Yui Kee Computing Ltd.

Newsletter

May 2003

Contents

Incident Update

May saw a variety of incidents, F-Secure issued a Radar Level 2 warning about W32/Kickin.A@mm on the 7th. It sends emails to addresses it finds in the Windows address book, HTML files, and XML files. The emails have a variety of content, including personal, sexual, the Iraq war and SARS.

W32/Fizzer@mm appeared on 8th May, F-Secure initially issued a Radar Level 2 warning, but upgraded that to Radar Level 1 on the 13th. MessageLabs currently has it rated as High Risk from its statistics. Fizzer can spread on KaZaA peer-to-peer networks, and by emailing itself to addresses from the Windows and Outlook address books and random addresses at some major webmail domains. It includes an IRC backdoor Trojan.

W32.Sobig.B@mm appeared on the 18th, but various anti-virus developers named it W32/Palyh@mm or W32.HLLW.Mankx@mm. F-Secure upgraded their Radar Level 2 alert to Level 1 on the 19th, and MessageLabs currently rates it as High Risk. That is likely to change as it is programmed to stop spreading on 31st May. Sobig.B arrives in an email that appears to come from support@microsoft.com.

On the 29th, F-Secure issued a Radar Level 2 alert for W32/Holar.h@mm. It spreads over email and KaZaA peer-to-peer networks. It also has a destructive payload, after 30 reboots, the virus attempts to delete all files on drive C:.

Information Security Showcase 2003

This event will take place from 16th to 18th June at Room 301 of the HK Convention and Exhibition Centre. There will be 20 free sessions covering all aspects of information security. Our Chief Consultant, Allan Dyer, will be a Keynote Speaker in his capacity as the President of AVAR at 13:30 on the 18th, his topic is "Anti-Virus Defence in Depth".

New Alert Services

Yui Kee will also have a booth in the exhibition, showing our latest solutions for anti-virus, encryption, gateway security and alerting. The show will be the first public presentation of our virus and security alert services, that deliver critical notifications direct to your mobile. We hope to see you there.

http://www.hkpc.org/infosec2003

SSH Against SARS Campaign

One month free usage of SSH Secure Shell

50% discount on tele-working package!

To help company and government employees to work from their home, Yui Kee in association with SSH Communications Security Corp would like to contribute to the fight against the SARS disease by extending a one month free usage of SSH Secure Shell as well as offering a special 50% discount for purchase of bundled package SSH Secure Shell for remote access. SSH Secure Shell allows employees access to their office networks and servers in an easy and secure manner.

With the SARS looming around, many companies would prefer their staff to avoid risk of infection by not coming to the office. That would be possible if their employees could work from home. But what about all the documentation the employees need for their daily work, that are stored in their computer or the company server? And what about access to their daily mail that is received on their company mail server?

Yui Kee and SSH understand the need for business continuity while maintaining the health of employees during this time of heightened anxiety. Remote access can be a safe and an effective way to maintain employee productivity during emergency situations, as well as during routine business operations if a few simple guidelines and procedures are followed.

Thanks to SSH Secure Shell, and its multi-application support, all these needed information left on the company network and server, can now be accessed securely from the employees home. Customer mails can be retrieved, confidential files can be transferred, the corporate database can be accessed and so on.

And if security is your concern, fret not. At Yui Kee, closing security loopholes has been our business for many years. And SSH is one of the world's leading developers of Internet-based data security solutions. It invented Secure Shell, which is now a de-facto industry standard for secure remote connection, already used in many respectable Hong Kong government organizations and multinational companies.

Tele-working has always been a welcomed alternative to long commuting in crowed train. But in a time like this, it is a necessary weapon for company to survive the economical effect of the disease.

SSH Against SARS special prices (50% discount campaign)

Teleworking package	Tele-Working Bundle	Normal Price	Special Price
SSH Against SARS 10	One Server and 10 Clients	HK$17,542	**HK$ 8,599**

SSH Against SARS 25	One Server and 25 Clients	HK$34,507	**HK$ 16,999**
SSH Against SARS 50	One Server and 50 Clients	HK$62,782	**HK$ 29,999**
SSH Against SARS 100	One Server and 100 Clients	HK$119,332	**HK$ 59,999**

Note: This offer is valid until June 30, 2003. This offer is valid only for usage of SSH Secure Shell in tele-working environment, which means remotely accessing the company server and gateway fitted with SSH Secure Shell for Servers, from personal computer at the employee's home, connected to the internet and also fitted with SSH Secure Shell for Workstations

CISCO Certified Security Professional in Hong Kong

Expand your Professional Option and advance your career in security with a new security certification accredited by Cisco Systems.

Yui Kee, Informatics and Smart Wise inaugurate the CCSP course. From left to right: Allan Dyer, Karen Cheung, Ip Ngai Keung, Louie Au, Simon Cheung.

Starting in June 2003, Yui Kee, Informatics CAL Education and Development Centre and Smart Wise Professional Development Centre offer CCSP training courses. These will be the first courses leading to the CCSP qualification available in Hong Kong. "We are always pleased to see positive developments in information security expertise and Informatics training centre is an excellent venue for these courses", commented Allan Dyer. Mr. Ip Ngai Keung, Director of Informatics CAL Education and Development Centre said, "With Yui Kee's decade of experience in Information Security solutions, we are pleased to collaborate with them". Simon Cheung, Director of Smart Wise Professional Development Centre said, "The courses combine a good venue, instructors and equipment. CCSP is a valuable qualification, don't miss out."

Cisco Systems has elevated the area of network security from its previous status of "specialization" to that of a full career track. As with other Cisco career tracks like CCNA /CCNP, network security will carry three levels of certification – Associate **(CCNA)**, Professional **(CCSP)**, and Expert **(CCIE-Security)**

What is Cisco Certified Security Professional (CCSP)?

This new certification recognizes the increased importance placed on individuals who are responsible for developing business solutions and designing and delivering multiple level of security for underlying network architectures. The CCSP includes three focused specializations – firewall (FW), virtual private network (VPN) and intrusion detection systems (IDS) – which combine with other courses leading to readiness for full CCSP status.

Why Cisco Security Training and Certification?

As a leader in networking, Cisco sets the standards for integrated network security. Most importantly, Cisco has designed its entire product line with security built into the fabric of the network. This crucial differentiator sets Cisco security products, training and certification apart from methods that employ a patchwork of point solutions.

What is the value of a CCSP to the individual?

The expertise developed when preparing for the CCSP adds to skill sets and helps expand career options by providing a professional-level certification to validate capabilities and readiness to design and implement complete end-to-end network security solutions. In a recent salary survey by Certmag in April 2003, professionals with the title CCSP earn higher averages salary than CCNA or CCNP. Only those professionals with the title of CCIE command greater average salaries.

Register for Free Seminars

We are holding free seminars to introduce CCSP and our available training courses, the next one is 19:00-20:30 on 6 June at 6/F Hang Seng Causeway Bay Building, 28 Yee Wo Street, Causeway Bay, Hong Kong. **Contact** 28708553 or 28708556, info@yuikee.com.hk for registration and full details. The first course starts 16th June.

University to Teach Virus Writing

The University of Calgary announcement of a course that teaches virus-writing has sparked controversy around the world. Sophos' Graham Clueley condemned the course as irresponsible, Rob Rosenberger ridiculed the idea, Robert Vibert expressed his concern and AVIEN organised a public letter. Security News This Week sentenced Sophos to the Dog-House for their remarks and Jan Hruska made clear the potential student's job prospects with his company.

Our Chief Consultant, Allan Dyer gives his opinion:

I met a similar situation: a few years ago a Hong Kong University was preparing a "continuing education" course on information security and I was invited to give the module on viruses and worms. The course organisers listed what they considered suitable content, including writing viruses. At that time, I was already very aware that the anti-virus industry strongly condemned any involvement with writing viruses but I made my own assessment and came to the same

conclusion. I decided to refuse to include that activity, and the course organiser acquiesced. Instead, I asked the students to write anti-virus software.

What a lost opportunity! If I had included that I could, today, be refuting the University of Calgary's claims that it, "explores new territory" with a course that is "unique". I do not regret the loss.

There is obviously a large difference between the ethical standards of many people in the anti-virus industry and Dr. John Aycock which I suspect stems from many security experts attempting to classify viruses and worms as just another vulnerability when there are crucial differences.

Computer Virus Basics

Everything I explain here has been said or written before by other, more distinguished writers (see Dr. Cohen, A Short Course on Computer Viruses), but it appears that not everyone was listening. A virus or worm, of course, is just another program, and it can do anything another program can do. The only difference is that it makes copies of itself. This leads to three properties: Generality, Range of Effect and Persistence. A virus can be created for any general-purpose programming environment. A virus can spread outside of the control of its creator. A virus can persist and cause a new outbreak an indeterminate time in the future.

Practical Considerations

In practical terms, the Lecturer asks a class of, say 30, students to create their viruses. At the end of class, there are 30 new viruses in the classroom. What does the Lecturer do to prevent them escaping? He could ask the students to destroy them - what if one copy is missed, or a student secretly saves it? The virus can start to spread around the world, and virus-specific scanners will not be able to recognise it. So the Lecturer should collect copies of the 30 viruses, and send them to the anti-virus developers. The viruses are then added to the glut of new viruses that products must detect, making them (slightly) slower. Each time the course is run virus glut gets worse.

Educational Benefits

A little thought will show that creating a program that copies itself is not a difficult problem, any competent programmer should be capable of doing it. What then is the learning benefit of actually performing such a simple task, and how does that benefit outweigh the risks associated with the new virus escaping?

What if the students were asked to create a "good" virus? Dr. Bontchev has adequately shown that there is no such thing as a good virus. Because of their properties of range of effect and persistence, they can reach environments that the author was unaware of, or that were not even created when the virus was written, with unpredictable consequences.

But Dr. Aycock says that in order to develop more secure software, and countermeasures for malicious software, you first need to know how malicious software works and the mindset of its creators. So how can students learn to create secure software? They can use the techniques without creating self-replicating code! The payload of a virus can always be studied independently - it is just another program. The infection techniques can be studied using programs that create or modify other programs, *without copying themselves*. However, more useful skills for a malware researcher are in reverse engineering - if you are presented with an unknown program, how do you quickly and accurately figure out what it does and how much of a threat it presents?

Medical Ethics

The course blurb also says, "This attitude is similar to what medical researchers do to combat the latest biological viruses such as SARS." But medical researchers normally put safety as the number one priority. One of the questions that needed to be urgently answered for SARS was

whether it was airborne or droplet-borne, but, as far as I know, no-one suggested the simple, obvious and accurate test of placing human subjects in rooms with appropriate sources, and waiting to see who got infected.

The DogHouse

I feel that Security News This Week's sentencing of Sophos to the DogHouse for their article is entirely unjustified. Their comments about the work are entirely consistent with the information on the course description page - it clearly states, "it will focus on developing malicious software such as computer viruses, worms", and it is this highly unethical practice Graham attacks. Additionally, the University of Calgary says the course "will help prepare them for careers dealing with computer security", so it is entirely appropriate for Sophos' CEO, Dr. Hruska, to warn potential students, "Don't bother applying for a job at Sophos if you have written viruses because you will be turned away," - Sophos is a leader in the field that the University thinks it is preparing its students for.

Dr Aycock, self-proclaimed not-Author of Yoga for Buffaloes, obviously has a sense of humour. I just hope that this course announcement is another joke.

References:

http://www.ucalgary.ca/news/may03/virus.html
http://www.sophos.com/virusinfo/articles/calgary.html
http://vmyths.com/rant.cfm?id=596&page=4
http://www.avien.org/publicletter.htm
http://securitynews.weburb.dk/show.php3?item=InformationSecurity&p[newsletterId]=540
http://www.sophos.com/virusinfo/articles/calgary2.html

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/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE