Yui Kee Computing Ltd.

Newsletter

May 2005

Contents

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
- 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

Soccer Fans Targeted

A version of the Sober worm (W32/Sober.N) spread widely at the beginning of May in email messages purporting to be from the world soccer body, FIFA. The message claims that the recipient has been successful in applying for World Cup tickets, and instructs the victim to open the attachment, which, of course, contains the worm. The message is written in English or German, depending on the domain of the recipient address.

Graham Cluley, senior technology consultant for Sophos, said "Computer users who don't practise safe computing will feel as sick as a parrot, and will only be passing this worm onto other unsuspecting victims."

This is not the first time the World Cup has been targeted by virus writers, in 1998 WM97/ZMK-J hit and in 2002 the event saw VBS/Chick-F.

More information:

http://fifaworldcup.yahoo.com/06/en/050502/1/3kvw.html

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

http://www.sophos.com/virusinfo/analyses/w32sobern.html

http://www.theregister.com/2005/05/03/world_cup_virus/

HK Scores a World-First

The HK Scout Association, the HK Motion Picture Association (MPA), and the Intellectual Property (IPD) and Customs & Excise Departments of the HK Government have launched the world's first Scout Badge on Intellectual Property Rights. At least, it is assumed that the Customs & Excise Department is involved, but although the Press Release on the IPD website lists them, the Customs & Excise Department website contains no mention of the launch.

Reaction around the world has been mixed, with some questioning the appropriateness of the badge. Declan McCullagh commented, "It's not clear, though, how much time the MPA's merit badge curriculum will devote to the value of fair use, the problems that region coding on DVDs can create for legitimate purchasers, and the unintended consequences of 'anti-circumvention' laws like the Digital Millennium Copyright Act."

Perhaps a better way to foster respect for creativity is to encourage young people to be creative thus experiencing the effort involved.

More information:

http://www.mpaa.org/MPAAPress/2005/2005_05_02.doc

http://www.ipd.gov.hk/eng/pub_press/press_releases/press_release_30042005_e.pdf

http://www.theregister.com/2005/05/05/scout_ip_badge/

http://www.thestandard.com.hk/stdn/std/Metro/GE04Ak06.html

http://67.19.9.2/?article=23038

http://www.boycott-riaa.com/article/16720

http://www.slyck.com/forums/viewtopic.php?t=10994

Anti-Virus Company Tests Car

In our February 2005 issue, we reported on rumours, and dismissal of the rumours, that a Symbian virus had infected a Bluetooth-enabled Lexus. Although we have not been taken up on our offer to in-depth test any cars delivered to us, we can (jealously) report that F-Secure, in conjunction with Helsingin Sanomat, a major Finnish newspaper have obtained a Toyota Prius for testing in their underground bunker.

F-Secure concluded that the car was immune to known Bluetooth attacks.

Full Report:

http://www.f-secure.com/weblog/archives/archive-052005.html - 00000553

VOIP Emergencies

As important issue with VOIP services is the ability to connect to emergency services, and the ability of the emergency services to determine the location of the caller. The U.S. Federal Communications Commission (FCC) recently ruled that VOIP service providers must

automatically link customers to a 911 service (911 is the U.S. emergency number), and provide an originating address for the call.

Some analysts are seeing this as an attempt by traditional phone companies to raise the costs of VOIP providers and slow their business growth.

More information:

http://www.theregister.com/2005/05/20/ne_phone_charges_may_rise/

Cyber-kidnappers take files hostage for Internet ransom

In late May 2005 an extortionate trojan exploiting a well-known vulnerability of Microsoft Internet Explorer (MS04-023) was widely circulated. As usual, anti-virus vendors are using a variety of names for the malware:

- Troj/Gpcode-B (Sophos)
- TROJ_PGPCODER.A (Trend Micro)
- PGPcoder (McAfee)
- Trojan.Pgpcoder (Symantec)
- Win32.Gpcode.B (CA)
- Virus.Win32.GPCode.b (Kaspersky Lab)

The trojan downloads and executes malicious codes, then encodes all files found on the storage media with these extensions: ASC, DB, DB1, DB2, DBF, DOC, HTM, HTML, JPG, PGP, RAR, RTF, TXT, XLS, ZIP. Then the trojan drops a text file named ATTENTION!!!.txt which says:

```
Some files are coded.
To buy decoder mail: n{removed}@yahoo.com
with subject: PGPcoder 000000000032
```

The Trojan adds registry keys so that it will be run on startup.

The intention of the "cyber-kidnappers" is to ask for a US$200 ransom from users to decode the files hostages. Some security experts refer this kind of trojan as "ransom-ware". No doubt, the relevant police forces are making efforts to trace the bank transactions, but intelligent criminals will have made efforts to obscure the trail. Even if the criminals are caught, victims may never recover their encrypted data.

The security patch of Microsoft Internet Explorer for that vulnerability was issued on 12th July 2004. Users are recommended to:

- backup their data frequently,
- patch the operating system with latest security patches,
- install anti-virus software with latest virus definition signatures included and with on-access scanning turned on,
- install server-side/client-side firewall hardware/software if possible,
- download the latest version of Microsoft Internet Explorer with latest patches installed, or use another web browser.

The encrypt-and-extort technique is not new, possibly the first use was in December 1989 when the "AIDS Diskette" was sent out by mail on 5.25 inch floppies.

More information:

http://www.theregister.co.uk/2005/05/25/trojan_hostage_attack/

http://www.viruslist.com/en/weblog?weblogid=164377138

http://news.yahoo.com/news?tmpl=story&u=/cmp/20050525/tc_cmp/163700577

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

http://www.sarc.com/avcenter/venc/data/trojan.pgpcoder.html

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FPGPCODER%2EA

http://vil.nai.com/vil/content/v_133901.htm

http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=43103

http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=194

http://www.microsoft.com/technet/security/Bulletin/MS04-023.mspx

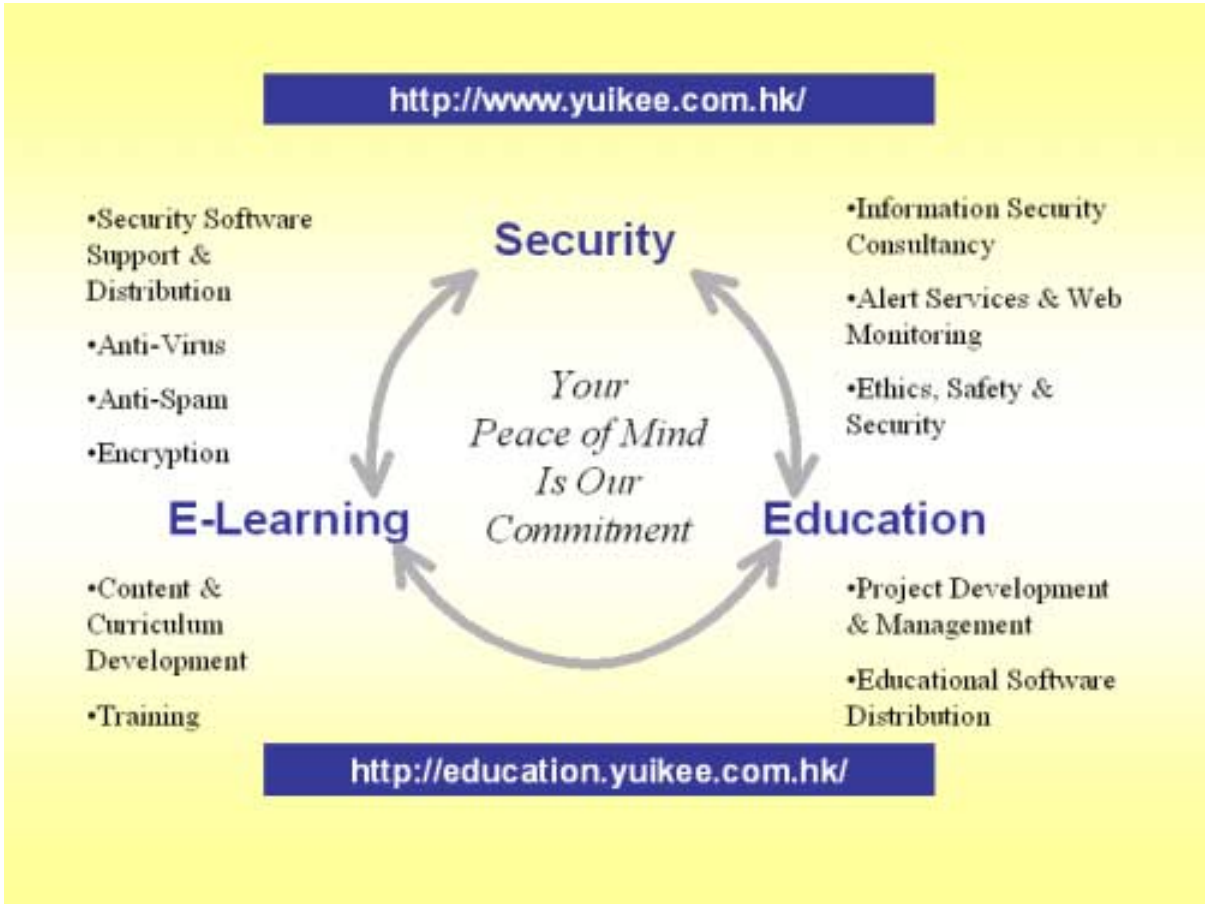
Sophos Developing Client Firewall for the Enterprise

Many of today's malware threats involve unauthorized connections, either remote attackers scanning for vulnerabilities to use as an entry point, or malware that has already been downloaded attempting to fetch more components, infect other machines, or sending confidential information: perhaps personal or banking details. Personal firewalls have been developed to address this problem, allowing the user control over what makes connections when.

However, in a corporate environment, local configuration and lack of features to prevent users changing settings make personal firewalls unmanageable.

To meet the needs of organisations to have central management of local connections, Sophos is using Agnitum's award-winning Outpost Pro technology as a technology base to engineer an industrial-strength solution for future integration into Sophos's suite of products designed specifically for networked environments. A free technical preview of the product will be made available.

"Sophos is committed to providing a best-of-breed integrated security suite for its customers, which is why we've chosen to acquire award-winning firewall technology," said Jan Hruska, chief executive officer, Sophos.


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/