Yui Kee Computing Ltd.

Newsletter

August 2001

Contents

Contents 1
Incident Update 1
Can I have Cheese on my Net Meltdown? 1
YKScan Popularity Soars 2
"The Emperor has No Clothes" - "Arrest that boy!" 2
AVAR Conference 2

Incident Update

W32.SirCam.Worm@mm is still the most common virus spreading in email. An important point to remember is that it includes a random document from the victim's desktop when sending itself, therefore, it may be revealing confidential documents. Also, the attached document might be very large and some uninfected users have effectively been DOS'ed because they have received so many large documents from victims. Because SirCam searches the victim's Temporary Internet Files for email addresses, this is likely to affect people whose email address is listed on popular sites.

Code Red has also continued to spread. Although the original variant is less common now, two new variants have been spreading. They exploit the same vulnerability as the original, and can be stopped by the same patch:

http://www.microsoft.com/technet/security/bulletin/ms01-033.asp

Some people have asked if anti-virus software can detect Code Red, the answer is not straightforward. Anti-Virus (AV) software searches files, but Code Red only exists as a process in memory and an exploit in an http session,. Therefore, AV software does not detect it directly. Intrusion Detection (IDS) software can be configured to detect the http sessions.

However, Code Red II does write a Trojan to the disk of the infected machine, which AV software can detect, for example, Symantec says, "Norton AntiVirus is able to detect an infection on the Web server by detecting the payload (Trojan component) of this worm as Trojan.VirtualRoot."

Can I have Cheese on my Net Meltdown?

Some security experts seem a little too keen on predicting the end of the Internet, for example, on 29 July Russ Cooper wrote, "This doesn't alter my prediction that we're going to experience a 'net meltdown on the 1st or 2nd, I believe far too many machines are vulnerable still and will likely be re-infected. "

What is a "net meltdown"? Sounds bad - brings up images of nuclear reactor meltdowns. That implies shutting down the damaged reactor, evacuating the population within a large radius and

permanently encasing it in concrete. I might be unobservant, but I didn't notice anyone doing that on 1 Aug. My Internet connection is still not covered with concrete.

Or maybe more like a cheese meltdown? Stops being firm and supportive, gets gooey round the edges, still tasty - but you might burn your tongue if you're not careful. That could describe the Internet any day of the week.

Cooper was right about "far too many machines", but the result was not comparable to a nuclear meltdown. Finding how large my firewall log was on the peak day was annoying, and we can cry over all that wasted bandwidth, but it is not a disaster. Information Security **is** important, but unjustified hype is not going to make anyone listen.

YKScan Popularity Soars

Sales of our YKScan email anti-virus service (powered by MessageLabs) have increased by over 100% so far in August.

Yui Kee can provide a 30-day no obligation free trial of YKScan to any customer interested in the service.

To request this trial or for more information on the YK service please contact our Customer Services department at:

- Tel: 2870 8553
- Fax: 2873 6164
- e-mail: offer@yuikee.com.hk

"The Emperor has No Clothes" - "Arrest that boy!"

I have previously commented on laws that fail to connect with the reality of Information Security and which are therefore "bad". The case of Dmitry Sklyarov and the US Digital Millennium Copyright Act (DMCA) is also in this category. The DMCA outlaws the sale of copyright protection circumvention technology. Sklyarov, a Russian, was arrested when visiting the USA to present a paper on flaws in the Adobe Systems's eBook Reader at the DefCon conference.

This is a complex case, with issues of jurisdiction (Sklyarov worked in Russia, where there is no similar law) and constitutional rights (does the DMCA restrict Fair Use rights?) but it has already had a detrimental effect. A Dutch researcher, Niels Ferguson, has decided not to publish his paper detailing security weaknesses in the HDCP content protection system because of fear of prosecution when he visits the USA. Therefore, the weaknesses are unlikely to be fixed before HDCP comes into common use, and criminals will have an easier task of pirating the supposedly protected works.

The parable of The Emperor With No Clothes illustrates the value of truth - nowadays, the truthful boy would find himself in an American jail for 25 years.

AVAR Conference

Three years ago a small group of Anti-Virus researchers met in Hong Kong and linked hands for a photograph. This was the inaugural event of the Association of anti-Virus Asia Researchers, an independent and not-for-profit organization that is oriented in Asia Pacific region. AVAR was the brainchild of Seiji Murakami. Murakami is a leader in Japanese Anti-Virus, developing the first local anti-virus in 1990. After his company was acquired by Network Associates in March 1997, Seiji founded Japan Computer Security Research center (JCSR) and Japan Computer Security Association (JCSA) in July 1997 in order to spend more time on promoting anti-virus activities. He also realized that there was a need for non-profit

and independent anti-virus organization in Asia, and contacted other researchers around the region to form AVAR. The mission of the AVAR is to prevent the spread and damage caused by computer virus, and to develop cooperative relationship among anti-virus researchers in Asia, and, with that in mind, AVAR has organised a growing annual conference. The second, in Korea attracted fifty participants, and the third, in Tokyo, one hundred and eighty. This year it is back in Hong Kong, at the New World Renaissance Hotel, on the 4 and 5 of December.

Widely Supported

The conference is being co-organised by the Information Security Special Interest Group (IS-SIG) of the Hong Kong Computer Society (HKCS). The Hong Kong Computer Society (http://www.hkcs.org.hk/) was founded in 1970 as a non-profit making professional body with the primary objective to promote the uses of IT in Hong Kong. The IS-SIG was established in June 2000 focuses research and discussion on security related subjects.

Many other organisations are backing the conference. Network Associates is the Platinum Sponsor, and the Information Technology Services Department (ITSD) of the Hong Kong Government is the Gold Sponsor. Symantec and Ahnlab are Silver sponsors and the Bronze Sponsors are Virus Buster (Hungary) and HAURI. Supporting Organisations include the Hong Kong Information Technology Federation, the Computing Services Centre of City University of Hong Kong, the Singapore Computer Emergency Response Team (SingCERT), Hong Kong CERT and Infocomm Development Authority of Singapore (IDA).

Government Involvement

One special feature of the AVAR conference has been government involvement, with previous years speakers including the Korean Information Security Agency (KISA), the Japanese Ministry of International Trade and Industry (MITI, now renamed to Ministry of Economy, Trade and Industry) the Infocomm Development Authority of Singapore and the Chinese Tianjin Quality Testing and Inspection Service. This year government topics will include Information Security Policy in Japan and the introduction of a National Computer Virus Emergency Response Center in China.

The Art of War

However, the techies will not feel left out - two papers look at the future of virus detection in new Office versions. Other papers consider using Intrusion Detection Systems for catching viruses; and the security of Java mobile phones. Sun Tze recommended knowing the enemy and yourself, so the papers on how Worms can be successful and how best to compare AV software are entirely appropriate.

For the Corporate Security Manager, the presentation on a major corporation's virus checking service, and the one on grassroots exchange of anti-virus information will be of special interest. Anti-Virus industry leaders will make the keynote and honorary speeches. However, as the Conference Chairman, I would not like to suggest that this short list of topics are the conference highlights because that judgement should be left to the delegates, I hope you will be among them. Full details of the programme and the participation details will be on the AVAR website: http://www.aavar.org/

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/