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

Yui Kee Computing Ltd.

Newsletter

January - March 2004

Contents

Visit us at 14-17 April ICT Expo – Booth 5K23

(HK Convention and Exhibition Centre)

Have you been bothered by Email forging viruses, empty emails that came from addresses that you know, spams and other Security hassles? Let’s meet up and check out solutions that we have selected to recommend to you.

Incident Update

The lull in December and early January has been replaced by an accelerating parade of Mydoom, Bagle and Netsky variants.

19 Jan W32/Bagle.A@MM (details from: NAI, Trend Micro, Symantec, Norman)

27 Jan W32/Mydoom.A (details from: NAI, Symantec, Norman, CA, Sophos, F-Secure)

10 Feb W32/Doomjuice.A (details from: Trend Micro, NAI, F-Secure, Sophos)

14 Feb W32/Welchia.B (details from: Symantec)

16 Feb W32/Mydoom.E (details from: Sophos, Trend Micro)

16 Feb W32/Netsky.A@MM (details from: NAI, Trend Micro, Symantec)

17 Feb W32/Bagle.B@MM (details from: Norman, NAI, F-Secure, Trend Micro)

18 Feb W32/Netsky.B@MM (details from: Sophos, Trend Micro, NAI, Norman, Symantec)

23 Feb W32/Mydoom.F@MM (details from: Symantec, NAI, Norman)

15 Mar W32/Bagle.O@MM (details from: Sophos, NAI, Trend Micro)

15 Mar W32/Bagle.P@MM (details from: Trend Micro, NAI)

16 Mar W32/Netsky.D (details from: Norman)

18 Mar W32/Bagle.Q@MM (details from: Sophos, NAI, Treend Micro, Norman, F-Secure)

18 Mar W32/Bagle.R@MM (details from Sophos, NAI, Symantec, Norman)

22 Mar W32/Netsky.P@MM(details from: Sophos, NAI, Trend Micro, Symantec, Norman)

26 Mar W32/Bagle.U@MM (details from: Sophos, Symantec, Trend Micro, NAI, Norman)

29 Mar W32/Netsky.Q@MM (details from: Sophos, Trend Micro, NAI, Symantec)

Doomjuice was interesting because it dropped the source code for Mydoom.A - this appears to be to make prosecution of the author of Mydoom.A difficult. Both SCO and Microsoft have offered large rewards for information leading to the conviction of the Mydoom author. Before Doomjuice, presence of the Mydoom source code on a person's computer would have been damning evidence against them - who else would have the source code? Now, if the author is ever caught, he can claim Doomjuice framed him.

Doomsayers and Inaccurate Predictions

Bagle.A was given particularly high threat ratings, but it subsequently caused relatively low damage, causing some analysts to question the threat rating systems used by analysts and developers in particular, and vendor's reactions to incidents in general:

http://www.arnnet.com.au/index.php?id=999737219&fp=2&fpid=1

http://www.theregister.co.uk/content/56/35712.html

The article in The Register singled out a vocal analyst company, mi2g, for particular criticism. The Executive Chairman of mi2g, D K Matai, was quick to respond:

http://www.theregister.co.uk/content/35/35910.html

Interestingly, D K Matai found time to send an almost identical letter that was published in the South China Morning Post, 16 March 2004, page T2.

Editors Notes: My Inaccurate Predictions

In December 2002 I made some predictions for 2003, in our first issue of 2004 it is time to evaluate their accuracy:

- "*The top virus for 2003 will still be Klez. It first appeared in October 2001, it has dominated 2002, and it shows no signs of going away. I expect it will top the monthly lists for at least seven months of the year, and still be in the top 5 next December.*"

  Wrong. Klez.H only spent three months of 2003 at no. 1, and it faded to no. 8 by December. It was remarkably persistent, but not as extreme as I predicted.

- "*There will be a small number of viruses for PDA's or other mobile devices. They will not spread well, because the numbers and connectivity of such devices is still too restricted.*"

  Wrong. Or right; if you consider zero to be "a small number". The non-existent PDA viruses certainly did not spread well.

- "*There will be an accelerating number of security flaws found and hacking attempts on Linux and Open Source software. This is because the popularity of Linux and Open Source software will continue to grow as more realise its' advantages, thus making it a more prominent target. The Open Source Community will demonstrate its' ability to effectively deal with the security flaws.*"

  Partially Right. There have been some prominent security flaws in Linux and Open Source software, but not enough to justify "an accelerating number". Those that have been found have been dealt with effectively.

- "*Email will continue to be the most common route of virus spread. I hesitate to call this a prediction, it seems so obvious, but it is really saying what will **not** happen: there will not be a new, wildly successful virus spreading method that overtakes email in 2003. The most common route of virus spread will change as the computing environment changes: mobile devices and .NET will increase in 2003, but won't become the mainstream.*"

  Right. We are still getting most of our viruses in email.

Conclusion: The future is uncertain.

SCO Controls Doom

Despite a press release where the company claimed Mydoom is "overwhelming the Internet", SCO appears in complete control of the situation. Netcraft reported that the replacement web site, www2.sco.com, was enjoying good response times. The SCO hostmaster also removed the DNS record for www.sco.com, thus preventing traffic from infected machines to the site clogging the Internet.

SCO currently controls the most powerful DDoS weapon on the Internet: potentially, they could point the DNS record for www.sco.com anywhere, and the target would be flooded from all the infected machines.

More information:

Netcraft Data: http://news.netcraft.com/archives/2004/02/01/www2scocom_enjoys_good_response_times.html

SCO Press Release: http://biz.yahoo.com/prnews/040201/nysu004_1.html

Beating Spam with SPF

Email was the original Killer App of the Internet, but it is now being choked because spammers are taking advantage of the trust assumed in the original email standards. Things have improved - open relays used to be normal, now they are configuration mistakes or, probably more likely, installed by the spammers without authorisation. The next hole to block is the forging of sender's addresses and a proposed Internet standard, the Sender Policy Framework, allows this.

The concept is simple, organisations add a DNS record specifying which IP addresses are permitted to send email for their domain, and receiving mail servers can check that the source of a message is listed. No more "Joe-Jobs". Two areas that require special care when introducing SPF are mail forwarding (including mailing lists) and travelling email senders. The Sender Rewriting Scheme is useful in this regard.

Microsoft has announced a similar, competing standard: Caller ID for E-mail, but there are no announcements for products supporting it and Microsoft claims it has patent rights on the technologies involved.

Although the IETF standards process is expected to take at least a year, you can start using SPF today; already 9450 domains are known to be publishing SPF records, including Yahoo. Yui Kee now publishes and checks SPF records. Your current mail server software might be able to check SPF records; support is already available for Postfix, Sendmail, Qmail and Exim. Sophos' Puremessage anti-spam software supports SPF.

SPF is not a magic bullet that will eliminate spam, but it is an important part of a larger solution.

More information:

SPF: http://spf.pobox.com/

Internet Draft: http://www.ietf.org/internet-drafts/draft-mengwong-spf-00.txt

SRS: http://www.anarres.org/projects/srs/

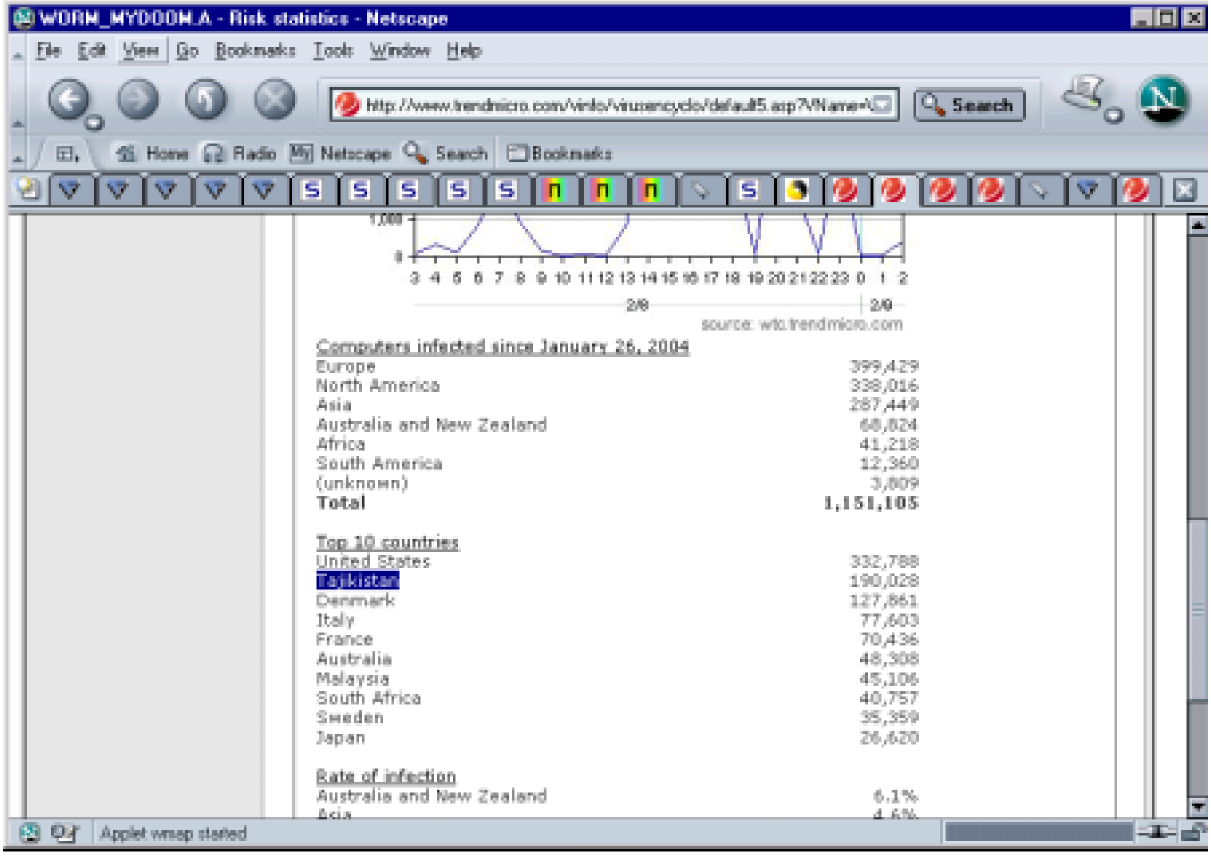
Caller ID for Email: http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx

Tajikistan Leads World in Internet Growth!

Trend Micro's statistics for the Mydoom.A virus revealed a startling fact: Internet growth in the central Asian republic of Tajikistan has exceeded 3800% during the last two years. The CIA World Factbook reports that Tajikistan, population 6.8 Million, had 5,000 Internet users in 2002, and Trend Micro's statistics place the country second only to the USA for Mydoom.A, with 190,028 infected computers.

Or perhaps Trend Micro's figures are inaccurate?

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDOOM.A&VSect=S


WORM_MYDOOM.A - Risk statistics - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=
Search
Home Radio Netscape Search Bookmarks
1,000
0
3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 0 1 2
2/8
2/9
Applet wmap started

source: wtc.trendmicro.com

Computers infected since January 26, 2004	
Europe	399,429
North America	338,016
Asia	287,449
Australia and New Zealand	68,824
Africa	41,218
South America	12,360
(unknown)	3,809
Total	**1,151,105**

Top 10 countries	
United States	332,788
Tajikistan	190,028
Denmark	127,861
Italy	77,603
France	70,436
Australia	48,308
Malaysia	45,106
South Africa	40,757
Sweden	35,359
Japan	26,620

Rate of infection	
Australia and New Zealand	6.1%
Asia	4.6%

SSH Receives FIPS 140-2 Certification

Key U.S. Government Certification Underscores Robustness of SSH Tectia(TM) Encryption

The encryption module (SSH Cryptographic Library Software Version 1.2.0) used in SSH Tectia^{TM} Client/Server 4.0 has been awarded the United States Level 1 Federal Information Processing Standards (FIPS) 140-2 certification. In addition to current availability (SSH Tectia Client/Server 4.0), the FIPS 140-2 approved cryptographic module will also be available in future releases of SSH Tectia client/server software.

The Cryptographic Module Validation (CMV) Program of the U.S. National Institute of Standards and Technology (NIST) provides specifications for software and hardware products that employ cryptographic algorithms, cryptographic key generation and distribution techniques. Authentication techniques that are FIPS 140-2 approved are certified for protecting U. S. Federal Government unclassified information. Vendor products are tested for compliance to these specifications by NIST-approved testing laboratories. In accordance with the NIST certification guidelines, the SSH cryptographic module has been certified at Level 1, which defines software cryptographic functions to be performed in a general purpose PC without any additional hardware security mechanisms.

"Protecting various agencies of the U.S. Government from unauthorized access to sensitive data has become even more critical in today's environment," said George Adams, president and CEO of SSH Communications Security, Inc. "We are delighted not only to have this all-important validation of the robustness of our encryption methodology, but also to be doing our part to help ensure that U.S. Government communications are secure."

Tests performed by the NIST validated several algorithms implemented in the crypto module used in SSH Tectia, including AES, Triple DES, DSA and SHA-1, giving it approval for use in Federal agencies within the context of a complete security program. Many U.S. Government organizations are already using SSH's Secure Shell-based technology, even before the option for FIPS 140-2 crypto module use is available. These include the U.S. Army, U.S. Navy, U.S. Marine Corps, U.S. Air Force, the Department of Defense, the Department of Justice, Lawrence Livermore National Labs, NASA, the Naval Air Warfare Center, and others.

SSH Tectia is an enterprise class suite of security solutions based on SSH's industry leading technologies. SSH Tectia client/server solution is based on the award-winning SSH Secure Shell used by millions worldwide. SSH Tectia enables end-to-end secure communications throughout the internal and external network. SSH Tectia provides transparent strong encryption and authentication and easily integrates into heterogeneous, multi-platform environments. SSH Tectia's management capabilities allow for easy scalability and centralized policy deployment.

More Information:

http://csrc.nist.gov/cryptval/140-1/1401val2003.htm

Hong Kong Considers Controlling Spam

Momentum is gathering to call for action against spam. The Hong Kong Internet Service Providers Association surveyed their members and found that about 50 % of email in Hong Kong was spam, costing an estimated $10 billion a year. Sin Chung-kai, the Legislative Councillor for IT, also conducted a survey; and found over 80 percent of people wanted government action to regulate unsolicited e-mails.

The Hong Kong Anti-Spam Coalition which includes the HKISPA, the Asia Digital Marketing Association (ADMA) and Microsoft, released a white paper on possible legislation:

http://www.asiadma.com/adma/resources/researchlist.asp

ISP Gets Tough on Zombies

A lot of current spam is sent from "zombies", computers of innocent users that have become infected with malware, and are therefore under remote control by the attackers. TeliaSonera has become the first ISP in Europe to introduce the controversial policy of cutting off "zombies" without warning.

More information:

http://www.theregister.co.uk/content/56/33763.html

Why Hack when you can Blackmail?

Blackmailers are claiming they can take control of victims' computers and delete valuable files or install pornography to get the victim into trouble. Victims or told to pay up, or else. With the high prevalence of malware, the threats sound plausible, but the blackmailers are probably sending large numbers of messages, and making a tidy sum from those who are easily intimidated.

More information:

http://www.cnn.com/2003/TECH/internet/12/29/cyber.blackmail.reut/index.html

Gigabyte Arrested

The vocal, female virus writer, known by her nickname, "Gigabyte", was arrested in her hometown, Mechelen, near Brussels. Belgium authorities also confiscated her five computers, and shut down her website. While the stereotypical virus writer is a young male, Gigabyte is a clear demonstration that women can be just as stupid as men.

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

New Sophos PureMessage provides consolidated defence against spam and viruses

Multiple-language message processing and filtering capacity ideal for large organisations

Sophos has announced the release of its consolidated anti-spam and anti-virus solution, PureMessage 4.5. Specifically designed to meet the requirements of large organisations, PureMessage combines Sophos's industry-leading virus and spam protection, filtering millions of messages per day. This unprecedented scalability, plus its multiple-language message processing, makes PureMessage ideally suited for organisations with multiple-server deployments.

In a recent Sophos poll of over 4,400 companies*, 89.4% of respondents representing large companies indicated that employers have a duty to protect their staff from unsolicited, offensive email. With a growing reliance on email, companies are increasingly finding that a scalable anti-spam solution, that is easy-to-administer, is required.

PureMessage's proprietary anti-spam technology performs

- content scanning to defend against spam messages that are disguised as legitimate email
- message analysis to look for thousands of spam indicators, such as genotype campaign analysis and structure heuristics
- asset tracking to evaluate message source and destination locations for spammer activity.

In addition, PureMessage scans all inbound and outbound email traffic at the gateway for viruses, Trojans and other malicious code.

"The spam problem is bigger than ever. Spammers are adopting new techniques, ensuring spam bypasses traditional filters." said Gary Thomassen, head of product management at Sophos. "Sophos's new PureMessage solution helps overcome these problems by delivering advanced spam protection, ideally suited for the corporate enterprise."

More information:

http://www.sophos.com/products/pm/

China is World No. 3 Spam Source

Statistics from Sophos show that China (including Hong Kong) is the third biggest source for spam, producing 6.24% of the world total. However, the U.S.A. produces more spam than the rest of the world put together!

More details:

http://www.sophos.com/spaminfo/articles/dirtydozen.html

F-Secure Mailing List Spreads Netsky.B

In an embarrassing incident, F-Secure's anti-virus mailing list was a vector for Netsky.B spread. The problem arose because the mailing list was unmoderated, and an infected computer in the U.S.A. posted to the list. F-Secure took, "immediate steps to change how messages can be sent to this list" to prevent a repetition. F-Secure is not the first anti-virus company to make a similar blunder.

More details:

http://www.theregister.co.uk/content/56/35911.html

http://www.pcmag.co.uk/News/1153081

How Safe Are Your Archives?

Many people are using CD-R as a convenient and cheap archive medium, but how long will they last, and how should they be stored? The NIST has answers:

http://www.itl.nist.gov/div895/carefordisc/disccare.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/