Yui Kee Computing Ltd.

Newsletter

November 2005

Contents

Incident Update

- Tue Sep 13 17:16:36 2005 CA: Win32.Mydoom.O Medium
- Mon Sep 19 23:31:24 2005 FSC: Bagle variant spammed as TEXT.EXE 2
- Thu Oct 6 11:01:19 2005 NAI: W32/Sober.r@MM Medium
- Thu Oct 6 15:46:26 2005 CA: Sober.P Medium
- Thu Oct 6 16:01:53 2005 CA: Win32.Sober.P Medium
- Thu Oct 6 19:01:21 2005 FSC: Sober seeded worldwide 2
- Tue Oct 11 21:01:19 2005 TREND: WORM_SOBER.AC Medium
- Thu Nov 3 08:46:27 2005 CA: Glieder.CC Medium
- Wed Nov 16 16:02:06 2005 FSC: Four new Sober variants spammed in 24 hours 2
- Mon Nov 22 22:31:22 2005 FSC: ALERT: Sober sending "warnings" from FBI & CIA 1
- Mon Nov 28 17:31:22 2005 TREND: WORM_MYTOB.MX Medium
- Mon Nov 28 17:31:22 2005 SARC: W32.Sober.X@mm L3
- Mon Nov 28 17:31:22 2005 NAI: W32/Sober@MM!M681 Medium
- Mon Nov 28 17:31:22 2005 CA: Sober.W Medium
- Mon Nov 28 17:31:22 2005 CA: Win32.Sober.W Medium

Sober.Y Outbreak

F-Secure issued its first Radar Level 1 alert for many months in response to the spread of Sober.Y. Sober.Y is written in Visual Basic and sends e-mail messages with English and German texts and its file attached. The attachment is a ZIP archive containing the worm's executable. Some of the email messages pretend to be from the CIA, FBI, or the German equivalent the BKA.

More information:

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

http://www.f-secure.com/weblog/archives/archive-112005.html#00000711

http://www.f-secure.com/weblog/archives/archive-112005.html#00000715

AVAR 2005 Conference

The 8th Association of Anti-Virus Asia Researchers annual conference was held in Tianjin, China on th 17th and 18th of November. The conference theme was "Wired to Wireless, Hacker to Cyber-criminal".

Speakers from around the world reported on the developments they are seeing, how we can understand and prevent new threats and the technologies involved. Chen Mingqi reported on CNCERT/CC's response to botnets. Eugene Kaspersky addressed the challenges we face. Vesselin Bontchev and Kyu-beom Hwang reported on very different mobile threats. Richard Marko, Andrew Lee and Gabor Szappanos reported on their varied efforts to capture malware in the wild.

The End of the Virus Problem?

A trend highlighted by many speakers is that we are seeing a clear move away from self-replicating malware. Over 80% of the new malware is not self-replicating, we are seeing thousands of variants of Trojans, there are very few massive virus outbreaks (see Sober.Y Outbreak, above, for the exception) but a host of botnets. Large, blended threats have been replaced by modular malware that downloads new components as required.

This is related to the increased criminality of malware authors: a large outbreak attracts attention and arrest, as Jeffrey Lee Parson and Sven Jaschan discovered. But a large outbreak is unnecessary for a successful crime: it takes time to use stolen credit card details, so gathering them in small batches, and frequently changing the Trojans used to collect them, makes sense. Attacks like a DDoS also do not need massive numbers; a botnet of a few thousand machines can overwhelm almost any site.

A virus can easily spread out-of-control; a trojan is therefore a preferable for criminals. Viruses are therefore fading in importance because even the criminals have realised that self-replicating code is a bad idea.

The Cutting Edge of Biometrics

A 15 year old US boy conceived by an anonymous sperm donation has traced his father by using the Internet, including an online genealogy DNA-testing service.

This demonstrates the power of biometrics: identification of an individual; but also its weakness: the same online data makes biometric information public, and therefore of very limited use in authentication. There is a tendency to think of a biometric as a "shared secret" when, in reality, it is a difficult-to-forge identifier.

More information:

http://www.newscientist.com/article.ns?id=mg18825244.200

Sony Rootkit

A quick summary for readers that have been asleep for the last month:

Sometime in March 2005, Sony BMG began distributing music CDs that were "protected" using software from First 4 Internet Ltd. The software installed hidden software and made system changes to prevent removal after the user accepted a (typically verbose and unclear) EULA. The software would also hide any files or registry keys with a name starting with the string "sys" – a feature that has now been taken advantage of by malware authors. Attempting to uninstall the software might cripple windows.

After the initial reports on the software at the beginning of November there was a lot of discussion, the consensus being that Sony BMG had greatly overstepped the bounds of acceptable behaviour. Now most anti-virus companies have descriptions and disinfection tools for the rootkit.

Sony is now facing lawsuits in the USA, and the rootkit may infringe copyright held by Jon Johansen.

Unauthorised modification of computer programs or data is a crime in Hong Kong. If any of these rootkit CDs have been distributed in Hong Kong, then Sony BMG should face criminal prosecution under the Computer Crimes Ordinance.

Don't miss F-Secure's T-shirt.

More information:

Description: http://www.europe.f-secure.com/v-descs/xcp_drm.shtml

http://www.theregister.com/2005/11/03/secfocus_drm/

http://www.theregister.com/2005/11/01/sony_rootkit_drm/

http://www.theregister.com/2005/11/10/sony_drm_trojan/

http://www.theregister.com/2005/11/10/sony_drm_unmasked/

http://www.theregister.com/2005/11/10/sony_sued_for_rootkit/

http://www.theregister.com/2005/11/18/sony_copyright_infringement/

http://www.theregister.com/2005/11/21/gaffer_tape_trips_up_sony_drm/

http://www.schneier.com/blog/archives/2005/11/sony_secretly_i_1.html

http://www.schneier.com/blog/archives/2005/11/more_on_sonys_d.html

Description: http://www.sophos.com/virusinfo/analyses/trojrkprocfam.html

Disinfection: http://www.sophos.com/support/disinfection/rkprf.html

http://www.sophos.com/pressoffice/news/articles/2005/11/stinxe.html

http://www.sophos.com/pressoffice/news/articles/2005/11/sonydrmpoll.html

http://www.f-secure.com/weblog/archives/archive-112005.html#00000714

http://www.f-secure.com/weblog/archives/archive-112005.html#00000709

http://xforce.iss.net/xforce/alerts/id/208

http://www.f-secure.com/weblog/archives/archive-112005.html#00000703

http://www.theinquirer.net/?article=27649

http://www.f-secure.com/weblog/archives/archive-112005.html#00000701

http://www.f-secure.com/weblog/archives/archive-112005.html#00000700

http://www.f-secure.com/weblog/archives/archive-112005.html#00000696

http://www.f-secure.com/weblog/archives/archive-112005.html#00000695

http://www.f-secure.com/weblog/archives/archive-112005.html#00000694

http://www.f-secure.com/weblog/archives/archive-112005.html#00000691

Password Cracking

The big joke is that the site users a username and password to authenticate paying customers… do they offer a hash table to crack those?

http://www.theregister.com/2005/11/10/password_hashes/

Charitable Spammers?

Have spammers given up their nefarious, misleading practices and dedicated themselves to good? A recent message said:

```
From:  "Alta Berger" <          @      .com>
To:<     @      .com.hk>
Subject:   Re: your web site is interesting...
Date sent: Mon, 28 Nov 2005 23:40:28 +0600
Send reply to: "Alta Berger"     @   .com

this is your non-profit/charity contact email address right?

If so... we will email your web site to 2,500,000 opt-in emails for
free
```

It says the addresses are opt-in, so that is OK and legitimate, right? The message continues on about the worthy charities they have contributed to in the last year. Finally! An ethical, generous spammer!

But wait, if they are using an opt-in list, why did I receive it? Why did they think my address was a charity contact address? What is their real agenda? At the end, the message says,

```
if this is not a non-profit/charity contact email address and/or you
are not interested in our occassional non-commercial,
non-transactional, non-cost, non-relationship, courtesy emailings we
perform for various nonprofits and charities, delist at:
http://                    .    .     .com
```

This looks like the standard "tell us your address is working" ploy. The offer to charities could be genuine… with a hidden catch. Spammers are facing increasing pressure from proposed legislation, but maybe they can blunt the laws by claiming spam has beneficial value to society. Or maybe there plan is to encourage legitimate charities to spam so that the spammers fraudulent "charity appeals" appear more plausible.

Wise charities should avoid spamming: they will annoy millions of potential donors who might have responded favourably to a different approach.

Cyber-Criminals bigger threat than Cyber-Terrorists?

Bruce Schneier, speaking after the SANS Institute released its latest security report at an event in London argued that talk of cyber-terrorism could have a damaging effect on IT security. However, at the same event, NISCC director Roger Cummings claimed that foreign governments are the primary threat to the UK's critical infrastructure.

More information:

http://software.silicon.com/security/0,39024655,39154523,00.htm

Phishing by SMS

Criminals in Beijing are using SMS messages to trick people into revealing their credit card details.

More information:

http://www.chinadaily.com.cn/english/doc/2005-10/12/content_484196.htm

Cryptography for Kids

The friendly face of the NSA: http://www.nsa.gov/kids/

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/