Yui Kee Computing Ltd.

Newsletter

February 2005

Contents

Contents 1
Incident Update 1
Information Security is Everybody's Business - Except OFTA's? 1
Sophos Acquires Client Firewall Technology, Announces Industrial-Strength Solution 2
CPCNet Hypocrisy Revealed 3
ISS X-Force finds AV Scanner Problems 3
SHA-1 Broken by Chinese cryptographers 4
Lexus Virus? 4
John Tsang Speaks on Spam 4
Will Anti-Spam Laws Curb the Problem? 5

Incident Update

- Tue Feb 1 18:46:41 2005 TREND: WORM_BAGLE.AZ Medium
- Thu Feb 3 11:16:45 2005 TREND: WORM_BROPIA.F Medium
- Thu Feb 3 13:31:37 2005 TREND: WORM_AGOBOT.AJC Medium
- Mon Feb 7 09:31:57 2005 CA: Win32.Lovgate.AO
- Mon Feb 14 13:02:05 2005 CA: Win32.Mydoom.O
- Mon Feb 14 13:02:05 2005 CA: Win32.Netsky.Z
- Thu Feb 17 08:16:49 2005 NAI: W32/Mydoom.bb@MM Medium
- Thu Feb 17 09:16:45 2005 SARC: W32.Mydoom.AX@mm L3
- Thu Feb 17 10:16:55 2005 TREND: WORM_MYDOOM.BB Medium
- Thu Feb 17 13:01:49 2005 TREND: BKDR_SURILA.O Medium
- Thu Feb 17 15:47:09 2005 NORMAN: MyDoom.AQ Medium
- Thu Feb 17 17:31:43 2005 FSC: Another Mydoom variant spreading 2
- Mon Feb 21 20:17:04 2005 NAI: W32/Mydoom.be@MM Medium
- Tue Feb 22 13:02:00 2005 CA: Win32.Mydoom.AU
- Thu Feb 24 17:16:59 2005 NORMAN: Netsky.D Medium

Information Security is Everybody's Business - Except OFTA's?

On 23 December 2004 OFTA wrote a letter to Yui Kee stating, in part, "On the issue of information security, please note that it is outside the ambit of this Office. You are advised to contact the organisations named in Attachment 2 as appropriate for enquiries." Attachment 2 was a printout of the webpage: http://www.infosec.gov.hk/english/general/pubsrv.htm. The slogan for the website, displayed on every page, is, "Information Security is Everyone's Business".

The website is produced and managed by the Office of the Government Chief Information Officer of Hong Kong, and OFTA is a Hong Kong Government department responsible for regulating the telecommunications sector. For some reason, parts of Hong Kong Government consider information security to be "Everybody's Business", but another department considers it outside its ambit.

We asked OFTA to clarify the matter, "is OFTA rejecting the slogan ("Information Security is Everyone's Business") of the very same website it kindly printed the page from?" They have not responded at the time of writing.

Sophos Acquires Client Firewall Technology, Announces Industrial-Strength Solution

Sophos grows at more than twice market rate with 36% increase in turnover Global security provider prepares to extend security offerings with acquisition of firewall technology

Sophos has acquired an award-winning client firewall technology and expertise in a non-exclusive transfer deal with Agnitum Ltd. Sophos will use Agnitum's Outpost Pro product as a technology base to engineer an industrial strength solution for future integration into Sophos's suite of products designed specifically for networked environments.

In mid-February Sophos will announce significant product upgrades that incorporate a number of benefits, including advanced technologies which enhance the proactive interception of new viruses and emerging spam campaigns.

"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. "Our consistent performance and impressive growth year-on-year proves that the market appreciates our strong focus on business markets and our efforts to meet customer demand for simplified, consolidated endpoint and gateway protection against the latest security threats."

Over the past 16 months, and with the consolidation of anti-spam protection and email policy enforcement protection into its product portfolio, Sophos has successfully moved from being an established anti-virus firm to a respected security company with an expert focus on gateway and endpoint solutions. In the UK alone, sales of Sophos PureMessage, the company's consolidated email gateway protection, have increased 100-fold since April 2004. Sophos products are used by over 50% of the companies listed in the latest FTSE 100 as well as protecting many well known names such as Marks & Spencer, Orange, Oxford University and Sainsbury's.

"Increasingly organizations are looking for flexible, easy to manage security solutions that address the spectrum of threats as well as protect data through policy enforcement and regulatory compliance, said Chris Christiansen, Program Vice President for IDC's Security Products program. "By broadly defining the threat environment, recognizing the convergence and complexity of those threats and adding personal firewall to its offering, Sophos is ahead of the curve in providing protection at all points of the network."

Analyst group IDC predicts the security software market as a whole to grow at 16.9% annually between 2003 and 2008*. In the last financial year, Sophos's turnover grew at more than twice this rate - 36% - demonstrating the company's continued momentum in capturing market share in the highly competitive security market. Sophos's customer base has grown 18% in the same period, with an impressive global renewal rate of 76%.

CPCNet Hypocrisy Revealed

CPCNet Hong Kong Limited has failed to take action when presented with evidence that its IP addresses have been used to transmit viruses to Yui Kee. As reported in the November and December 2004 issues of this newsletter, CPCNet has previously taken a very strict position, insisting that its network must not be used for the transmission of viruses under any circumstances. When Yui Kee pointed out that this would prevent the transfer of samples in the fight against viruses and refused to accept the new Terms and Conditions, CPCNet terminated Yui Kee's connection.

Yui Kee carefully examined its anti-virus gateway logs and identified thirteen occasions between July 2004 and January 2005 when an IP address owned by CPCNet transmitted a message containing a virus to Yui Kee's mail server. On 29 January, 2005, Yui Kee sent this evidence to CPCNet. Further incidents occurred on 12 February, 13 February and 23 February, and a report was sent to CPCNet on each occasion. Each report requested an explanation of the potentially criminal act, and pointed out that the incidents violated CPCNets Terms and Conditions. To date, CPCNet has provided an "explanation" for just one of the incidents, stating that their server was bouncing an undeliverable message to the apparent sender. The message in question contained W32/Netsky-P, which is known to forge the sender's address. Yui Kee publishes SPF records for its domains, so CPCNet could have checked the origin of the message and rejected it. Worse, CPCNet's server constructed a bounce message that contained the virus itself, and sent it to an innocent party without anti-virus scanning. CPCNet has not responded to these points.

In a telephone conversation, CPCNet staff said that the company could not respond because Yui Kee was not a CPCNet customer. Of course, Yui Kee is not a CPCNet customer because CPCNet terminated the relationship. It is not clear why this would absolve CPCNet of responsibility for continued incidents of virus transmission from CPCNet's IP addresses.

Yui Kee's Chief Consultant, Allan Dyer, commented, "CPCNet wants to have its cake and eat it. If they insist on this ridiculously strict policy, they must be prepared to take action when there are clear violations, as in these cases. We will continue to question this company's hypocrisy."

ISS X-Force finds AV Scanner Problems

ISS X-Force has discovered vulnerabilities in the way some Symantec and F-Secure products handle specific types of compressed files. The vendors have released fixes, but this shows that systematic searching for problems can discovered previously unknown flaws. There has also been an announcement concerning ZIP file handling in ClamAV. There may be more vulnerabilities related to the handling of compressed files discovered in the near future.

More information:

Symantec: http://www.symantec.com/avcenter/security/Content/2005.02.08.html

F-Secure: http://www.f-secure.com/security/fsc-2005-1.shtml

ClamAV: http://www.gentoo.org/security/en/glsa/glsa-200501-46.xml

Trend:
http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VName=Vulnerability+in+VSAPI+ARJ+parsing+could+allow+Remote+Code+execution

http://www.theregister.com/2005/02/11/f-secure_patch/

SHA-1 Broken by Chinese cryptographers

Xiaoyun Wang and Hongbo Yu from Shandong University and Yiqun Lisa Yin from Princeton University, have released a paper briefly outlining their findings. They claim that a collision can be found in the full version of SHA-1 in 2^{69} hash operations, which is about 2,000 times faster than brute force.

Bruce Schneier commented, "It's time for us all to migrate away from SHA-1."

http://www.schneier.com/blog/archives/2005/02/sha1_broken.html

http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

http://www.theregister.co.uk/2005/02/17/sha1_hashing_broken/

Lexus Virus?

There were widespread reports that Kaspersky Labs was investigating a suspected incident of a Lexus car onboard computer being infected with a Symbian virus, via Bluetooth. However, Lexus soon clarified that, although their cars are equipped with Bluetooth for uploading addresses to the navigation system, the operating system is proprietary and the data cannot be exported from the navigation system to other systems in the car. The threat from this type of virus transmission is, currently, approximately zero.

In the interests of safety, Yui Kee's experts will perform free in-depth testing of Lexus cars delivered to our offices with a full tank of petrol, and "any driver" insurance.

More information:

http://vmyths.com/hoax.cfm?id=284&page=3

http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=c794e3d0-7b09-4329-af07-c65dfd75fcd6&newsType=News

http://www.engadget.com/entry/1234000760029037/

http://news.com.com/Lexus+a+nexus+between+cars+and+phone+viruses/2100-7349_3-5551367.html

http://news.zdnet.co.uk/internet/security/0,39020375,39185480,00.htm

John Tsang Speaks on Spam

The Government will take a number of measures including launching a campaign entitled "STEPS" to fight Hong Kong's spam epidemic, the Secretary for Commerce, Industry and Technology, Mr John Tsang, said on February 24.

Speaking during a luncheon meeting organised by six information and communication technology organisations, Mr Tsang said spamming was a problem that had affected almost everyone in Hong Kong.

Drawing on the views expressed to an earlier consultation and the trend on recent developments, the Government will launch the "STEPS" campaign to contain the problem of spamming.

The first letter "S" stands for strengthening existing regulatory measures. In conjunction with relevant industry associations and service providers, the Government will start work in two areas:

> For fax, the Government will work closely with the service providers to reduce the timeframe required to cut off abusers fax lines.
>
> For SMS and MMS, the Government plans to work with the industry to extend the existing code of practice for mobile network operators to cover all SMS and MMS unsolicited promotional messages, including those sent by the operators themselves.

The second letter "T" stands for technical solutions. The Government will collaborate with the industry to organise seminars, conferences and exhibitions to promote the latest anti-spam technical solutions to all users.

Echoing the Australian "Don't Try, Don't Buy, Don't Reply" campaign, the third letter "E" stands for education. "In the fight against spam it is vital that the recipients play their part in denying the spammers by not purchasing anything marketed through spam or, better still, not responding to spam at all." Mr Tsang said.

The fourth letter "P" stands for partnerships. Mr Tsang highlighted that one possible partnership was the development of a common blacklist to filter spam at the local Internet service provider level.

On global partnership, Mr Tsang revealed that the Commerce, Industry and Technology Bureau would soon become one of the Founding Signatories of a Multilateral Memorandum of Understanding on Co-operation in Countering Spam.

"This MoU will facilitate co-operation among Asia-Pacific signatories on many fronts in tackling the spam problem. We will continue to develop international partnerships and play a leading role in the fight against spam," he said.

The last letter "S" stands for statutory measures. Mr Tsang said that the Government believed it would be necessary to enact legislation to regulate spamming, "Such a piece of legislation would prevent Hong Kong from becoming a safe haven sheltering illicit spammers. It would also facilitate co-operation with overseas jurisdictions with similar legislation in investigation and enforcement work against spammers."

The Government has an open mind on the exact form and content of the legislation, but Mr Tsang said that a balance was required between the need to discourage spamming and enabling legitimate e-marketing activities to develop properly.

"Our aim is to work out a legislative framework which is largely acceptable to different stakeholders before we proceed to draft the legislation. We will engage representative stakeholder groups over the next few months for detailed and pragmatic discussions. We intend to introduce the full draft legislation into the Legislative Council some time next year," Mr Tsang said.

http://www.citb.gov.hk/speech/pr24022005b.htm

http://www.info.gov.hk/gia/general/200502/24/02240201.htm

http://www.ofta.gov.hk/press_rel/2005/feb_2005.html - 1

Will Anti-Spam Laws Curb the Problem?

Allan Dyer

(An edited version of this letter appeared in the South China Morning Post, page C2, 1 Match 2005)

People who point out that laws would be ineffective because 95% of the spam we receive comes from overseas are missing the damage that lack of legislation is inflicting on our economy. This is not merely, as John Tsang said in his speech, that our "online marketers" will have their efforts diluted when their messages are wrongly blocked as spam. Many email administrators are already blocking countries indiscriminately - I have seen a message advocating blocking of Hong Kong because it is "another spammy Asian country". Even more extreme, in a widely criticised move, the large US ISP Verizon recently blocked all email from many European and Asian countries.

We can imagine a local SME that invests in a booth at an overseas trade fair. They collect many namecards, and follow up by email, not realising that over-zealous spam filters are silently

discarding many of the messages. The entire investment in the physical booth might be wasted because of failure in the virtual world.

To avoid this in future, we need legislation that will be effective at shutting down spammers operating from Hong Kong.

Mr. Tsang also mentioned existing statutory measures that can help control spammers, but he did not mention the difficulties in current legislation. For example, the Telecommunications Ordinance prohibits the blocking of messages - does this mean that an ISP could be prosecuted for blocking spam or viruses? OFTA and the ISPs routinely gloss over this difficulty, but it would be preferable to have legislation that makes sense. In this case, there should be clearly defined criteria for when a service provider is permitted (or maybe required) to block a message - probably including forging of the senders information, and content sent with malicious intent.

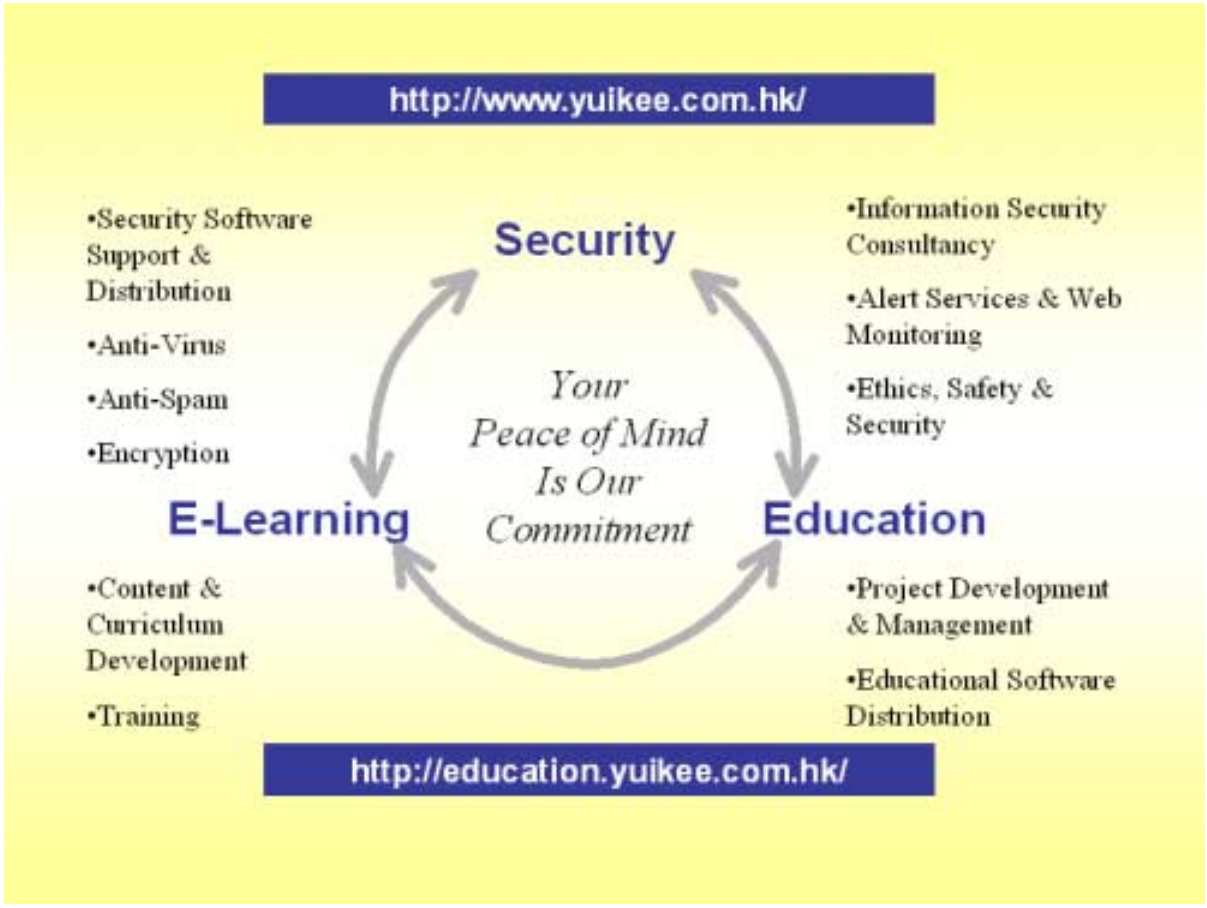
The idea of a local common blacklist may seem attractive, but what would its purpose be? If it is to control spam that is originated or relayed locally, surely the preferred course of action is to use the law to shut down the operator. If it is to identify overseas sources, then much wider cooperation is required, and the purpose would be better served by participation in the many international blacklist efforts. Besides, the ISPA has a poor track record for acting on their pronouncements - they published a Code of Practice on spam some years ago, but they have never even published the list of ISPs that agreed to it.

I am also disappointed that Mr Tsang describes the Penny Black project as "promising" - this would add an artificial additional processing cost to email that would have a disproportionate effect on those least able to cope - those using less-powerful (perhaps second-hand) hardware, thus widening the Digital Divide. It would have no effect on the worst spammers, because they use zombies and so are already stealing the resources to send their messages. They would quickly find methods to steal "stamps" too.

The "STEPS" campaign puts Statutory measures last, but Hong Kong is already behind many other countries, including the USA, Australia and the EU, which already have anti-spam legislation. Our only advantage is that we can benefit from their experience.

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/