it could still cost Symantec sales, as there has been considerable negative commentary concerning big corporations supporting Government censorship.

More information:

http://www.theregister.com/2004/09/16/symantec_relabels_freegate/
http://www.dit-inc.us/news.htm
http://www.theregister.co.uk/2004/09/14/symantec_targets_freegate/
http://209.157.64.200/focus/f-news/1215867/posts

F-Secure Focuses on Anti-Virus, not Encryption

F-Secure and WRQ Inc. have entered into a strategic partnership, where WRQ will become the global exclusive distributor of F-Secure's SSH products. This exclusive agreement further enables F-Secure to focus on its core Anti-Virus and Intrusion Prevention business.

Established in 1981, WRQ develops software for accessing and integrating legacy applications. The company has over six million users worldwide, including four out of five Fortune 500 companies. WRQ takes over the sales of new license and maintenance agreements starting October 1st. WRQ will take over the technical support services during fall 2004.

"Through this agreement we can focus on our key strength areas to further develop our approach to a broader concept of content security and intrusion prevention", says Risto Siilasmaa, President and CEO of F-Secure Corporation.

More information:

http://www.f-secure.com/products/fsssh/f-secure-wrq-faq.shtml

SSH Communications Security Pursues Mission

SSH's mission is to enable its customers' secure business operations and data communications. In 1995, Tatu Ylönen invented the SSH protocol, which became an Internet standard. In December of the same year, he started SSH Communications Security to make SSH solutions commercially available. In March of 1996, the SSH Secure Shell product family was licensed to F-Secure (called, at that time, Data Fellows).

Since then, SSH Communications Security has gone from strength to strength, improving its SSH-based products and its business. It is still committed to securing its' customer's business operations and data communications through changing times.

If you are a current user of the SSH protocol who needs continued support from experts, or if you want to see how SSH can enhance your operation, please contact us: kason@yuikee.com.hk

Council of Europe Promotes Cybercrime Convention

The Council of Europe is holding a three-day conference to encourage more countries, both inside and outside Europe, to sign its Cybercrime Convention, which is the first international treaty to address electronic crimes. The treaty is controversial: on the one hand, computer crime is overtaking more traditional criminal activities. In Germany, for example, computer crime was just 1.3% of recorded crime, but it accounted for 57% of the financial damages arising from crime.

However, critics point out that the treaty expands law enforcement authority, and has insufficient safeguards. It will allow countries to exchange information without regard to data protection, for example.

Eight countries have ratified the treaty so far, which came into force in July 2004.

More information:

http://www.theregister.com/2004/09/17/euro_cybercrime_conference/
http://www.epic.org/privacy/intl/ccc.html
http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm
http://www.iptablog.org/2004/03/19/cybercrime_convention_commences.html

New Linux-based High-Speed Perimeter Protection

F-Secure has unveiled a new Linux-product for high speed virus and content scanning at the corporate network perimeter. F-Secure Internet Gatekeeper for Linux provides comprehensive Internet gateway protection: it scans SMTP, HTTP and FTP traffic for viruses, worms and trojans as well as blocks and filters out specified file types. Also ActiveX and Java code can be scanned or blocked. Furthermore it is able to scan POP3 streams to prevent virus attacks through personal Internet email accounts, or from ISP-hosted email. The product automatically and securely receives updates from F-Secure, always keeping the virus protection up to date. A powerful and easy to use web-based management console simplifies the installation and configuration of the product.

Viruses and malicious code can enter the network of an organization from multiple directions. Though email has been known to be the most common way of spreading viruses, today many web sites are also filled with programs including harmful and malicious content. "End users may download various files from the Internet, for example games, screensavers, music, applications, etc. What the users don't realize is that these files might actually be or include viruses and other harmful content. Therefore, it is very important for organizations to implement web traffic virus and content scanning already at the perimeter of the network", says Mikko Hyppönen, Director of F-Secure Anti-Virus Research Lab. Performance is also a key factor when choosing a solution for gateway level security. In throughput and scanning performance, F-Secure Internet Gatekeeper for Linux sets the bar for others to follow.

F-Secure Internet Gatekeeper for Linux is designed to run on different Linux platforms and provides industry leading throughput, reliability and security. Thanks to its flexible product architecture F-Secure Internet Gatekeeper for Linux is a suitable solution for any organization, small or large.

More information:

http://www.europe.f-secure.com/products/anti-virus/gw/index.shtml

Bank Discloses Credit Card Customers Details

HFC, a UK subsidiary of HSBC, inadvertently sent 2,600 credit card customers a message with the entire distribution list in the outgoing mail. Even worse, "vacation" bounces were also distributed to the whole list, revealing, in many cases, names, phone numbers and holiday dates.

More Information:

http://www.theregister.com/2004/09/27/e-bank_email_blunder/
http://64.233.179.104/search?q=cache:m6qq9jbJjXwJ:news.ft.com/cms/s/d7af7b16-0e8f-11d9-97d3-00000e2511c8.html+hfc+%22operator+error%22&hl=en
http://64.233.179.104/search?q=cache:u9X5KCdz6IwJ:news.ft.com/cms/s/90acf920-0e60-11d9-97d3-00000e2511c8.html+hfc+%22operator+error%22&hl=en

Rouge Diallers Bring Down IDD

In an effort to crackdown on auto-dialler programs, Ireland will block IDD calls to 13 countries. Auto-diallers change Internet users' dial-up settings to connect to premium-rate and International access numbers, sometimes without making the charges involved clear, or without requesting permission at all. Ireland's phone regulator, the Commission for Communications Regulation (ComReg), has received complaints from over 300 victims of such scams this year, and it defends the action of blocking calls to the Cook Islands, Comoros, Diego Garcia, Kiribati, Mauritania, Norfolk Island, Nauru, Sao Tome and Principe, the Solomon Islands, Tuvalu, Tokelau, Wallis and Futuna, and French Polynesia as "necessary to provide consumers with the protection they need".

Representatives of some of the countries affected are planning to lobby the Irish Government in Dublin, but ComReg says it is compiling a list of "legitimate" phone numbers that will not be blocked.

More information:

http://www.theregister.com/2004/09/22/ireland_rogue_dialler_crackdown/
http://www.theregister.com/2004/09/26/ireland_rogue_diallers/
http://www.sophos.com/virusinfo/articles/irelandban.html

Virus Writer Charged, Becomes Celebrity, Gets Job

Sven Jaschan, the German teenager arrested for the Netsky and Sasser worms has been formally charged with causing damages of US$157,000 to four specimen victims: three German city Governments and a broadcaster that were disrupted by the Sasser worm. If he is tried in a regular court, he may be sentenced with up to 5 years in prison, however, he was under 18 at the time of the offences, so he may be tried in a juvenile court and be sentenced accordingly.

Jaschan has also become something of a celebrity; the popular German magazine Stern has interviewed him, a recent version of Mydoom contained his photograph, and a website to solicit donations for him was started (though that seems to have collapsed due to incompetence). Following the Stern interview, Securepoint, a German security software developer, made him a job offer. Lutz Hausmann, the technical director at Securepoint, said, "He is a young kid, who did bad things but I think he deserves a second chance."

Yui Kee's Technical Director, Allan Dyer, commented, "The most damaging effect is that Jaschan is becoming a hero to the 'computer underground', encouraging other young people to do the same, to become famous. It is useful to understand the motivations of virus writers, and reformed criminals should be able to get a rewarding job, once their debt to Society is paid, but Jaschan is a self-confessed criminal, awaiting trial. Stern and Securepoint appear to be motivated by the publicity opportunity, without regard for the wider good of Society."

More information:

http://www.theregister.com/2004/09/08/sasser_charges/
http://www.sophos.com/virusinfo/articles/jaschanjob.html
http://www.sophos.com/virusinfo/articles/netskyhero.html
http://news.bbc.co.uk/2/hi/technology/3677774.stm
http://news.com.com/Security+firm+looks+to+hire+alleged+Sasser+author/2100-7349_3-5374636.html?tag=nefd.top
http://www.pcmech.com/show/influence/393/
http://www.forbes.com/technology/feeds/ap/2004/09/08/ap1534275.html
http://www.xatrix.org/article.php?s=3667
http://www.blawgchannel.com/2004/07/sven_jaschan_a_.html

http://p2pnet.net/story/1461
http://www.boredguru.com/modules/news/article.php?storyid=633
http://news.zdnet.co.uk/internet/security/0,39020375,39167171,00.htm

Centralised Security Status Monitoring with F-Secure Policy Manager

F-Secure Policy Manager 5.60 features new web based tool for centralised security status monitoring

The new release comes with a graphical reporting tool, F-Secure Web Reporting that allows an IT administrator to view the security status in the company network with a standard web browser. The administrator can easily monitor the network by generating extensive reports on the security status. One example of the reports is a trend line of network attack activity against corporate workstations over the past month.

"One important aspect for virus protection and intrusion prevention is to provide on-line reports of the security status in the network. If a new fast-spreading virus breaks out, the IT administrator is not always at the office to check the protection level. F-Secure Policy Manager 5.60 with Web Reporting is a perfect tool to provide peace of mind by offering remote access to this information with a standard web browser", says Topi Hautanen, Product Marketing Manager at F-Secure.

F-Secure Policy Manager 5.60 is available for Windows and Linux platforms in the English, German and French languages. F-Secure Policy Manager 5.60 is available immediately and it supports all F-Secure Antivirus corporate solutions.

Web Reporting Screenshots:

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

F-Secure Spam Filtering Solution

F-Secure has introduced a new, easy to use, automatic spam filtering solution for corporate customers. F-Secure Spam Control transparently and automatically detects and filters annoying and offensive spam messages from email traffic, and frees time for productive work in organizations.

F-Secure Spam Control can be installed as an option to F-Secure's email content scanning solutions that already today provide virus detection and removal capabilities to organizations around the world with world-leading response times to new threats. Working alongside F-Secure's virus scanning engines, F-Secure Spam Control engine detects spam automatically using advanced content analysis and categorization. Messages that are found to be spam by F-Secure Spam Control are marked at the gateway level so that they can later be placed to specific spam folders in the user's mail client. The end users remain in control of the messages and have the ability to retrieve and view spam tagged messages if needed. High accuracy spam detection rates are achieved and maintained by scanning email using advanced content analysis, combining multiple filtering mechanisms and updating the product with frequent automatic updates from the F-Secure Anti-Spam Lab.

"Our aim was to make a solution that is easy to install, use and maintain, and that would integrate tightly with our existing products making it a complete email security solution for our corporate customers. The feedback we have received from our early beta customers indicates that we have succeeded in our objective", says Ari Alakiuttu, the Business Channel Director at F-Secure.

The City of Malmö in Sweden has been using an early version of F-Secure Spam Control in conjunction with their existing F-Secure Internet Gatekeeper product. "We are very happy with the results we have achieved together with F-Secure", says Patrik Flensburg, responsible for the IT operations at the City of Malmö. "The F-Secure Spam Control provided low TCO, was easy to take into use and it detects spam reliably and with good accuracy" adds Mr. Flensburg.

F-Secure Spam Control can be purchased as an as an add-on to the F-Secure Internet Gatekeeper and F-Secure Anti-Virus for Microsoft Exchange products. Customers wishing to evaluate F-Secure Spam Control together with either the F-Secure Internet Gatekeeper or the F-Secure Anti-Virus for Microsoft Exchange can download an evaluation version from the F-Secure Website at:

http://www.f-secure.com/download-purchase/list.shtml