Yui Kee Computing Ltd.

Newsletter

November 2003

Contents

Incident Update

Yet another new variant in the Mimail family, W32/Mimail.J appeared on 17 November. It arrives in a message purporting to be from the PayPal online payment service, and attempts to fool the victim into revealing credit card details and other personal information.

On 25 November, a Trojan, called W32/Sysbug, was sent to large numbers of email addresses. The messages suggested the Trojan's executable contained sexy, personal pictures from someone called James to someone called Mary. If a recipient is fooled into launching the file, the Trojan installs itself, sends information about the victims computer to a website, and opens a backdoor on TCP port 5555.

Suspected Virus Writer Arrested

Spanish police have arrested a 23-year-old man in Madrid who is believed to be responsible for the W32/Raleka worm. It is the first arrest of a suspected virus writer in Spain, and the Spanish Interior Ministry has hailed the arrest as a "landmark".

http://www.sophos.com/virusinfo/articles/spanisharrest.html
http://www.theregister.com/content/69/34226.html

Bounty on Virus Writers

Microsoft has announced rewards of US$250,000 each for information leading to the conviction of the people who launched W32/Blaster.A and W32/Sobig worms on the Internet as part of its' US$5 million "Anti-Virus Reward Program". Microsoft notes that it is very difficult to trace virus writers by technical means, and intends that the rewards will encourage associates of virus writers to inform on their friends.

Anti-virus companies and other commentators have been cautious in predicting the outcome of the campaign. It may induce some interesting revelations, or it may just encourage more

paranoia and secrecy in an already paranoid group. Certainly, although several people have been arrested in connection with producing variants of the Blaster worm, the original author has kept a much lower profile.

An unfortunate (and unintended) side effect might be that misguided vigilantes attempt to break into anti-virus companies. After all, it is a well-known Urban Myth that anti-virus companies write viruses, as seen in this recent Dilbert cartoon: http://www.unitedmedia.com/comics/dilbert/archive/dilbert-20031129.html, so what better place to look for incriminating evidence?

Recent attempts to use large bounties to capture wanted persons in Iraq have had minimal effect; perhaps Microsoft will publish a new version of Solitaire?

More information:

http://www.theregister.com/content/56/33866.html
http://www.idg.com.hk/cw/readstory.asp?aid=20031106001
http://www.sophos.com/virusinfo/articles/virusbounty.html

Critical Bug in Windows Workstation Service

Microsoft Security Bulletin MS03-049 announces a new Buffer Overrun in the Workstation Service affecting Windows 2000 and Windows XP. Blocking access to UDP ports 138, 139, 445 and TCP ports 138, 139, 445, or disabling the Workstation service can mitigate the bug. Microsoft notes that disabling the Workstation service will prevent access to shared file and print resources, so it should only be used on stand-alone systems. Installing the patches is, of course, the preferred method of dealing with the problem.

More information:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-049.asp
http://www.cert.org/advisories/CA-2003-28.html

Microsoft Attacks Linux Security

Microsoft is taking a long, hard look at Linux security. Steve Ballmer is quoted saying, "In the first 150 days of Windows 2000 we had seventeen critical vulnerabilities... The first 150 days of Red Hat 6 -- go check the number, just go check the number. It's five to ten times higher than what we are showing" at the Gartner Fall Symposium.

The figures might have come from a strategy, called "Days of Risk", that Microsoft denies exists. According to reports, the Days of Risk strategy measures the number of days it takes programmers to release a public patch after a vulnerability is revealed and Microsoft intends to prove that, on average, Windows poses less of a security risk than Linux.

Regardless of who is behind the Days of Risk strategy, the question remains that, if Steve Ballmer has really made security a top priority, why does he think that saying, basically, "Your security is worse than mine!" is going to have a positive effect?

More information:

http://www.idg.com.hk/cw/readstory.asp?aid=20031112002
http://www.groklaw.net/article.php?story=20031022014413296
http://www.microsoft.com/presspass/exec/steve/2003/10-21Gartner.asp
http://www.techworld.com/news/index.cfm?fuseaction=displaynews&NewsID=651
http://www.techworld.com/news/index.cfm?fuseaction=displaynews&NewsID=643

"ISO 17799 for Obese Couch Potatoes"?

In response to a question from the CIO of Wendy's International Inc., Steven Cooper, the new CIO at the U.S. Department of Homeland Security suggested that even fast-food restaurants could help disseminate information by putting cyber security pamphlets on their counters.

Obviously, we should consider the local culture before introducing similar measures in Hong Kong. Would you find it more useful to receive "Critical Updates for Windows XP" with your Dim Sum selection form, or as a wrapper for your fish balls from the illegal street hawker?

More information:

http://www.idg.com.hk/cw/readstory.asp?aid=20031114004
http://seclists.org/lists/isn/2003/Nov/0059.html

Fooling Fingerprint Readers Easier than Ever

In a letter to Crypto-Gram, Ton van der Putte has reported that duplicating fingerprints now is even easier than ten years ago, when he first experimented with the techniques. He concludes that the combination of an identity card and a biometric fingerprint sensor is less secure than using an identity card alone, because the biometric provides a false sense of security. The developers and users of the Hong Kong SmartID card would do well to take note.

http://www.schneier.com/crypto-gram-0311.html

U.S.A. Prepares to Legalise Spam

On 22 November the U.S. House of Representatives passed the CAN-SPAM ("Controlling the Assault of Non-Solicited Pornography and Marketing") bill, the Senate looks set to follow, and it is expected that the President will sign the bill on 1 January 2004.

The bill has some good features: it makes the use of open proxies or resource misappropriation, or the use of false headers illegal.

Unfortunately, the bill adopts an opt-out approach - messages are legal if they are clearly marked as advertisements, contain a U.S. postal address and have an unsubscribe link at the bottom. Does anyone know how many U.S.A. companies there are, and how long it would take an average user to read a single message from each one, and respond with an unsubscribe request?

Various companies and organisations have criticised the bill.

More information:

http://www.sophos.com/virusinfo/articles/usspamlaws.html
http://www.theregister.com/content/55/34164.html
http://www.spamhaus.org/news.lasso?article=150

Cases of Spam Rage

Charles T Booher, 44, was arrested on 20 November for threatening to torture and kill employees of an unnamed Canadian company that he believed was responsible for sending him an unrelenting stream of email featuring penis enlargement adverts.

In an unrelated incident, two weblogs, known for their satirical pranks, launched a sustained DDoS attack against the US spam firm Customerblast.com. The weblogs were soon hit by massive retaliatory DDoS attacks, and the weblogs retaliated I turn with a second wave of attacks. One of the participants in the scrap says he was cut off by his ISP and now faces ‘legal action’.

These attacks on spammers are clearly illegal, but they demonstrate that the growing problem of spam is pushing people to breaking point, and beyond. Effective legal control is required.

More information:

http://www.sophos.com/virusinfo/articles/spamrage.html
http://www.theregister.com/content/55/34146.html

Nachi infects ATMs

ATM-maker Diebold has confirmed that W32/Nachi infected its' machines at two financial institutions last August, and claims it is the first confirmed case of malicious code penetrating cash machines. W32/Nachi uses the same RPC DCOM vulnerability as the W32/Blaster worm to spread, and the machines infected were somehow missed in Diebold's normal patching procedures.

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