Yui Kee Computing Ltd.

Newsletter

May - June 2004

Contents

Incident Update

Sasser variants have dominated the recent news. A German teenager was arrested in connection with Sasser, see "Arrests and Prosecutions". Sasser.E was significant because it was released after the arrest of Sven Jaschan, implying he could not be solely responsible for the Sasser releases.

Wallon.A was interesting because of its use of a link to infect computers.

Although first reported on 11 June, Zafi.B really started spreading after the weekend.

1 May W32/Sasser.A

2 May W32/Sasser.B

4 May W32/Sasser.D

9 May W32/Sasser.E

12 May W32/Wallon.A

2 June W32.Korgo.F

11 June W32/Zafi.B@MM

Criminal Links Get Wider Attention

The evidence of links between virus writers, spammers and criminal gangs is growing, and getting the attention of the police and the wider IT press. MessageLabs estimates that two thirds of the spam it processes is from computers infected by viruses such as Sobig-F or Bagle.

More details:

http://www.theregister.com/2004/04/30/spam_biz/

F-Secure Celebrates Decade On The Web

The F-Secure website is ten years old. Ari Hypponen, Chief Technology Officer of F-Secure Corporation commented, "In April 1994, we had already been maintaining our antivirus BBS for several years, and realized how the graphical user interface just introduced by the Mosaic browser could make the Internet accessible to a much larger user base. Practically no commercial web sites existed at the time, but we saw that this www thing was simply so cool that we wanted to be part of it. Nobody knew it would explode like it did".

http://www.f-secure.com/news/items/news_2004051100.shtml

Witty: The Shape of Things to Come?

The Witty worm targeted a relatively small group of vulnerable machines - about 12,000 users of ISS's BlackIce and RealSecure products worldwide. However, commentators are pointing out that the attack was launched only 36 hours after the vulnerability was publicly announced, and it contained no significant bugs, implying that the attacker was a skilled programmer, familiar with worms, motivated and, because the payload of the worm is highly destructive, malicious.

More information:

http://www.computerworld.com/printthis/2004/0,4814,93584,00.html

http://www.icsi.berkeley.edu/~nweaver/login_witty.txt

First 64-bit Windows Virus Found

W64/Rugrat is a simple, proof-of-concept virus, but it is the first known 64-bit Windows virus. It is considered unlikely to spread significantly.

http://www.sarc.com/avcenter/venc/data/w64.rugrat.3344.html

http://www.vnunet.com/news/1155467

http://vil.nai.com/vil/content/v_125990.htm

SSH Tectia Seminar

On 20th May, Yui Kee organised a seminar for solution consultants and system engineers, to introduce and briefly train them on the new SSH Tectia Solution.

SSH as a technology is a de facto security technology supported by leading IT vendors and used by thousand of organizations worldwide. Traditionally however, SSH is mostly used for system administration.

Ms Karen Cheung, Business Development Manager of Yui Kee gave the welcome speech. JB Dumerc, Vice

JB Dumerc introduces SSH Tectia

President of SSH Communications flew from Japan to introduce managed security middleware for enterprise application security, explaining the need for unified application security middleware in enterprises and how SSH Tectia meets that need.

On his first Asian tour, Vesa Vatka, Product Manager of SSH Communications travelled from Finland to explain the technical details of the SSH Tectia Components After the coffee break, he continued with live demonstrations and the hands-on training.

Vesa Vatka explains secure tunneling

With the introduction of the SSH Tectia Solution, existing SSH infrastructure can be leveraged to seamlessly secure a wide range of applications. This allows IT solution providers to dramatically improve their solutions and services to their customers while lowering the system's cost of ownership, all this with the same trusted and reliable SSH technology.

The lucky draw winner and JB Dumerc

The participants received free evaluation copies of the SSH Tectia Servers and Clients and the seminar closed with a lucky draw for a USB MP3 player.

Arrests and Prosecutions

At the beginning of May, an 18-year-old computer enthusiast called Sven Jaschan was arrested by German Police in connection with writing and distributing the Sasser worm. Microsoft credited its reward scheme for the arrest but later reports suggested that the informants were also under suspicion. Sven is also believed to be connected with the Netsky worms:

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

http://www.newscientist.com/news/news.jsp?id=ns99994973

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

http://www.theregister.com/2004/05/19/anti_virus_bounty/

http://www.theregister.com/2004/05/18/sasser_informant_turns_suspect/

The other side of the Atlantic, the Royal Canadian Mounted Police (RCMP) have charged a 16-year-old youth in connection with the Randex worm.

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

At the same time, Taiwanese Police arrested a 30-year-old, Wang Ping-an, for creating and distributing a Trojan horse known as "Peep" which allowed remote access. Peep is claimed to have been used by Chinese hackers to access and destroy data on Taiwanese computers.

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

http://enterprise-linux-it.newsfactor.com/story.xhtml%3Fstory_title%3DVirus-Author-Busted-for-Making-a-Peep&story_id%3D24269&category%3Dnetsecurity

Near the end of May, the "Buffalo Spammer" was sentenced to a minimum of 3.5 years in prison for 14 counts of identity theft and forgery.

http://www.sophos.com/spaminfo/articles/spamslam.html

Passwords for Chocolate

A survey carried out for Infosecurity Europe revealed that 70% of people would disclose their password when offered chocolate! Over a third would disclose their password without being bribed. Unfortunately, there is no indication that the researchers tested that the passwords given actually worked, so we do not know the percentage of people willing to lie for chocolate:

http://news.bbc.co.uk/2/hi/technology/3639679.stm

Deloitte Publishes Global Security Survey

Deloitte's Global Financial Services Industry practice interviewed senior information technology executives of the top 100 global financial services organizations and found that 83% had had systems compromised during the past year.

http://www.deloitte.com/dtt/research/0,2310,sid%253D1013%2526cid%253D48978,00.html

Information Security Showcase

The Hong Kong Productivity Council help the Information Security Showcase on the 2nd to 4th of June. Highlight's included Dr. Jan Hruska's keynote speech, "Combating Spam and Viruses in Corporate Networks". Dr. Hruska, founder of Sophos PLC, gave a reasoned assessment of how we can expect these threats to develop.

Patrick Liu, Sophos' new technical support in Hong Kong, explained spammers tricks on day two of the event.

Mr. York Mok, the Chairman of the Hong Kong Internet Service Providers Association, explained his organisation's view of spam and Internet Content Rating.

Dr. Jan Hruska explains the growth of viruses

Microsoft Advises on Anti-Virus Protection

Microsoft has published "The Anti-Virus Defense-in-Depth Guide". A reasonable general introduction, but some inaccuracies have crept in, for example, on page 7, the definition of virus includes, "It may damage *hardware*, software or date." (my italics). Also, on page 9, rootkits are defined as "collections of software programs that a hacker can use to gain unauthorised remote access", neglecting their more significant role in concealing that a machine as been compromised, and maintaining the attacker's control.

The guide is inconveniently provided as an .MSI file that unpacks to a .PDF:

http://www.microsoft.com/downloads/details.aspx?FamilyId=F24A8CE3-63A4-45A1-97B6-3FEF52F63ABB&displaylang=en

YKAlert Upgraded with Chinese SMS Support

Yui Kee's alert service is under continual review to make it more useful and flexible. The latest improvement that is visible to end-users is the addition of the capability of sending Chinese alerts to mobile phones by SMS.

Allan Dyer, Chief Consultant of Yui Kee Computing, explained, "We previously had difficulty in the conversion of the character encoding as the data was transferred between applications. Although the operating system, programming language and SMS interface were all supposed to handle Unicode data, they did not interact as expected. Upgrading everything to the most recent versions improved the Unicode support and a few minor program changes fixed the problems."

The shots of the mobile screen and the corresponding alert in an email also illustrate YKAlert's ability to convert between GB2312 and Big5 encoding, as required.

Sign up for a free trial of YKAlert at: http://www.yuikee.com.hk/info-ctr/alert.html

Worm Targets Mobile Phones

Kaspersky Labs has detected Cabir (also known as EPOC.Cabir), the first network worm for mobile phones. Cabir infects telephones running Symbian OS (used by many Nokia telephones). It is thought that the "29a" group of virus writers, who specialise in creating "proof-of-concept" viruses, created the worm.

Detection of Cabir for F-Secure Anti-Virus for Symbian series 60 has been published at 11:55 on June 15th, 2004 in database build number 7.

Cabir is transmitted as a Symbian distribution file, but the file is disguised as Caribe Security Manager utility, part of the telephone security software. If the infected file is launched, the telephone screen will display the inscription "Caribe". Once the worm has penetrated the system it will be activated each time the phone is started. Cabir scans for all accessible phones using Bluetooth technology, and sends a copy of itself to the first one found. Symantec reports that this constant scanning for Bluetooth devices quickly drains the batteries of the infected phone.

More information:

http://www.kaspersky.com/news?id=149499226

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

http://www.sarc.com/avcenter/venc/data/epoc.cabir.html

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=EPOC_CABIR.A

Education Division News

Equal Opportunity Self-Learning Package Launched

"Equal Opportunities Begin at School" is a new, web based training programme designed specifically for teachers and comissioned jointly by the Equal Opportunities Commission and the Education and Manpower Bureau. Yui Kee developed the package, including the website, animations and videos.

Florence Chan of the EOC explains the package, assisted by Patrick Lee of Yui Kee, as Press photographers snap

The package allows teachers to learn at their own pace, and, once they have successfully completed the programme, they can download an "e-certificate" for their Continuing Professional Development scheme.

The package was launched at a well-attended press conference on 2 June 2004. The website can be accessed at: http://equaled.hkedcity.net/

Yui Kee Commissioned to Organise GIS Course

Yui Kee is organising a course titled, "Use of Geographic Information System in Learning and Teaching of Geography" for the Education and Manpower Bureau. Five classes, each with four three-hour sessions will be held from June to August.

The course aims to:

- Introduce the basic concepts and techniques in using GIS.
- Prepare teachers for the new curriculum.
- Equip the participants with practical GIS skills for teaching and ways to apply GIS in Junior Secondary, Certificate Level, A Level and Project Based Learning.

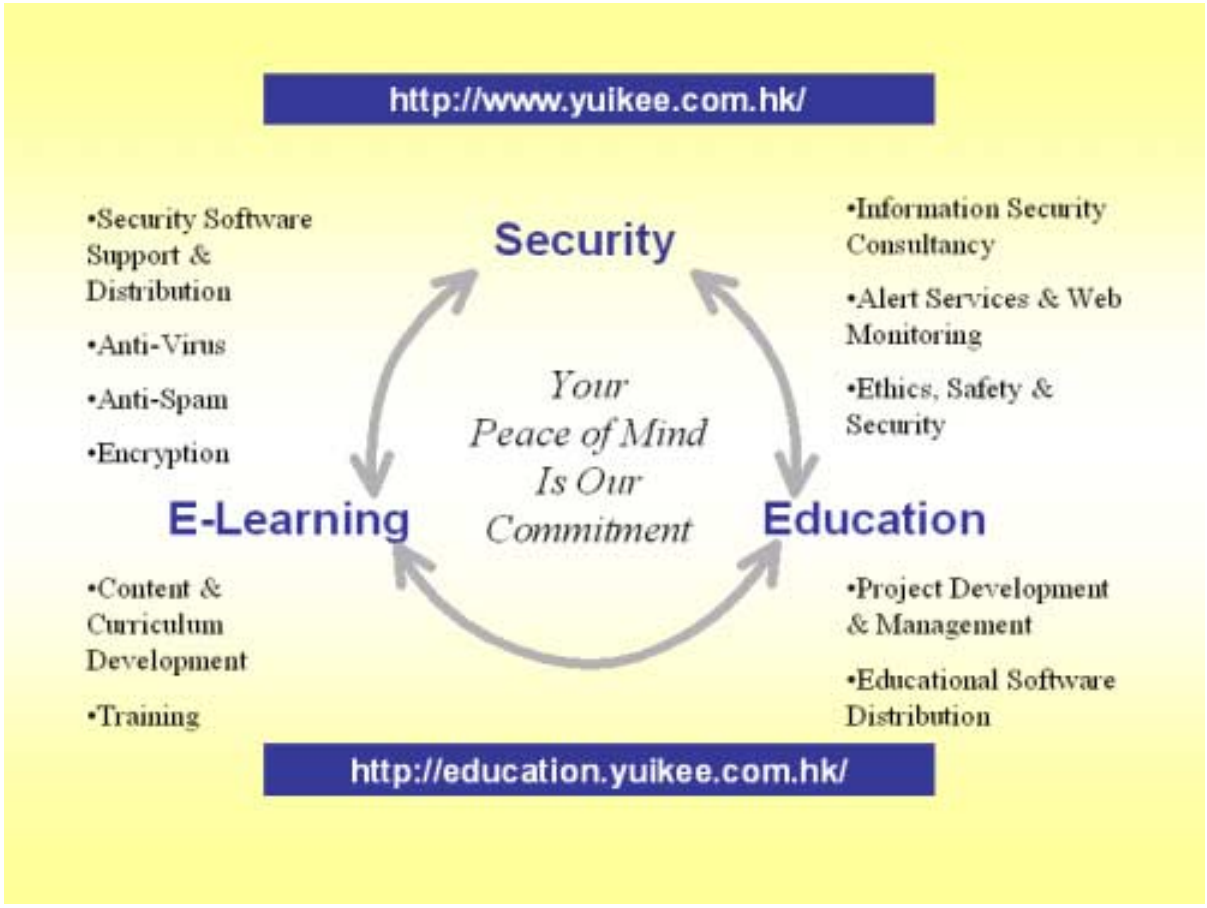
To design and teach the course, Yui Kee has recruited teachers who have pioneered the use of GIS in schools. Environmental System Research Institute Inc. (ESRI Inc.) China (Hong Kong) has provided the GIS software, and participants will receive a free evaluation license. ESRI has been the world leader in the GIS software industry for more than 30 years and ESRI China (HK) aims to bring state-of-the-art GIS and mapping software technology to the local community.

More information:

http://iclassroom.hkedcity.net/teacher/rtc-gis/

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/