Yui Kee Computing Ltd.

Newsletter

November 2004

Contents

Editors Notes

November was another busy month, with many developments. The AVAR Conference was a particular highlight. A low point was the continuing attempt by CPCNet, one of our ISP's, to terminate our Internet connection, on the grounds that we (as an anti-virus and information security company) use it to send and receive viruses and Trojans. We found it necessary to issue a press release on the situation on 23rd November, the full press release is included below. Since then, OFTA has referred the issue to their legal section, and CPCNet has delayed the termination pending the outcome.

Yui Kee Computing remains committed to providing our customers with top-quality information security protection and services by legal means.

Incident Update

- Thu Nov 4 11:31:44 2004 CA: Win32.Bagle.AQ
- Thu Nov 4 17:02:25 2004 CA: Win32.Bagle.AQ
- Sat Nov 6 14:16:45 2004 CA: Win32.Mydoom.O
- Mon Nov 8 12:16:59 2004 CA: Win32.Bagz.F
- Tue Nov 9 13:31:33 2004 NAI: W32/Mydoom.ag@MM Medium
- Tue Nov 9 14:01:58 2004 NAI: W32/Mydoom.ah@MM Medium
- Wed Nov 10 04:02:31 2004 TREND: MS04-039_ISA_SERVER Medium
- Fri Nov 19 16:46:34 2004 NORMAN: Sober.H High
- Fri Nov 19 17:46:33 2004 TREND: WORM_SOBER.I Medium
- Fri Nov 19 18:01:50 2004 NAI: W32/Sober.j@MM Medium
- Fri Nov 19 19:46:33 2004 SARC: W32.Sober.I@mm L3
- Fri Nov 19 20:31:37 2004 NORMAN: Sober.I High
- Sun Nov 21 19:46:40 2004 TREND: SYMBOS_SKULLS.A Medium
- Wed Nov 24 10:16:47 2004 TREND: WORM_SOBER.I Medium

Rise of Mobile Malware

A Trojan written for the series 60 Symbian mobile phone operating system; Troj/Skulls, appeared in the middle of the month. Although it is quite destructive - it disables all applications on infected phones, most vendors gave it a low-risk assessment. Trend Micro initially rated it as medium, but later revised that downwards.

A second variant, Troj/Skulls-B, appeared at the end of the month; it also drops a copy of the virus SymbOS/Cabir.B. However, the virus would have to be started manually before an oubreak over Bluetooth could occur.

More information:

http://www.f-secure.com/weblog/archives/archive-112004.html - 00000373

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

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

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

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

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=SYMBOS_SKULLS.A

OFTA Publishes Anti-Spam Consultation Submissions

The Office of the Telecommunications Authority has published the submissions on its consultation paper, "Proposals to Contain the Problem of Unsolicited Electronic Messages". There were a total of 41 submissions, including ones from companies, societies, including the Hong Kong Computer Society, and individuals.

http://www.ofta.gov.hk/report-paper-guide/paper/consultation/20041102/table.html

Rob Rosenberger On-Form

Rob Rosenberger, the man behind Vmyths.com, the website that uses humour to make important points about the hype surrounding information security, has certainly been on-form in November:

- Sun Nov 14 14:31:44 2004 VM: mi2g plays the "voice of sanity" card
- Tue Nov 16 05:46:36 2004 VM: Let's give thanks for antivirus software that so often fails to do its job
- Wed Nov 17 08:31:33 2004 VM: The significance of one handwritten resignation letter

In his email newsletter, he also takes a shot at the lack of reaction to the revelation that over 60,000 PC's were messed up in a Windows XP upgrade, reported in The Register: http://www.theregister.com/2004/11/26/dwp_network_outage, saying, "If a computer virus did this, you know full well the media would go ballistic... Why, why, WHY does this double standard exist?"

Think about it next time someone warns you about the latest mobile phone malware that has messed up perhaps a dozen phones worldwide… oh, that's us!

Yui Kee Warns: CPCNet Puts Customers At Risk; OFTA Adopts a "Hands Off" Position

Press Release

Yui Kee Computing Limited is warning that CPCNet Hong Kong Limited's Terms and Conditions make their customers more vulnerable to malicious software, such as viruses. CPCNet has imposed a ban on its customers sending samples of malicious code, including if they are sent to an anti-virus developer or other information security expert. Current viruses can spread round the world at Internet speed, but CPCNet customers can only shout for help at snail mail speed. CPCNet has shown that it is willing to terminate customer accounts in support of this draconian ban.

Some customers may already be in violation of the ban because their anti-virus software is configured to automatically send a sample to the developer via the Internet. CPCNet has insisted that it will apply their Terms and Conditions equally to all customers, so these customers may have their Internet connection terminated.

The problem came to light when Yui Kee, a customer of the ISP since 1994, decided to change its existing Leased Line to a Broadband connection. The new Terms and Conditions included clause 18(c):

> 18. The Customer must not use the Services to store, transmit or distribute:
>
> (c) any virus, worm or Trojan horse software or any software for damaging or compromising the security of other computers, networks or sites.

"We knew immediately that this clause was a problem for us, we use the Internet to communicate with anti-virus researchers and other information security professionals around the world. Occasionally, this includes sending a sample of malicious code, in a safe, secure manner", said Allan Dyer, Chief Consultant of Yui Kee. "However, a little further thought reveals that it is a problem for anyone who cares about their information security."

When users encounter a problem, they ask their support staff. If it is new to the support staff, they will contact the vendors' technical support department. If the problem involves a suspicious program or file, they will send it with the question. Naturally, they will all use the easiest and quickest communication method: usually, the Internet. Some anti-virus products even automate this process, as can be seen from the following excerpts from the Symantec web site:

http://enterprisesecurity.symantec.com/products/products.cfm?productid=155

> "NAVEX^(TM) and Digital Immune System^(TM) technologies provide virus detection, analysis, and repairs via automated submission and response mechanisms."

http://securityresponse.symantec.com/avcenter/submit.html

> "If you would like to submit a virus sample manually, please use our secure Web Submission Tool."

http://service1.symantec.com/SUPPORT/ent-gate.nsf/df96e9c0a4b1dfa288256bc1005cd7d5/7b22e01d8ca57fdb88256c77005673af?OpenDocument&src=bar_sch_nam

> "You want to know what changes need to be made at the firewall to allow the Quarantine Server to communicate with Symantec for delivery of suspect files."

This shows that transmission of suspicious samples to anti-virus developers via the Internet is considered normal, and it may be configured to occur transparently to the user.

"We tried to explain the issues and our concerns to CPCNet, but they just reiterated their policy", Dyer reported, "We even re-wrote the clause for them":

> 18. (c) any software, including but not limited to any virus, worm or Trojan horse with the intention of infecting, damaging or compromising the security of other computers, networks or sites.

The modified clause allows transmission of samples to support or information security professionals because the intent of the customer is taken into account. Even Hong Kong Law does not seek to define a computer virus; it also uses the intent of the perpetrator when defining Criminal Damage.

"Then, on 15th October, they sent an ultimatum: sign an undertaking, or have our Leased Line terminated.", Dyer continued. The letter included a statement of CPCNet's understanding of the threat:

> "Transmission or storage of virius worm or Trojan horse software or anything of similar nature is hazardous and may cause significant and irremediable damages to the network system and any persons connected with the network."

Allan Dyer commented, "They are including irremediable damage to people? I suppose that must mean permanent injury or death. CPCNet thinks that emailing a computer virus sample can kill people! Even ignoring that hyperbole, CPCNet does not appear to understand the ISO Seven Layer network model, which guarantees that the content of a message will not affect the lower layers of the network infrastructure."

Yui Kee took the issue to OFTA. OFTA choose to view the matter as a contractual issue,

> "We would like to reiterate that OFTA's powers and functions do not extend to the arbitration on fairness of contractual terms or settlement of contractual disputes between individual customers and the operators."

Meanwhile, following the expiry of the deadline, CPCNet sent a Notice of Termination of Service on 1 November, saying that Yui Kee's leased line would be cut at 6:00 p.m. on 29 November. Dyer was confused, "Apparently, from their earlier ultimatum, they consider that our actions may kill someone, yet they wait six weeks before acting. These are not the actions of a responsible company."

Yui Kee's previous use of CPCNet's service, including the receipt of virus samples and the sending of encrypted virus samples, has caused no interruption or security problem. Dyer emphasised, "I can also state that we will always act to prevent such problems. CPCNet is claiming that we represent a grave threat to their network, but they have never explained the basis of these fears. The truth is we are not a threat, we have not been a threat, and we will not be a threat, CPCNet's fears are groundless."

Yui Kee is contending that they have not violated their existing Terms and Conditions, so CPCNet has no grounds for termination, and OFTA should act to prevent the disconnection of a customer that has done nothing wrong. OFTA has not yet responded to this.

However, Dyer points out that the more important issue is whether an ISP can be allowed to restrict their customer's access to effective anti-virus support, "CPCNet has failed to explain how users can quickly send samples to anti-virus researchers for analysis. It is not too late for CPCNet to take the sensible course, and change the problematic clause for all their customers."

Notes from the AVAR Conference

Allan Dyer

The seventh Anti-Virus Asia Researchers International Conference was held this year on the 25th and 26th November in Tokyo Bay, Japan. The conference theme was "Eutaxy or Chaos, Network Security Present and Future". Sessions included detailed discussion of the computer security situation in Japan, featuring speakers from the Ministry of Economy Trade and Industry, the Ministry of Internal Affairs and Communications, and the National Police Agency. Another session had Government representatives from Japan, Korea and China on-stage together discussing computer security in their countries.

More technical sessions included the cell phone environment in Japan, and how to script anti-virus definition updates for multiple products. I was honoured to chair a panel session on Microsoft's progress in security, with Mr. Takahiko Higashi, Microsoft's Chief Security Advisor on one side and five top anti-virus researchers on the other.

Another topic was how malware writers are changing, and how the good guys are catching them. I think a common thread through a lot of the talks and discussions was cooperation and coordination. The bad guys are already working together: virus writers are creating viruses that drop backdoors to make zombie networks; spammers are purchasing zombie networks to act as spam relays; phishers are using spam to attract victims to their fake sites and so on. Although they have disparate aims and methodologies, they are united in their greed and criminal intent. We need to improve how we work together, between ordinary users, companies and Government, to bring together the education, technology and laws to build an effective defence in depth.

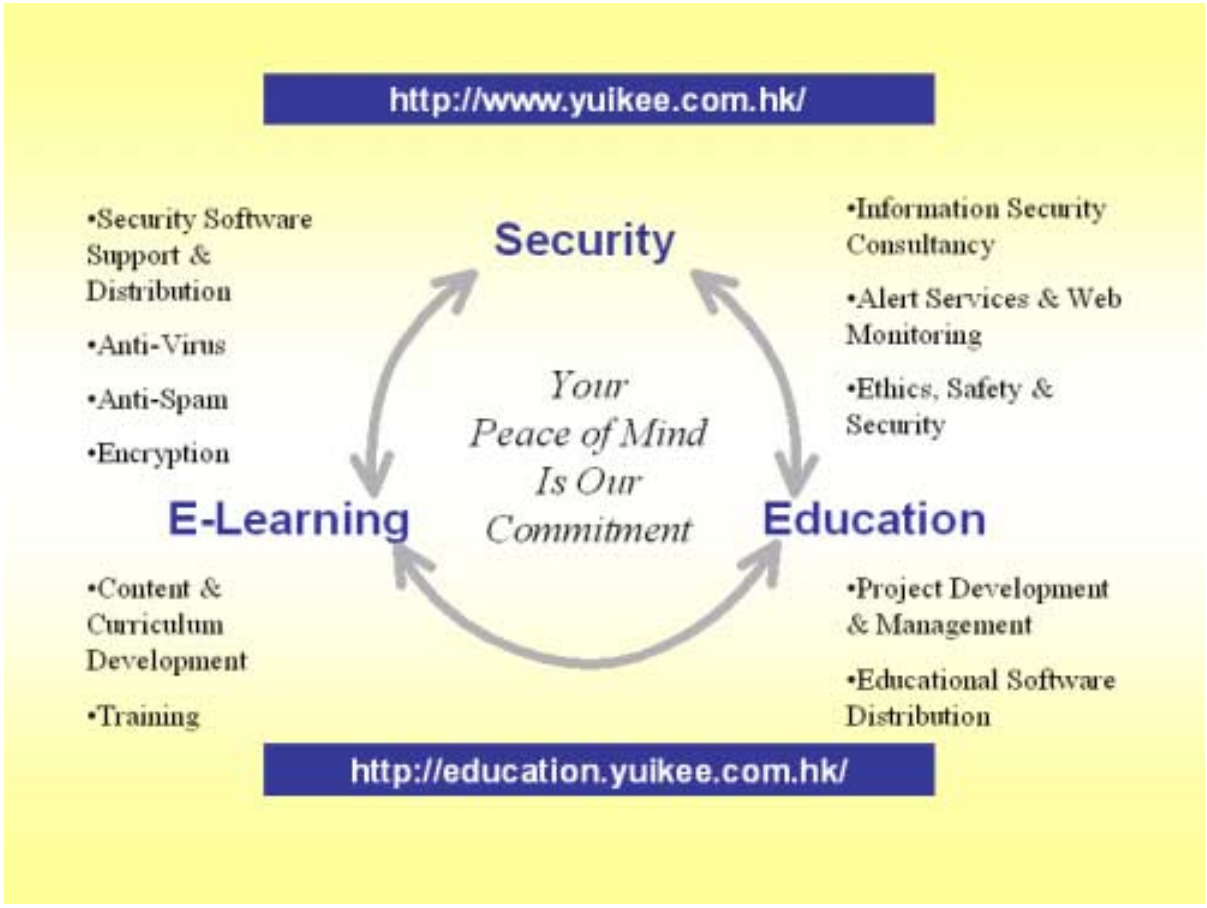
More Information:

http://www.aavar.org/

http://www.f-secure.com/weblog/archives/archive-112004.html - 00000367

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/