Yui Kee Computing Ltd.

Newsletter

August 2003

Contents

Stop Press

There is an early report that the FBI plans to arrest an 18-year-old suspect "early on Friday" in connection with one of the Blaster variants.

http://apnews.excite.com/article/20030829/D7T7CKQ00.html
http://www.news.com.au/common/story_page/0,4057,7101567%255E1702,00.html
http://seattletimes.nwsource.com/html/businesstechnology/2001659113_blaster290.html
http://www.theinquirer.net/?article=11258

Incident Update

"It never rains but it pours", August has been a busy month for viruses and worms.

It started with a mass-mailer, W32/Mimail.A on 2 August. To fool recipients into opening the attachment it uses a social engineering trick: Mimail forges the sender's address as 'admin@<recipients domain>', and uses the subject 'your account'. Mimail achieved good initial spread and is still spreading - it is currently listed as the second most prevalent virus in MessageLabs statistics..

However, Mimail was eclipsed on the 12th of August by W32/Blaster.A, a worm that exploits the DCOM vulnerability in the RPC service in some versions of Windows. A patch to fix the vulnerability has been available from Microsoft since the 16th of July. Blaster caused widespread disruption, a lot because of its' tendency to cause Windows XP to shutdown frequently, and was reported in the Media worldwide. It is discussed in depth throughout the rest of this newsletter.

Another worm that exploits the DCOM vulnerability appeared on the 18th of August. Known as W32/Nachi.A or Welchia or Welchi, it also exploits the WebDAV vulnerability in IIS 5.0,

Microsoft issued a patch to fix the vulnerability on the 17th March this year. An interesting feature of Welchia is that it attempts to download and install the patch to fix the DCOM vulnerability from Microsoft. Welchia also searches for new hosts to infect by sending ICMP echo request ("ping") packets, some sites have found it necessary to block these packets because the flood of traffic is effectively a distributed denial of service attack.

On the 19th of August, another mass-mailer, W32/Sobig.F, started spreading. It contained a date trigger, set for 3am on 23rd August, Hong Kong time, when it would attempt to download and execute an unknown program. This is discussed further in the article, "Doomsday Countdown", below. By August 22nd, the outbreak of W32/Sobig.F had become the biggest recorded so far - MessageLabs stopped about 1.5 million infected messages, mostly carrying W32/Sobig.F that day, accounting for one in 17 of the emails they processed. Although the numbers have decreased since then, W32/Sobig.F is still the most prevalent virus in MessageLabs statistics.

Microsoft Website Blasted

The W32/Blaster worm carries a Denial of Service payload, attacking the windowsupdate.com website starting on the 16th August 2003. The payload has been extraordinarily effective before it even sent a single packet because Microsoft has announced it has withdrawn the targeted site, permanently! Sean Sundwall, a spokesman for Microsoft said: "One strategy for cushioning the blow was to extinguish Windowsupdate.com. We have no plans to ever restore that to be an active site." Microsoft users can still update their systems by visiting http://windowsupdate.microsoft.com or http://www.microsoft.com.

"(Microsoft) figured out - quite correctly - that no web server could survive under the attack load generated by tens of thousands of infected computers. So Microsoft simply disconnected this server from the web and removed its name from domain name systems," explains Mikko Hypponen, Director of Anti-Virus Research at F-Secure Corporation. "Windowsupdate.com will probably never return. So in this sense, the worm accomplished what it wanted: windowsupdate.com is no more."

The possibility that the high volume of traffic for windowsupdate.com would overload switches and routes at ISPs around the world was very real, but, because the site no longer exists, the worm will not send the traffic.

Power Blackout Prevents Worm Spread

An estimated 50 million people in New York, Detroit, Toronto and Ottawa as well as other cities were saved from spread of W32/Blaster by a massive power blackout. O.K., that is rather facetious, but there have already been unfounded rumours that Blaster caused the blackouts, so why not consider the flip side? All those PC's deprived of power were certainly not spreading Blaster. This also injects some reality into the disaster "statistics" that are often quoted for viruses and worms. We have never seen thousands of people trudging home on foot, or sleeping in the streets, because of a virus. Viruses do frequently cause disruption and sometimes damage, so we need to protect against them, but keep things in perspective.

Microsoft has not claimed responsibility for the power outage.

Blaster Worm should have been no problem

A new worm called W32/Blaster.A started spreading in the early hours of the 12th of August, Hong Kong time but Allan Dyer, Chief Consultant at the local information security company; Yui Kee Computing Ltd. says the outbreak was preventable.

Mr. Dyer described the outbreak, "During Tuesday, we received a small number of enquiries from companies that had been infected, and we blocked a far larger number of connection

attempts by the worm at our firewall." In fact, Yui Kee recorded over 37 thousand attempted attacks on their systems during Tuesday. "Obviously, there are a large number of systems on the Internet that got infected, but the administrators of those systems could have prevented it", Dyer continued.

Good information security management will have multiple lines of defence, some of the measures that would have prevented the spread of W32/Blaster.A include:

- A firewall: "Least privilege" firewall rules would have blocked the connection attempts made by the worm, preventing it from entering companies. Home users and SMEs can use personal firewalls. A default installation of F-Secure Distributed Firewall blocks the ports used by the worm.
- Updating systems: Software developers issue security patches for their products when a vulnerability is found. In this case, Microsoft issued a patch in Microsoft Security Bulletin MS03-026 on the 16th of July 2003. Fixing the vulnerability was described as "critical". Administrators have had almost a month to apply the patch.
- Tracking the information security news for important alerts. Yui Kee first notified the users of its' YKAlert service about the vulnerability announcement on the 17th July (Hong Kong time). They were alerted again on the 1st of August when CERT/CC advised that the vulnerability was being exploited. YKAlert users were alerted about the outbreak of W32/Blaster.A on 12th August at 07:05, before it had become widespread and in sufficient time to take emergency action.

Dyer sent a stern warning to malware writers, "This is not about blaming the victim, the responsibility for this disruption clearly lies with the criminal who wrote and released this worm. He or she should face a court for this crime, just like Simon Vallor." Simon Vallor was jailed in the UK earlier this year for two years after being convicted of writing and releasig three viruses, known as Redesi, Gokar and Admirer. "However, prudent computer users and administrators will pay attention to safety and security, just like we do in the real world whenever we handle money, cross the road, or take another risk."

Testing Your Firewall

If you want to check that your firewall or personal firewall is blocking W32/Blaster and W32/Welchia, browse to this URL: https://grc.com/x/portprobe=135

It will send a test to the port, and report the result. Note that, if you use a proxy server, it will report on the status of the proxy server, not your machine, because that is the apparent source of the request.

Microsoft Tool to Scan for DCOM RPC vulnerability

Microsoft has released a KB 823980 Scanning Tool (KB823980scan.exe) that can be used to scan networks to identify computers that do not have the 823980 security patch (MS03-026) installed.

For information on the scanning tool, please refer to:

http://support.microsoft.com/default.aspx?kbid=826369

Laptops sneak round Firewalls

Some organisations that thought they had protected against W32/Blaster got a nasty surprise when roaming laptops brought the worm in, bypassing their firewalls. When the Blaster outbreak began, some organisations wisely checked that their firewall was blocking the ports it uses, but then made the mistake of becoming complacent and delaying the patching of

computers inside - why hurry, they thought, when the firewall stops Blaster getting in? A rude awakening was in store: an unprotected laptop can be infected when it is outside, and "sneakernet" carries the laptop with worm into the office. Complacency is replaced by frantic activity to control the internal outbreak.

"Don't forget about the laptops when you are sorting out your computer security," reminds Graham Cluley, senior technology consultant at Sophos Anti-Virus. "It is because they are not always connected to the network that administrators need to be extra vigilant about making laptops as impenetrable to viruses as possible."

Sophos Remote Update provides an easy way for remote workers (such as laptop users or employees based at their homes) to be kept up-to-date with their virus protection. Remote Update keeps Sophos Anti-Virus up to date on an end-user's computer via a website or network connection provided by their employer. It is ideally suited to employees of organisations who are infrequently, or never, connected to the main company network, but who do connect to the internet from time to time.

F-Secure Distributed Firewall is a good way for Admins to extend the protection of their firewall rules to roaming computers. By using F-Secure Distributed Firewall you can safely access Internet from any place, whether it is home, office, airport or hotel. F-Secure Distributed Firewall is a software-based firewall product that offers complete protection against Internet threats. It extends your corporate security outside the corporate premises. It closes the door to hackers and eliminates new vulnerabilities.

Graybird Trojan and Dumaru Virus disguised as Blaster Fix

On the 15th of August, a backdoor Trojan, known as Troj/Graybird.A, was widely distributed in messages that claimed it was an update to fix the vulnerability used by Blaster. Of course, users who believed the message and executed the attachment did not fix the DCOM vulnerability, but opened a backdoor into their computer for attackers.

W32/Dumaru.A, which appeared on the 19th of August, sends itself in emails purporting to be from security@microsoft.com. It claims to be a patch for Internet Explorer, and warns, "There are dangerous virus in the Internet". If executed, it installs a backdoor that connects to an IRC server and awaits further commands.

It seems likely that the authors of the Graybird Trojan and the Dumaru virus saw the panic caused by Blaster's spread as the perfect opportunity to trick users into installing their backdoors. Users should always be suspicious of unsolicited attachments, even if they arrive from apparently trustworthy sources.

Additional Information:

http://www.sophos.com/virusinfo/articles/graybird.html
http://www.sophos.com/virusinfo/analyses/trojgraybirda.html
http://www.f-secure.com/v-descs/dumaro.shtml
http://www.sophos.com/virusinfo/analyses/w32dumarua.html

Fools Rush In: W32/Welchia a Practical Demonstration in Stupidity

Every so often, someone suggests using a virus for a good purpose: killing other viruses or fixing security holes, but the anti-virus developers do not use this "brilliant" idea. W32/Welchia, which started spreading on the 18th of August, demonstrates why not.

W32/Welchia, also known as W32/Nachi-A, is apparently designed to clean up the W32/Blaster worm that started spreading last week, and install the fix to the vulnerability Blaster used to infect computers. Welchia searches for computers by sending ping packets and then uses the same vulnerability as Blaster to try to infect the target. Once installed, it checks the version of the operating system and downloads and installs an appropriate patch from Microsoft. It even cleans itself up - if the date is 1 January 2004 or later, it deletes itself.

This all sounds harmless enough, but Welchia is currently causing more disruption at many sites than Blaster did. Allan Dyer, Chief Consultant for Yui Kee Computing Ltd. commented, "The 'cure' is worse than the disease. We do not need mysterious, unknown, unqualified people attempting to usurp legitimate systems administrators."

The problems are:

i) Thousands of infected machines are all searching for more victims using ping packets, causing network congestion and even Denial of Service conditions at some sites.

ii) To complete the installation of the patch, the worm reboots the machine, causing an unexpected service interruption.

iii) Although the worm appears benign, it has come from an untrusted source and may contain a hidden backdoor.

Dyer said, "There have been several previous viruses that attempted something similar, but I think this has spread the most and caused more disruption."

Anti-virus and information security professionals have known about the dangers of using a virus to install patches for a long time, in August 2000 the well-known cryptographer, Bruce Schneier, said, "Viruses, by their very nature, spread in a chaotic and unchecked manner; good system administration is anything but."

Dyer gave his opinion, "The owner of a computer system should be responsible for making sure it runs properly and, if that computer is connected to the Internet, they should make sure it does not cause disruption for other users. Companies will probably delegate that responsibility to their Systems Administrators, home users might get assistance from their software vendor but we do not need vigilante viruses usurping that responsibility."

Doomsday Countdown

The spread of W32/Sobig.F started a race against time for anti-virus and information security organisations. The analysis of the mass-mailing virus revealed that it contains an encrypted list of IP addresses within its' code, tese are "master servers". If the time is between 19:00 and 22:00 GMT on any Friday or Sunday Sobig.F sends a notification to the master servers, and waits for one of them to send a URL. It then downloads from the URL, and executes the content. The first activation of this routine would take place at 19:00 GMT on Friday, 22 August 2003 (3am Saturday, Hong Kong time). The master servers on the list were well spread out, under the administration of different ISP's. In all likelihood, they were the machines of innocent users that had been broken into taken over by the virus writer.

So thousands, possibly hundreds of thousands, of machines infected with Sobig.F were ready to download and execute an unknown program (or programs). If the virus author only made the download locations available at the last moment, security experts would have no chance to analyse it before it started work. The program could do anything, up to and including wiping the victim's hard disk. More likely scenarios would be launching Distributed Denial of Service attacks and acting as relays for spam.

Passively waiting for the attacks to happen was not an option, so organisations around the world, including CERTs, the FBI and anti-virus developers, co-operated in tracing and

contacting the administrators of the "master servers" to get them shut down. Sophos and F-Secure participated in the effort. The race was close at the finish, the timeline for 22 August was:

13:00 GMT 11 master servers disconnected

16:00 GMT 18 master servers unavailable

17:00 GMT 17 master servers unavailable - apparently one that was previously unreachable was started by it's owner.

18:20 GMT 19 unavailable. It was feared that the remaining master server would still be enough for the attack to start.

19:00 GMT The final master server was still connected to the Internet, but did not respond to the virus requests. It remained dormant for the whole 3 hour attack period.

So, the attack failed, this time. Sobig.F is programmed to stop working after the 10th of September 2003 and this appears to be part of a plan by the author. Four of the earlier versions of Sobig also had expiry dates, and shortly after one expired a new variant was released. We can anticipate a new Sobig variant appearing in mid-September.

The Changing Virus Writer?

A persistent myth has grown up that virus writers are all teenage males with no girlfriends doing a high-tech version of vandalism. The myth has survived and even grown stronger, despite the studies of Sarah Gordon (see The Generic Virus Writer and The Generic Virus Writer II) and mounting evidence to the contrary. Unfortunately, the myth distracts attention from an alarming development in virus writing: a trend towards organised crime.

Some anti-virus experts reinforce the myth, for example, Graham Cluley, senior technology consultant for Sophos Anti-Virus said, "Vallor's website reveals he pretty much fits the profile of a typical virus writer - he is young, techie and preoccupied with female nudity," about a virus writer convicted earlier this year. However, the profile has almost no utility - 'techie' is a pre-requisite for anything involving programming, which leaves 'young' and 'preoccupied with female nudity', well it may be news to Mr. Cluley, but approximately 50% of young adults are preoccupied with female nudity. Vallor's website leaves an impression of a 'party animal' pretty much indistinguishable from many others you might bump in to in a crowded bar on a Saturday night. The profile does nothing to help us identify potential virus writers, or narrow down a search, but it is a nice soundbite that panders to the preoccupation with sex of the Media, and the Public they serve.

The myth might even be reinforced when it is being contradicted, for example, in describing the Sobig virus, F-Secure uses the phrase; "quite obvious it’s not written by a typical teenage virus writer". Here the teenage stereotype is the accepted fact, and Sobig is apparently a rare and unusual exception.

What about the 'teenage' stereotype? Notwithstanding the 18 year old suspect connected to Blaster (see Stop Press, above), identified virus writers are usually older.Here's a list of the virus writers, and their ages, who created some of the most prolific viruses in recent years (the majority have been convicted for their crimes): Jan de Wit: 20; Simon Vallor: 21; Chen Ing-Hau: 24; Onel de Guzman: 25; Christopher Pile: 26; David L Smith: 30. Not a teenager in sight, and Mr Smith sounds positively geriatric to a typical teenager - though older commentators would probably characterise them all as 'young adults'.

There are other hints that virus writers do not fit a stereotype - the recent Welchia worm contains the text, "I love my wife & baby :)", maybe still 'young adult', but nothing like Vallor's 'party animal', more probably 'family man'. Welchia is also designed to install a security patch

from Microsoft, probably *intended* as a benevolent act. This is not to condone Welchia, it is still a stupid idea to try to 'fix' a security problem without authorisation, using a worm.

Other recent malware shows deliberate planning: To date we have seen six variants of Sobig, and five have been released with a pre-programmed expiry date. The variants have different capabilities. There is an agenda behind the scheduled releases, and we do not know what it is. So far, some Sobig variants have been used to create open relays heavily used by spammers.

The virus Dumaru and the Trojan Graybird also show planning - they were released in messages designed to take advantage of the panic about Blaster, but developing a new program takes time. Therefore, the person or people behind them probably prepared the malware in advance, and waited for a suitable event before releasing them. Both installed backdoors on the compromised computers, again the potential for spamming is a possible motive.

Of course, unsolicited email is not a crime in most places, but a large proportion of the spam cluttering up our inboxes does show intent for dishonest gain. This may be the confidence trick - the infamous Nigerian 419 scam that offers fabulous rewards for some money laundering or other shady business, but where the victim is drawn into paying more and more up-front fees; or it may be offers of cheap software (often anti-virus software) that turn out to be pirated, or simply false marketing claims - to reduce bodyweight, or increase it in certain, specialised areas. The willingness of these spammers to use open relays without authorisation, and even to deliberately break into computers in order to create new open relays clearly demonstrates their lack of respect for others' computing resources and the law.

Computer viruses and other malware are no longer just reckless acts by irresponsible amateurs, Sobig, Dumaru and Graybird show forward planning and probable intent for dishonest gain. Mikko Hypponen, Director of Anti-Virus Research at F-Secure already has an opinion on who is behind Sobig, “Looks like organized crime to me”, he commented. Virus writers were never a cohesive group that could be easily stereotyped, but now there is opportunity for real financial gain we can expert a lot more trouble ahead.

Additional Information:

http://www.commandsoftware.com/virus/generic.html
http://researchweb.watson.ibm.com/antivirus/SciPapers/Gordon/GVWII.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