Yui Kee Computing Ltd.

Newsletter

March 2005

Contents

Incident Update

- Tue Mar 1 12:32:23 2005 FSC: Bagle.BB spreading globally 2
- Tue Mar 1 20:02:26 2005 TREND: WORM_BAGLE.BE Medium
- Thu Mar 3 21:02:05 2005 FSC: Another Mydoom spreading 2
- Sat Mar 5 15:02:20 2005 CA: Win32.Glieder.P
- Sat Mar 5 15:02:20 2005 CA: Win32.Glieder.N
- Sat Mar 5 15:02:20 2005 CA: Win32.Glieder.O
- Mon Mar 7 19:46:47 2005 TREND: WORM_KELVIR.B Medium
- Mon Mar 7 20:17:01 2005 TREND: WORM_FATSO.A Medium
- Mon Mar 7 21:31:46 2005 TREND: WORM_SDBOT.AUK Medium
- Mon Mar 7 21:31:46 2005 NORMAN: Kelvir.B Medium
- Tue Mar 8 04:32:04 2005 TREND: WORM_SOBER.L Medium
- Wed Mar 9 15:46:47 2005 CA: Tibick.E
- Wed Mar 9 15:46:47 2005 CA: Kelvir.D
- Wed Mar 9 15:46:47 2005 CA: Sumom.A
- Wed Mar 9 18:02:15 2005 CA: Kelvir.B
- Wed Mar 9 18:02:15 2005 CA: Glieder.S
- Wed Mar 9 18:02:15 2005 CA: Sober.L
- Wed Mar 9 18:16:57 2005 CA: Mytob.C
- Wed Mar 9 18:16:57 2005 CA: Mytob.B
- Wed Mar 9 18:47:33 2005 CA: Win32.Netsky.D
- Wed Mar 9 18:47:33 2005 CA: Win32.Lovgate.AB
- Wed Mar 9 18:47:33 2005 CA: Win32.Netsky.P
- Wed Mar 9 19:02:49 2005 CA: Mytob.C
- Wed Mar 9 19:02:49 2005 CA: ForBot.MY

- Wed Mar 9 19:17:01 2005 CA: Podilk.A
- Wed Mar 9 19:17:01 2005 CA: Mytob.D
- Wed Mar 16 23:32:13 2005 SARC: W32.Beagle.AZ@mm L3
- Thu Mar 24 09:46:47 2005 CA: Win32.Mydoom.O High
- Thu Mar 24 10:17:00 2005 CA: Win32.Netsky.Z Medium
- Tue Mar 29 14:46:57 2005 CA: Win32.Netsky.C High

Editors Notes

In this issue we report on the demise of both Cyberwar and Spyware - remember, you heard it here first, and appearances can be deceptive. Also, France will have no new security vulnerabilities.

Spam Software Developer Evicted

The anti-spam organisation Spamhaus, has finally seen success in its sustained campaign to force a recalcitrant ISP to kick send-safe.com and other proxy spam gangs off its network. US telecommunications company MCI was hosting the site, but terminated their services about the beginning of March. Steve Linford, director of Spamhaus, said, "Nobody else in the West will host Send-Safe, but we still expect to be fighting its developers for years."

http://www.theregister.com/2005/03/01/send-safe_evicted/

Website Indexing Vulnerability

Your website's local search engine might be revealing more than you intend. Amit Klein has described several techniques for exposing file contents using the site search functionality.

http://www.webappsec.org/articles/022805-plain.html

Networking Spiny Water Fleas

Ecologists at the University of Windsor in Ontario, have been using network theory to work out how the Russian spiny water flea (*Bythotrephes longimanus*) will travel through Canada's lakes. The flea is a zooplankton species that entered the Great Lakes in the 1980s, and it is eating other zooplankton needed by young fish for food. The researchers, Jim Muirhead and Professor Hugh MacIsaac claim that the spread of water fleas between lakes by boats is similar to the spread of viruses by email.

The findings will allow the limited resources available to control invasive species to be targeted at points on the network where they will have most impact. Muirhead and MacIsaac conclude, “Outbound vector traffic from hubs with large flows to non-invaded destinations should be targeted for management efforts to restrict the transportation of propagules across the network and to reduce the rate at which non-indigenous species disperse to novel sites.” In other words, use a gateway scanner and threat-reduction techniques.

Perhaps similar techniques could be used to control red fire ants in Hong Kong?

http://software.silicon.com/malware/0,3800003100,39128294,00.htm

http://www.lakemichigan.org/field_guide/habitat_fishery.asp

http://athena.uwindsor.ca/units/pac/newsrel.nsf/0/5e433fe7c71a85cf85256fb6005e0e10?OpenDocument

The End of Cyberwar

The "hackers group" HUC (Honkers Union of China), which enjoyed brief publicity in 2001 over a "hacking war" with US hackers, has finally been dissolved by its founder "Lion". In an

open letter, Lion admitted that the group had existed in name only for a long time. Articles claimed that the group ranked as number 5 in the world. Who decides these rankings? Based on what data?

Fear-mongers once touted attacks by groups such as HUC as the harbingers of "Cyberwar", even though the groups were amateurs, not members of any armed forces. Now not only have the professional military failed to follow the lead of the amateurs, the amateurs have gone home too.

More information:

http://news.xinhuanet.com/english/2005-02/22/content_2603191.htm

http://www.chinanews.cn/news/2004/2005-02-18/1759.shtml

http://all.net/iwar/archive/2001Q2/0100.html

http://tech.sina.com.cn/i/c/65664.shtml

http://www.cybertelecom.org/security/cyberwar.htm

http://www.totse.com/en/politics/anarchism/162004.html

No Spyware

Eugene Kaspersky has written a thoughtful article on why the category of "Spyware" is, "basically a marketing gimmick" with no technical validity.

http://www.viruslist.com/en/weblog?weblogid=160148863

The French Emperor's New Clothes

Security researcher Guillaume Tena has been given a suspended fine of €5,000 in a French court for publishing proof of concept code to highlight security flaws in ViGuard an anti-virus product, from the company Tegam. He demonstrated that Tegam's generic anti-virus failed to stop "100 per cent of known and unknown viruses" as claimed.

French security researchers are alarmed at the effect of the case, which essentially makes publishing a security vulnerability or a proof of concept illegal in the country.

http://www.theregister.com/2005/03/10/tegam_verdict/

Britain Leads the World

Unfortunately, the lead is in zombie PCs, according to a survey by Symantec. Twenty-five point two percent of zombie PCs are in the UK, overtaking the US, at 24.6% and China at 7.8%. This reflects growth in broadband use.

http://news.bbc.co.uk/2/hi/technology/4369891.stm

http://www.theregister.co.uk/2005/03/21/botnet_charts/

The Future of Cryptography is Cranks

Karl Mahlburg, a graduate student at the University of Wisconsin, has used a "combinatorial" approach to proved "the crank" can be generalised to all primes. The crank is a rule deduced in the 1980's that explained congruences, a number pattern discovered by genius Srinivasa Ramanujan in the early Twentieth Century.

The New Scientist comments, "The solution may one day lead to advances in particle physics and computer security."

http://www.newscientist.com/article.ns?id=dn7180

http://www.usna.edu/Users/math/meh/ramanujan.html

No Technological Fix

Activists have bypassed restrictions set on Apple's iTunes Music Store in less than 48 hours. This allows customers to play music downloaded from the site on any platform, not just Mac or Windows, thus increasing Apple's potential customer base. The downloaded music is not protected by DRM, so it is also vulnerable to illegal copying.

DRM has proved unpopular with many consumers because, in addition to protecting the content from illegal copying, it restricts the customer unfairly: dictating what equipment they must use and preventing permissible "fair use".

http://www.theregister.co.uk/2005/03/23/pymusique_unblocks_itunes/