Yui Kee Computing Ltd.

Newsletter

July 2004

Contents

Incident Update

Larger incidents this month included new versions of Bagle and Mydoom:

2004/07/20 WORM_BAGLE.AH or W32/Bagle.AI@MM

http://vil.nai.com/vil/content/v_126798.htm

http://www.sophos.com/virusinfo/analyses/w32bagleai.html

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.AH

2004/07/27 W32.Mydoom.M@mm

http://www.hkcert.org/valert/vinfo/w32.mydoom.m@mm.html
http://www.cert.org/current/current_activity.html - w32/mydoom
http://www.sarc.com/avcenter/venc/data/w32.mydoom.m@mm.html
http://www.sophos.com/virusinfo/analyses/w32mydoomo.html
http://www.f-secure.com/v-descs/mydoom_m.shtml

Microsoft Releases Unscheduled Critical Update

Microsoft's "second Tuesday of the month" patch cycle is in tatters with the release of Microsoft Security Bulletin MS04-025 on the 30th of July. The patch addresses the critical vulnerability exploited by JS.Scob.Trojan (alias Download.Ject) that was discovered in June. It is recommended that the patch is installed as soon as possible.

System Administrators can rest assured that Microsoft will continue to adhere to their update schedule, except when they don't.

More information:

http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx

http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx
http://www.theregister.com/2004/07/30/ie_scob_fix_imminent/
http://www.f-secure.com/v-descs/scob.shtml
http://www.microsoft.com/security/incident/download_ject.mspx

Arrests and Prosecutions

Microsoft vs. Khoshnood

Microsoft's vigorous prosecution of major, high profile spammers is proceeding well, with a recent case awarding a US$3.95M judgement against Daniel Khoshnood of California. Mr. Khoshnood used a spam campaign to trick users into running a toolbar that was supposed to download patches from "Windowsupdatenow.com". Instead, it displayed popup advertisements. Judge Manuel Real ruled that Mr. Khoshnood had violated Microsoft's trademark.

Previously, in the 1990's, Mr. Khoshnood cybersquatted domain names such as Presidentclinton.com, and Microsoft-networks.com.

This is one of 60 cases Microsoft has initiated against spammers since the beginning of 2003, and it reports that it has won six cases and received judgements totalling US$54M, pushing two spammers into bankruptcy.

More information:

http://www.theregister.com/2004/07/16/ms_spam_case_win/

Netherlands vs. 419ers

Highlighting the difficulty of proving electronic crimes, a Dutch court ruled that there was insufficient evidence linking 52 suspects individually to evidence of advanced fee fraud found in raids by Dutch police in January. The suspects and the evidence were found in the same locations. However, as none of the computers were actually in use, indeed, they were not switched on, at the time of the raids, there was nothing to show *who* had been using the computers to commit the crimes. The evidence included an ironing board with a list of names of fake companies and directors.

http://www.theregister.com/2004/07/16/amsterdam_419_charges/

Spain vs. Cabronator Author

Oscar Lopez Hinarejos received a two-year jail sentence for creating the Cabronator Trojan. The Trojan allowed an attacker to take control of the machine, collect personal data, and use the machine in DDoS attacks. Hinarejos, aged 26, was arrested in April 2003 and is the first person to be jailed for writing malware in Spain.

More information:

http://www.square.nl/en/00001/news/00099/
http://www.theregister.co.uk/2004/07/05/spanish_vxer_jailed/
http://bot.hellsparty.com/article?id=15

Sophos Customer Satisfaction Survey

From now till 13 August, Sophos is conducting an online customer satisfaction survey. All the respondents will have a chance to win an **Apple iPod**!

Sign up for the survey now. http://www.sophos.com/survey/

First Virus for Pocket PC

The first virus to infect Pocket PC executables has been named WinCE.Duts.1520. Obviously a proof-of-concept virus, it would not be viable in the wild, as it asks for permission to spread. It was created by the 29A virus-writing group.

More information:

http://www.f-secure.com/v-descs/dtus.shtml

Council Leaks Personal Data for 2 Years

Badly addressed emails intended for the auditor controller's office of the Contra-Costa County, California ended up at a Swedish Internet company that owned a .ac domain. The stray emails included personal data, such names, employee numbers, and benefits of workers. Some had payroll spreadsheets as attachments. The Director of the Swedish company, Robert Carlesten, tried reporting the problem, but the County only became aware after Carlesten told Computerworld.

Some reports claimed that anti-spam filters blocked Carlesten's messages, because he was not an authorised sender. The County immediately blocked outgoing email to the entire .ac domain as a preventative measure. It is suspected that the cause is bad addresses in some address books, but many employees have personal, locally-stored address books, making identification and correction of the rouge addresses a problem.

There are various lessons to be learnt:

- Things that fail silently can go unnoticed for a long time. Warning signs may never be reported ("Joe in audit never gets my reports…").
- Simple spam filters can have serious false positive problems.
- Encrypting sensitive internal communications could have prevented this accidental leakage.
- Blocking an entire top-level domain is over-reaction to an addressing error.

More information:

http://www.pcworld.com/resource/printable/article/0,aid,116808,00.asp
http://www.the-inquirer.com/?article=17094

Twisted Chinese naming on common viruses and worms

Patrick Lee

The May issue of Virus Bulletin highlights the lack of a 'universal naming and identification convention that's really nice' for viruses ("Hunting the UNICORN", VB May 2004, p.13-16) but the situation in Chinese is even worse. The names are often poorly translated and have a meaning totally unrelated to the original. Examples of the twisted Chinese naming include:

Novarg: from Norway to SCO?

The infamous Novarg (or MyDoom) worm first appeared in 27th January 2004. Rising named Worm.Novarg as “SCO 炸彈”, which means “SCO bomb” presumably because the first and second variants of the MyDoom worm launched DDoS attacks on SCO’s web site. Rising still uses this Chinese name for all MyDoom variants. The most recent one, Worm.Novarg.n in 27th July 2004, is still referred to as “SCO 炸彈”, even though the DDoS target is no longer SCO.

Jiangmin transliterated Novarg as “挪威客”, which means “Norwegian guest”. Well, I have no idea why the worm is related to a Scandinavian country.

References:

http://it.rising.com.cn/newSite/Channels/Anti_Virus/Virus_Alert/Virus_New/200401/27-084313734.htm
http://it.rising.com.cn/newSite/Channels/Anti_Virus/Virus_Alert/Virus_New/200403/04-192614289.htm
http://www.jiangmin.com/exec/news_sys/news/jiangmin/virusinfo/newvirus/2004127212656.htm

Bagle: an eaglet or a bad eagle?

Variants of another infamous worm, Bagle (or Beagle) were spreading again recently. This worm is so bad that Rising decided to translate W32.Beagle.K@mm as “惡鷹”, which means “bad eagle”. Why they don’t translate it as “bad beagle”, that’s another issue.

Jiangmin also chose the same theme, and named W32.Beagle.AB@mm as “雛鷹”, which means “eaglet”. This has a certain logic, as the worm uses an executable named bbeagle.exe, so if "bb" is taken as an abbreviation for baby, the whole name becomes baby eagle.

References:

http://it.rising.com.cn/newSite/Channels/Anti_Virus/Virus_Alert/Virus_New/200403/04-192614290.htm
http://www.jiangmin.com/exec/news_sys/news/jiangmin/index/important/2004716165055.htm

Does it matter?

Why bother about Chinese naming irregularities, when the International names are also in confusion? In most cases, the International names are similar across many developers, and they follow the CARO naming convention. Apart from defining a structure for the names, the convention recommends avoiding the names of people and companies. Using the name of an innocent company for a virus that has no direct connection is not appropriate, and, as the target of an attack can be changed without changing the structure of a virus, forward-thinking naming will never use such a name. The International names are also just that, International - by using the lowest common denominator, the ASCII character set, they can be displayed on any computer, which Chinese character names cannot. Viruses do not respect national boundaries, so erecting additional barriers to communication, by having names that are non-transferable, can only hamper the fight against viruses.

Sophos Names Virus Arch-Villain

A report published by Sophos has revealed that 70% of virus activity in the first half of 2004 can be linked to a German teenager. Sven Jaschan, 18, is the self-confessed author of the Netsky and Sasser worms which hit internet users hard in the first six months of the year.

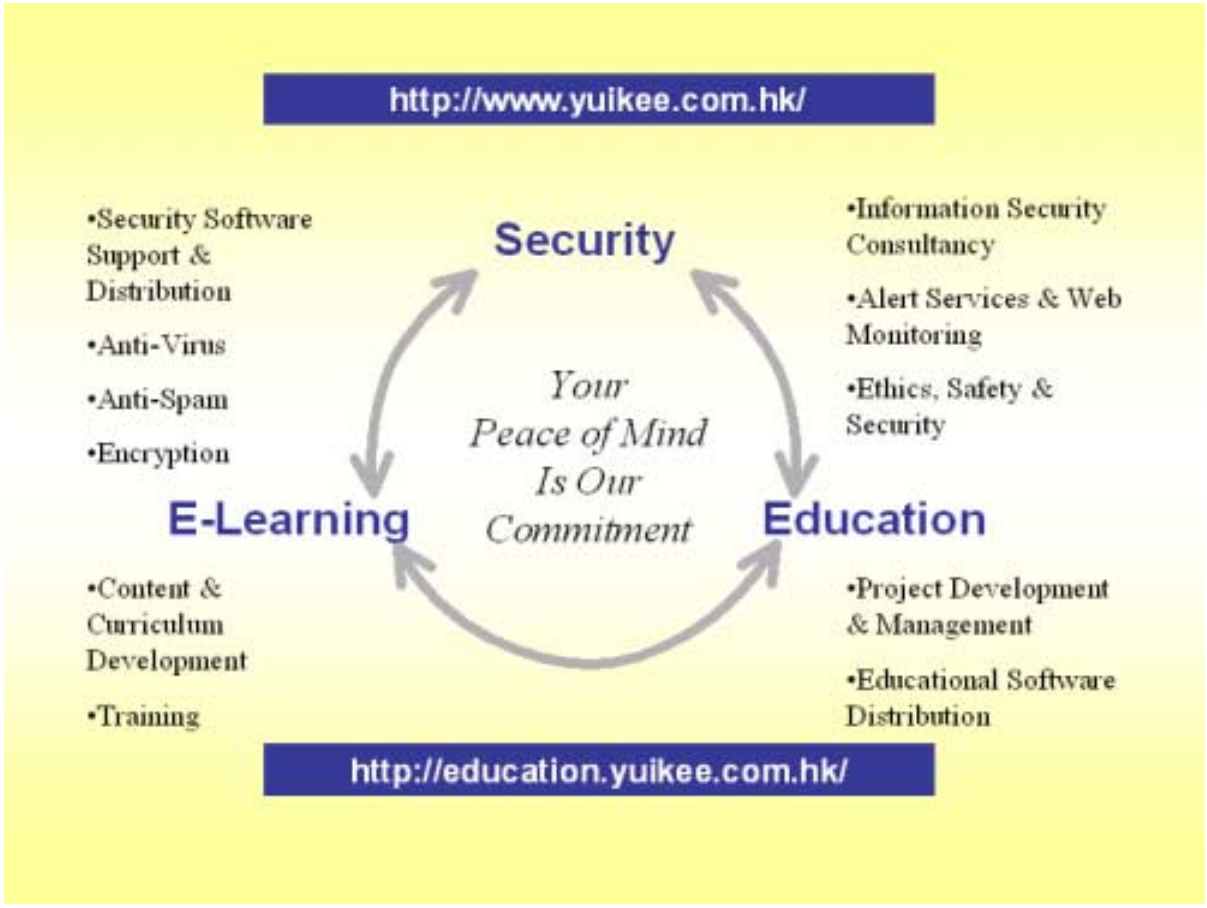
Just two of Jaschan's viruses, the infamous Sasser worm and Netsky-P, account for almost 50% of all virus activity seen by Sophos up until the end of June. Counting Jaschan's other released variants of the Netsky worm, the total figure accounts for over 70%.

Full Report:

http://www.sophos.com/pressoffice/pressrel/uk/20040728topten.html
http://www.sophos.com/virusinfo/articles/oneman.html

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/