Yui Kee Computing Ltd.

Newsletter

June 2005

Contents

Contents 1
Incident Update 1
Symantec vs Spyware Company 1
Gartner FUDbusters 2
Panda Misses the Point, Again 2
UK Intelligence Organisation On Trail of Far-East Hi-Tech Gang 2
MessageLabs Monthly Report 3
Hong Kong Scores Another First 3
Yui Kee On TV 3
Fault Tolerance in Pakistan? 3
MyTob outbreak leads to old problems 3

Incident Update

- Tue May 3 02:32:29 2005 FSC: Sober.P reported in-the-wild 2
- Tue May 3 02:47:02 2005 SARC: W32.Sober.O@mm L3
- Tue May 3 03:02:12 2005 TREND: WORM_SOBER.S Medium
- Tue May 3 03:31:55 2005 CA: Sober.N Medium
- Tue May 3 03:31:55 2005 CA: Win32Sober.N Medium
- Tue May 3 07:47:01 2005 CA: Win32.Sober.N Medium
- Wed May 4 17:31:53 2005 FSC: Sober.P spreading widely 2
- Mon May 9 16:17:08 2005 CA: Win32.Mytob Family Medium
- Mon May 9 19:46:54 2005 TREND: WORM_MYTOB.ED Medium
- Tue May 10 10:02:10 2005 TREND: WORM_MYTOB.EG Medium
- Wed May 11 08:46:59 2005 TREND: WORM_BROPIA.V Medium
- Wed May 11 11:16:56 2005 TREND: WORM_MYTOB.EG Medium
- Wed May 11 19:46:46 2005 TREND: WORM_WURMARK.J Medium
- Mon May 16 15:46:55 2005 CA: Win32.Netsky.D Medium
- Sat May 28 05:32:08 2005 CA: Win32.Sober.N Medium
- Mon May 30 18:17:22 2005 TREND: WORM_MYTOB.AR Medium

Symantec vs Spyware Company

Symantec has filed suit against Hotbar.com Inc of New York, a marketing company that makes software that tracks web use and displays advertising. This is a pre-emptive legal strike after months of Hotbar trying to persuade Symantec to remove detection of certain Hotbar programs from Symantec's anti-virus software. Symantec is not seeking damages, but is asking for a ruling that the Hotbar programs are computer security risks.

Joy Cartun, senior director of legal affairs for Symantec, said, "Through this effort, we're trying to ensure that our customers have more control over the programs that run on their computers." Hotbar has reportedly been threatening to sue Symantec, so it seems likely they will counter-sue.

More information:

http://www.computerwire.com/industries/research/?pid=B0D6D580%2D9840%2D4816%2DB937%2DBD903AFE8126

http://www.symantec.com/press/2005/n050607.html

http://www.theregister.com/2005/06/09/symantec_hotbar_lawsuit/

Gartner FUDbusters

Hosting an IT security conference at its Stanford, Connecticut HQ, Gartner, the analyst firm targeted “the five most over-hyped threats”. According to Gartner, the five most over-hyped security threats are:

- Internet Protocol (IP) telephony is unsafe
- Mobile malware will cause widespread damage
- "Warhol Worms" will make the Internet unreliable for business traffic and virtual private networks (VPNs)
- Regulatory compliance equals security
- Wireless hot spots are unsafe

Although how the fourth can be classed as a threat is unclear.

More information:

http://www.theregister.com/2005/06/09/gartner_attacks_fud/

Panda Misses the Point, Again

Spanish celebrity-research company, Panda Software has released a ranking of the famous people most often used to spread viruses on the internet. There is no explanation of how this helps protect us against malicious software.

More information:

http://www.theregister.com/2005/06/14/celebrity_virus_chart/

http://www.vmyths.com/rant.cfm?id=549&page=4

UK Intelligence Organisation On Trail of Far-East Hi-Tech Gang

The National Infrastructure Security Co-ordination Centre, which is part of MI5 (a U.K. Intelligence organisation), has warned that a highly sophisticated high-tech gang has been trying to place bugging programs inside sensitive computer systems in a bid to steal Government and business secrets.

The gang’s *modus operandi* is highly targeted: first particular individuals in a company or organisation are identified and their email addresses are obtained. Then an email designed to appeal to their interests is sent to the victim. The message contains tailored Trojan, which installs itself without the users knowledge and them gathers and sends out information. The gang then either blackmails the person (by threatening to make them appear as a willing

accomplice in the information theft) or the company or organisation (by threatening to send the information to a competitor).

Alex Ship, a senior virus analyst with MessageLabs explained, "[The Trojans] are different every time and must put around one to two days to put together. They are very well crafted, often look as though they come from a news organisation and all of the sources indicate that they are coming from the same place in Asia."

More information:

http://www.theregister.com/2005/06/17/niscc_warning/

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

MessageLabs Monthly Report

Using data from their worldwide virus control centers, MessageLabs have produced detailed statistics about the virus and spam situation worldwide. Findings include that 7.2% of emails to Hong Kong contain a virus, and 61% of emails to Hong Kong are spam. Users of Malaysian email addresses should beware: in that country 13.1% of emails contain a virus.

Full Report:

http://www.messagelabs.com/Intelligence-MonthlyReport

Hong Kong Scores Another First

Hong Kong has ranked top in Prolexic's Zombie Report for the first quarter of 2005, with the highest number of zombies participating in large-scale DDoS attacks per capita. Hong Kong also ranked 11th in the actual number of infections per country. This is not good.

The high numbers could be attributed to the high broadband penetration but Hong Kong does not have the highest number of broadband connections per capita. We must question why there is lax security, and how can it be improved effectively and efficiently.

Full Report:

http://www.prolexic.com/zr/

Commentary:

http://blogs.hk.com/index.php?/archives/29-HK-1-in-the-world-in-Zombie-PCs-per-capita..html

Yui Kee On TV

The Radio Television Hong Kong (RTHK) interviewed our staff for a documentary about spam. The interviews are expected to be broadcast in 鏗鏘集 ("Hong Kong Connection" in English) on TVB Jade channel at HKT 7:00pm 11th July 2005 (Monday). Stay tuned.

Fault Tolerance in Pakistan?

An undersea cable has been damaged about 35Km off the Karachi coast, effectively disconnecting Pakistan from the Internet. A repair ship may take two weeks to arrive.

More information:

http://www.theregister.com/2005/06/28/pakistan_cable/

MyTob outbreak leads to old problems

The MyTob worm was first discovered in last February 2005, which was only five months ago, but this worm and its variants have already caused major anti-virus vendors to publish more

than four hundred virus alerts. That is about eighty MyTob family virus alerts per month. Trend Micro alone has published 139 such alerts, but only five of them were Medium level, the remainder being as Low level. Symantec has published almost as many, 114, with two ranked as Level 1 and the rest Level 2. Here is the summary (last updated 29th Jun 2005):

Vendor	Total Number of Alerts	First Alert Date	Last Variant Reported
Trendmicro	139	28th Feb 2005	WORM_MYTOB.HQ
Symantec	114	26th Feb 2005	W32.Mytob.GK@mm
Sophos	89	1st Mar 2005	W32/Mytob-GZ
CA	58	31st Mar 2005	Win32.Mytob.FI
McAfee	24	3rd Mar 2005	W32/Mytob.db@MM

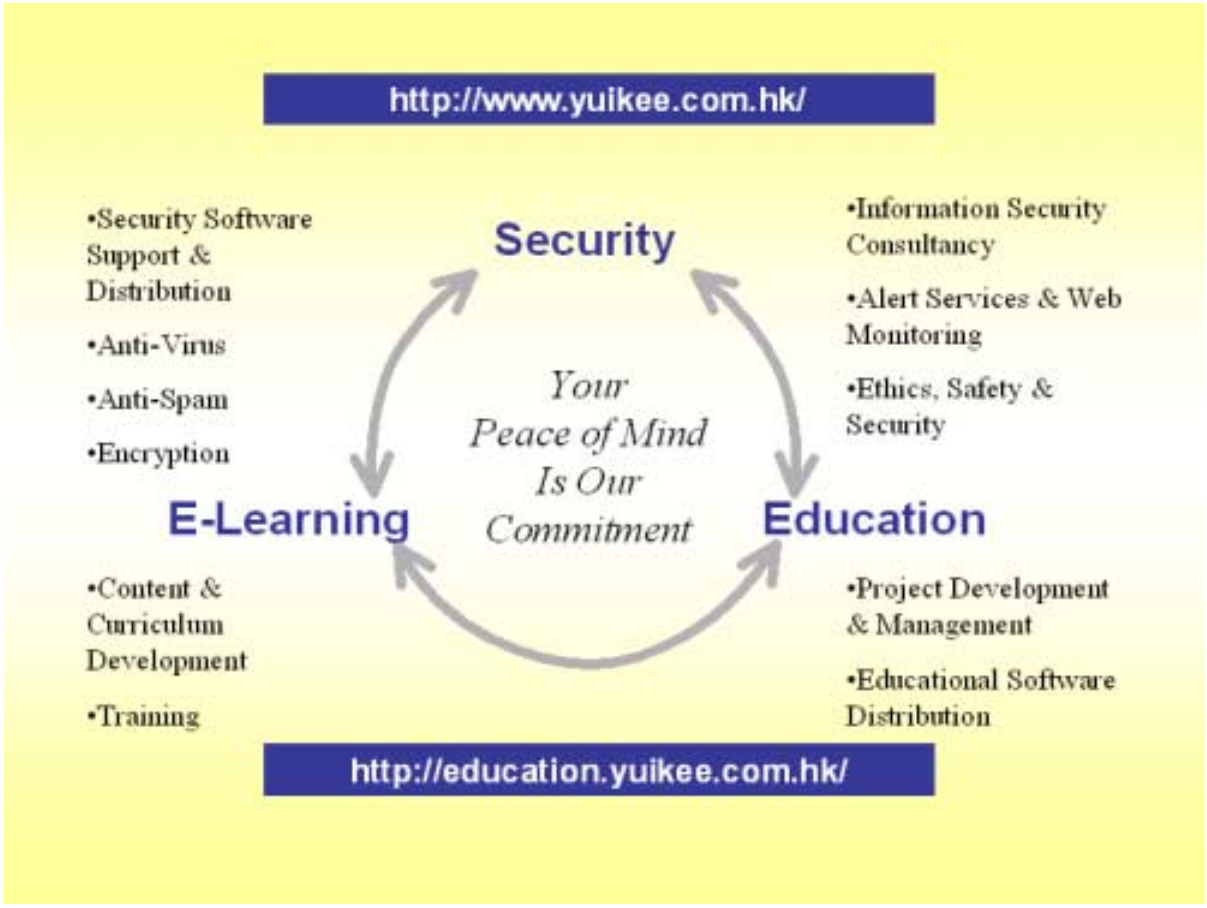
As we can see, the last variant reported by different vendors varies a lot. The last variant reported by Trend is HQ. This is the (26*8+17) = 225th variant in only five months!

The naming situation is still confusing. The relevant Trend Micro virus description page for WORM_MYTOB.HQ lists an alias W32.Mytob.EE@mm. However, the Trend Micro page for WORM_MYTOB.EP also lists the alias W32.Mytob.EE@mm. These might both be referring to the variant named EE by Symantec, which Symantec says is called WORM_MYTOB.EP by Trend Micro – or perhaps not. Do the vendors think that users are not confused enough to see so many variants and aliases? Where is the unicorn? ("Hunting the UNICORN", Virus Bulletin May 2004, p.13-16)

References:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.HQ
http://www.sarc.com/avcenter/venc/data/w32.mytob.ee@mm.html
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.EP

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/