Yui Kee Computing Ltd.

Newsletter

August 2004

Contents

Incident Update

There has been the usual confusion over variant names, but Bagle and Mydoom have caused the most notable incidents in the last month.

9th August

Symantec: W32.Beagle.AO@mm
http://www.sarc.com/avcenter/venc/data/w32.beagle.ao@mm.html

Norman: W32/Bagle.AI@mm
http://www.norman.com/Virus/Virus_descriptions/16605/en

Sophos: W32/Bagle-AQ
http://www.sophos.com/virusinfo/analyses/w32bagleaq.html

F-Secure: Bagle.AL http://www.f-secure.com/v-descs/bagle_al.shtml

Trend Micro: WORM_BAGLE.AC
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.AC

Network Associates: W32/Bagle.aq@MM
http://vil.nai.com/vil/content/v_127423.htm

16th August

Trend Micro: WORM_RATOS.A
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_RATOS.A

W32/Mydoom.S@MM:

F-Secure: Mydoom.S http://www.f-secure.com/v-descs/mydoom_s.shtml

Sophos: http://www.sophos.com/virusinfo/analyses/w32mydooms.html
http://www.sophos.com/virusinfo/articles/mydooms.html

Network Associates http://vil.nai.com/vil/content/v_127616.htm

Norman: http://www.norman.com/Virus/Virus_descriptions/16785/en

W32.Mydoom.Q@mm

Symantec: http://www.sarc.com/avcenter/venc/data/w32.mydoom.q@mm.html

Writer Arrested, but the Worms Live On

Although it has been three months since Sven Jaschan, the author of the Netsky worms, was arrested, the worms keep spreading. No new variants have been released but the existing ones are still haunting the wild.

According to MessageLabs statistics, W32/NetSky.P-mm has remained in first place and W32/Netsky.Z-mm in second or third place for many months. Many other variants have occasionally made it into MessageLabs Top Ten Virus Threats during July and August:

W32/NetSky.B-mm:	10th July, 15th July, 30th July, 2nd August, 13th August, 16th August, 26th August, 30th August (8 times)
W32/NetSky.C-mm:	7th July, 10th July, 19th July, 26th July, 26th August (5 times)
W32/NetSky.D-mm:	3rd July, 6th July, 7th July, 9th July, 31st July, 2nd August, 11th August, 16th August, 17th August, 24th August (10 times)
W32/NetSky.K-mm:	26th July
W32/NetSky.Q-mm:	13th August, 19th August, 30th August (3 times)
W32/NetSky.S-mm:	17th July
W32/NetSky.AB-mm:	7th July, 21st July (2 times)

F-Secure also reports that Netsky variants are persistent and prevalent.

It is painful for network administrators to handle complaints from users who keep on receiving either emails containing NetSky variants or rejection emails from other email gateways that are incorrectly bouncing the infected messages to the forged sender's address. The volume of these wrongly directed warnings is even rivalling the spam clogging our in boxes.

Some advocate that email anti-virus gateways should not warn the sender when a virus is detected, but this contravenes the SMTP standard, and makes email even less reliable than now. Messages can simply disappear, with no clue as to their fate.

To combat the problem, email anti-virus gateways should be modified to return a rejection error code at the end of the DATA phase when they detect a virus, instead of generating a new message that gets sent to the (possibly forged) envelope sender address. Thus, the sending SMTP client is clearly informed that the message has not been accepted for delivery before the connection is closed.

While the Netsky variants and other similar mass-mailing worms are still in the wild, the headache continues.

References:

http://www.messagelabs.com/viruseye/threats/
http://www.f-secure.com/weblog/archives/archive-072004.html#00000232

Arrests and Prosecutions

Jeffrey Parson

Minnesota teenager Jeffrey Lee Parson, 19, pleaded guilty in a Seattle court on 11th August to damaging computers used by the US Government with a variant of the Blaster worm. He is expected to receive a sentence of between 18 months and 3 years.

Parson was not the brains behind the original Blaster worm, which caused much more damage than his "B" variant. He simply modified the original, including, rather stupidly, instructing it to contact his personal website, www.t33kid.com, which allowed the FBI and Secret Service to track him down quickly.

Microsoft's US$250,000 reward for information leading to the arrest of the author of the Blaster.A worm remains unclaimed.

More information:

http://www.sophos.com/virusinfo/articles/parsonguilty.html
http://www.f-secure.com/weblog/archives/archive-082004.html - 00000260

Microsoft Makes a Good Decision

Microsoft's decision to introduce security features that will break many old applications with XP SP2 has been praised by the information security community. XP SP2 is a major security upgrade for Windows XP, and some of the fixes will be incompatible with existing applications, especially ones that were 'sloppily' written.

Microsoft has a knowledgebase article listing about 40 of the over 200 programs known to be affected, and how to workaround the problems.

Understandably, Microsoft's explanation of SP2 contains a lot of "spin" - they can hardly say, "We've been screwing up security for years, this will improve things, but it is going to hurt." Instead, SP2 will provide a "Better user experience". The "Guiding Principles" for SP2 are:

- Secure by Design
- Secure by Default
- Secure by Deployment

These are excellent principles; it might have been better to make them rules, not just guides. Overall, SP2 is a great improvement and big step on Microsoft's path to becoming security-focussed. But it is only one step, and already a security flaw in SP2 has been reported.

More information:

http://www.informationweek.com/story/showArticle.jhtml?articleID=23902063
http://www.eweek.com/article2/0,1759,1624994,00.asp
http://support.microsoft.com/default.aspx?kbid=842242
http://www.theregister.com/2004/08/20/sp2_scripting_vuln/
http://secunia.com/advisories/12321
http://www.theregister.com/2004/08/20/sp2_scripting_vuln/

Linux: Look to your Laurels

Allan Dyer

While Microsoft users are waiting for XP2 to download, Linux users, administrators and developers should stop laughing and check that they are not falling behind in security. Probably in largest contributing factor to the poor level of security in Microsoft products was "user friendliness" - installing everything, and enabling everything, just in case it might be wanted later. Unfortunately, the developers of some Linux distributions are going the same route.

A recent incident illustrates this: a website in Hong Kong was defaced by hackers, but a little examination showed that the organisation's main website was not affected. Instead, the hackers had modified a webpage on a Linux mailgateway. Someone had done a default installation, and not removed the unnecessary services, leaving the system open to attack.

Systems are not secure because one operating system is magically superior to another. Security depends on the people involved in development, administration and using the systems being security-conscious, and always acting to improve security.

Windows XP SP2 and Your Anti-Virus Software

Windows XP SP2 is a major security upgrade, so it can be expected that there will be some effect on security software that is already installed. Anti-virus developers are providing information for their customers:

Sophos: http://www.sophos.com/support/knowledgebase/article/1732.html
F-Secure: http://www.f-secure.com/products/news/prod-news_2004-08-09.shtml

Hong Kong's Top IT Story

Hong Kong was the location of a recent story in The Register. What did the UK's online high-tech news ("Sci/Tech News for the World") think was so significant in HK? Was it the Cyberport? The use of HK-designed processors in PDA's? The exciting race for the IT Functional Constituency seat?

It was a crime story. How the HK Police lead the region against hi-tech crime? Software piracy (again)? Illegal online gambling? Getting close, it was… the smashing of the cricket gambling ring. Um, OK, it is good to know we are keeping a hi-tech reputation.

http://www.theregister.com/2004/08/16/cricket_fighting_ring/

Dilbert and Security

http://www.comics.com/comics/dilbert/archive/dilbert-20040801.html

Wireless Security

Your local wireless network, or your "Personal Area Network" may not be so local or personal after all. Two devices demonstrated at the "DEFCON" conference in Las Vegas radically increase the range of Bluetooth and WLAN connections.

The "BlueSniper rifle" is a high-gain, directional antenna for BlueTooth which has been successfully connected to a Nokia 6310i phone at a distance of 1.1 miles.

The Sniper Yagi has a claimed range of 15km for wireless networks.

More information:

http://www.wired.com/news/privacy/0,1848,64463,00.html
http://www.f-secure.com/weblog/archives/archive-082004.html - 00000247

First AMD 64-bit Virus

The first known virus written in AMD64 assembly code has been named W64.Shruggle.1318. It is a direct-action infector that targets AMD64 Windows Portable Executable (PE) files and is unlikely to spread in the wild.

More information:

http://securityresponse.symantec.com/avcenter/venc/data/w64.shruggle.1318.html
http://www.theregister.com/2004/08/26/virus64bit_redux/

Know Your Enemy

Sven Jaschan, the author of the Netsky and Sasser worms, has been interviewed in Stern magazine. The interview gives an impression of a young man typical of young virus writers who are caught: a certain naivety, a bungled attempt to use a virus to fight a virus, an inability to understand the far-reaching consequences of releasing self-replicating code. In the interview, Sven also alleges that his siblings and many of his classmates knew what he was doing, and even encouraged and helped him. This shows the need to include information security in the school curriculum, starting when children first touch a keyboard.

Of course, this tells us nothing about the virus writers who do not get caught.

More information:

http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5501940.html?tag=adss
http://www.stern.de/computer-technik/internet/?id=525454 (in German)
http://www.sophos.com/virusinfo/articles/netskyhero.html

F-Secure Opens San Jose Anti-Virus Research Lab

New Lab To Further Improve Award-Winning Response Times

San Jose, Calif., August 30, 2004 - F-Secure® Corporation (HEX: FSC), a worldwide leader in antivirus and intrusion prevention software, announced today that it has opened an anti-virus research lab in San Jose, California. The lab will share 24-hour anti-virus research responsibilities with F-Secure's other award-winning anti-virus research labs.

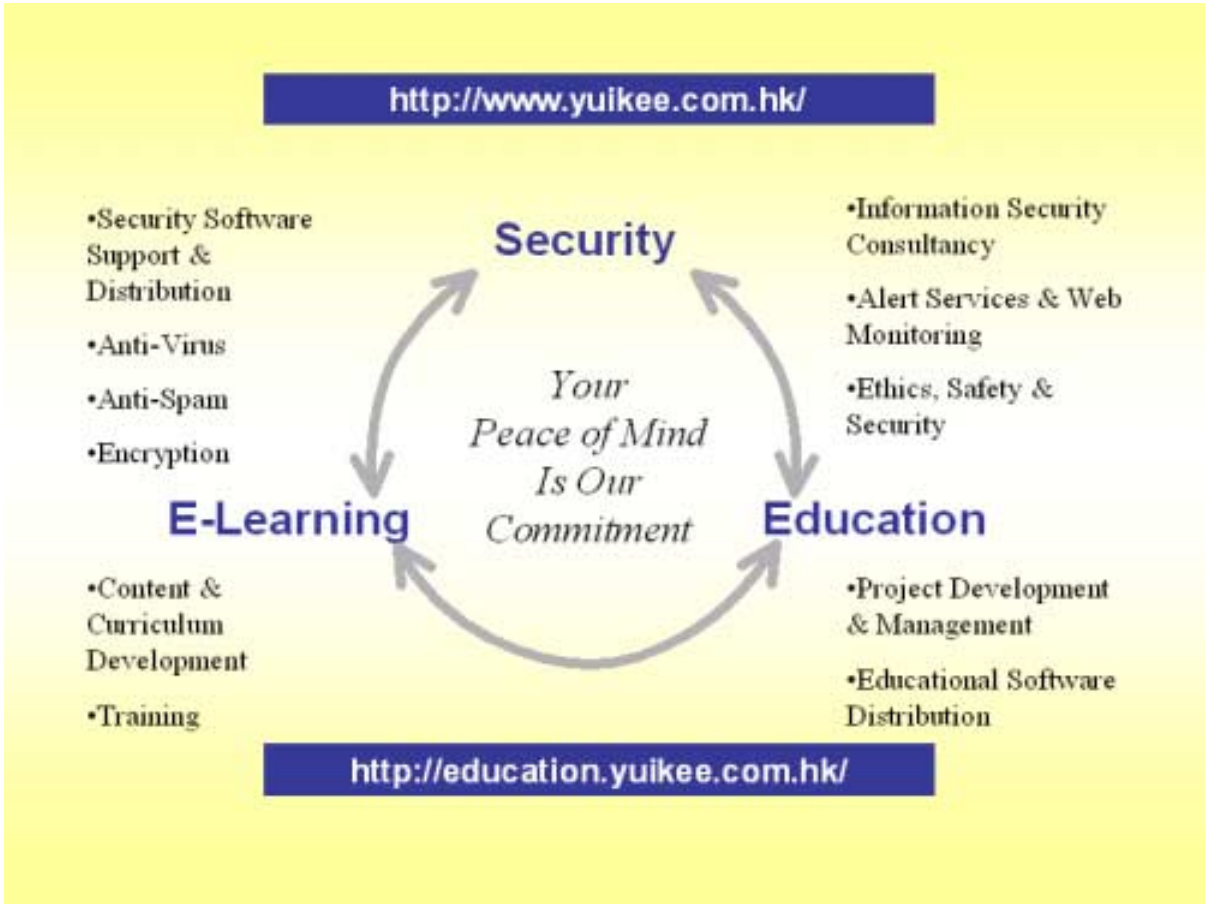
Tzvetan Chaliavski from Bulgaria and Ero Carrera from Spain will staff the San Jose research lab. Chaliavski comes to F-Secure from the Command Antivirus/Authentium team in Florida, and Carrera is moving to San Jose from F-Secure's Finland office.

Both cybersecurity professionals are recognized experts in the antivirus community. Tzvetan "Ceco" Chaliavski has worked in the anti-virus industry for more than ten years, and started in the Bulgarian National Laboratory of Computer Virology. Ero Carrera is credited with cracking the Mydoom virus, the largest e-mail outbreak ever, in less than two hours in January 2004.

"The virus writers have been extremely active lately, so we want to have our best researchers always available," said Mikko Hypponen, global director of antivirus research at F-Secure. "When Europe sleeps, USA works and vice versa. All of our researchers focus on global security threats, not just local situations."

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

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/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/