Yui Kee Computing Ltd.

Newsletter

April 2008

Contents

Contents 1
Impersonating the German Interior Minister 1
A Million Viruses, Advanced Rootkits and Mobile Ransomware 2
    Drive-by downloads 2
    Advanced rootkit emerges 3
    First mobile ransom Trojan 3
    More mobile trouble 4
RAPIL Technology Catches SearchStorageAsia 4
Going for Gold: Advanced Fee Fraud Spam with an Olympic Flavour 5
AVAR 2008 Call For Papers 5
Pen. Testing Microsoft 6

Impersonating the German Interior Minister

<web-link for this article>

The Chaos Computer Club has published a fingerprint of the German Interior Minister, Wolfgang Schauble in their magazine Die Datenschleuder in an attempt to point out and publicise the insecurities of biometrics. Schauble is a proponent of fingerprint and other biometric technology, and has announced a new electronic passport that stores individuals' fingerprints on an RFID chip, saying the biometric would, "prevent authentic passports from being misused by unauthorized persons who happen to look like the person in the passport photo.".

The printed version of the magazine contains an ink image of a fingerprint, believed to be Schauble's right index finger, captured from a water glass he used while participating in an event at the University of Humboldt in Berlin, and the same fingerprint on a plastic film. The film can be covertly affixed to an imposter's finger to fool fingerprint readers.

Biometrics in any form are an identifiers, they are not secret.

08th April 2008

No2ID and Privacy International have offered a £1,000 reward for the fingerprints of Gordon Brown's and Jacqui Smith's (Britain's Prime Minister and Home Secretary, respectively) fingerprints. The fingerprints should be "lawfully obtained" and provided with corroborating evidence. The groups intend to make the fingerprints publicly available, if they are obtained.

No2ID National Coordinator Phil Booth directly challenged the UK Government's biometric ID scheme saying, "If they truly believe that the ID scheme will 'secure' their personal identities, the best thing Gordon Brown and Jacqui Smith could do would be to surrender their OWN fingerprints and get us to donate the grand to a charity of their choice. Failing to surrender their fingerprints could be seen as tacit acknowledgment that they have no real faith in their own scheme."

More Information

Get your German interior minister's fingerprint here
Authentication Pitfalls
Die Datenschleuder
Wanted: Gordon Brown's fingerprints, £1,000 reward
Privacy International and NO2ID's Wanted Poster
Wanted Poster! A call for the UK Prime Minister's fingerprints
Wolfgang Schauble's fingerprint

A Million Viruses, Advanced Rootkits and Mobile Ransomware

<web-link for this article>

F-Secure has released its Quarterly Security Wrap-up for the first quarter of 2008, predicting that the number of viruses will reach a million by the end of the year and reporting various emerging malware threats.

The amount of new malware has never been higher. F-Secure's labs are receiving an average of 25,000 malware samples every day, seven days a week. If this trend continues, the total number of viruses and Trojans will pass the one million mark by the end of 2008.

While there are more viruses being created than ever before, people often actually report seeing less of them. One reason behind this illusion is that malware authors are once again changing their tactics in how to infect our computers. A year or two ago, most malware was spread via e-mail attachments, which resulted in mass outbreaks like Bagle, Mydoom and Warezov. Nowadays sending .EXE attachments in e-mail doesn't work so well for the criminals because almost every company and organization is filtering out such risky attachments from their e-mail traffic.

The criminals' new preferred way of spreading malware is by drive-by downloads on the Web. These attacks often still start with an e-mail spam run but the attachment in the e-mail has been replaced by a web link, which takes you to the malicious web site. So instead of getting infected over SMTP, you get infected over HTTP.

Drive-by downloads

Infection by a drive-by download can happen automatically just by visiting a web site, unless you have a fully patched operating system, browser and browser plug-ins. Unfortunately, most people have some vulnerabilities in their systems. Infection can also take place when you are fooled into manually clicking on a download and running a program from the web page that contains the malware.

There are several methods criminals use to gather traffic to these websites. A common approach is to launch an e-mail spam campaign containing messages that tempt people to click on a link. Messages like "There is a video of you on YouTube", or "You have received a greeting card", or "Thank you for your order" have been popular baits.

Another method used by criminals is to create many web pages with thousands of different keywords which are indexed by Google, and then simply wait for people to visit these sites. So when you do a search for something innocuous like "knitting mittens" (as a random example), and click on a search result that looks just like all the others, you are actually getting your computer infected. Typically, an infection by an automatic exploit happens without you realizing it or seeing anything strange on the computer screen.

The third method of distributing malware involves the criminals hacking into existing high profile, high traffic web sites. Unlike the joke defacements that some hackers played on the

front pages of prominent web sites in the past, today's criminal hackers don't change the front page at all. They simply insert a line of javascript on the front page which uses an exploit to infect your machine when you go there. Everything works and looks as normal.

This has happened to the web sites of some popular magazines which can have a million users every single day. People trust sites that are part of their daily routine, and they couldn't suspect that anything bad could happen when they go there.

Another vector for drive-by downloads are infiltrated ad networks. There is more and more advertising displayed on high-profile websites. By infiltrating the ad networks, the criminals don't have to hack a site but their exploit code will still be shown to millions of users, often without the knowledge of the webmaster of those sites. Examples of where this has happened include TV4.se, Expedia, NHL, and MLB.

It is important to be aware of this shift from SMTP to HTTP infections, which can be exploited by the criminals in many ways. Companies often measure their risk of getting infected by looking at the amount of stopped attachments at their e-mail gateway. Those numbers are definitely going down, but the actual risk of getting infected probably isn't.

Individuals and companies should therefore be scanning their web traffic for malware - as well as filtering their FTP traffic. In parallel to the switch from SMTP to HTTP as a way of spreading malware, there are more and more malicious e-mails that link to malware via FTP links.

Advanced rootkit emerges

A MBR rootkit - known as Mebroot - is probably the stealthiest recent malware F-Secure has observed, and has so far been distributed by drive-by downloads.

Mebroot replaces the infected system's Master Boot Record (MBR), which is the first physical sector of the hard drive and contains the first code loaded and executed from the drive during the boot process. It keeps the amount of system modifications to a minimum and is very challenging to detect from within the infected system.

MBR viruses used to be the most common form of viruses at the time of the DOS operating system about 15 years ago. Recently there were academic papers published in conferences discussing whether this kind of MBR stealth could ever happen in the age of Windows. We have been very surprised to see it happening for real now in 2008.

This means that the criminals have both the funds and the high level expertise to develop such complex attacks. They have succeeded in developing code that loads from the boot sector of the hard drive, stays alive while Windows boots up, then loads parts of itself and injects to the operating system when Windows is up and running, and manages to hide all this very effectively.

We are likely to see this technique being used by quite a variety of malware. These first MBR rootkits are banking Trojans targeting several online banks, where the criminals are clearly seeing an opportunity to make a return on their investment.

First mobile ransom Trojan

Making money is what today's malware is all about and the first ransom Trojans for smartphones have been found in China. We have already seen similar Trojans on the PC side before which infect your computer, take your data 'hostage' or somehow disrupt your computer's capabilities, and then offer to restore everything back to normal if you pay out the ransom money. Typically, the ransom Trojan first encrypts your hard drive and then sends you a password after you have sent money to the criminals via an online money transfer system.

In the case of Kiazha, the first smartphone ransom Trojan, you get infected by downloading a shareware lookalike program on your phone, which then drops several known older viruses on your phone. Next it sends a message explaining that you can only get the phone fixed by transferring the equivalent of seven dollars to the attackers through an online payment system. Today's smartphones are so important to many people that they are prepared to pay a ransom to get back their phonebook, calendar and mobile emails, so we might well be seeing much more of this type of malware in the future.

More mobile trouble

The Beselo worms spread via MMS and Bluetooth by using a novel form of social engineering to trick users into installing an incoming SIS application installation file. What makes Beselo interesting is that instead of a standard SIS extension, the Beselo family uses common media file extensions. This leads the recipient to believe that he or she is receiving a picture or sound file instead of a Symbian application. The recipient is then far more likely to answer "yes" to any questions the phone prompts after clicking on such an incoming file.

The filenames used by Beselo are beauty.jpg, sex.mp3, and love.rm. So if you have a Symbian S60 phone and receive a media file, answer "no" to any installation prompt that appears when trying to open the file. There is no reason for any image file to ask installation questions on the Symbian platform, so any image or sound file that does something else than play immediately is definitely not what it claims to be.

Beselo worms are compiled for S60 2nd Edition phones. Attempting to open the file on a 3rd Edition phone will probably cause an error message rather than an installation prompt.

HatiHati.A is another troublemaker, a worm-like application that spreads via MMC cards. Once the worm has copied itself to a new device, it starts sending SMS messages to a predefined number which can prove very expensive.

Both PC and smart phone users can protect themselves by using an up-to-date security services from well known vendors.

More Information

F-Secure Quarterly Security Wrap-up for the first quarter of 2008

RAPIL Technology Catches SearchStorageAsia

<web-link for this article>

Significantly, Sophos chose to announce groundbreaking technology - RAPIL (Recognition and Analysis of Potentially Intruding Lifeforms) - on the first day of this month. Apparently, the significance was lost on SearchStorageAsia, who chose to re-publish the story on the 3rd of April.

It seems that the journalists at SearchStorageAsia failed to pick up on the more improbable aspects of the technology and the story:

- ✓ The acronym is an anagram
- ✓ The version number is v0.401
- ✓ "able to produce a real-time forensic analysis of a PC or Mac user's facial features to determine if they exhibit any characteristics commonly associated with hackers"
- ✓ "assess the facial characteristics of computer users, and cross-references them against features typically found in cybercriminals"
- ✓ “Being able to stop the hackers before they even get a chance to write their malware, let alone spread it, is a breakthrough"

You can help Sophos develop the technology by uploading your photos with and without "face obfuscation".

More Information

RAPIL - a slap in the face for hackers and virus writers
Sophos facial recognition technology hopes to identify hackers by their look alone
flickr: Sophos RAPIL: A slap in the face for hackers and virus writers

Going for Gold: Advanced Fee Fraud Spam with an Olympic Flavour

<web-link for this article>

Cheating people out of their money is a highly-competitive "industry" where innovation is essential to keep ahead, so it is hardly surprising that spammers are now taking advantage of the Beijing Olympics. An example received is basically a variant of common lottery fraud messages, saying that the recipient's email address was "selected" to receive five tickets to the entire Olympics, with hotel and flights included, to a total of half a million US dollars. Naturally, the chances of someone receiving the promised prize are rather less than the chances of the development of porcine aviation.

The message was received from an IP address in Madrid, Spain, but the contact email address was in the yahoo.com.cn domain, and the contact phone number had a +86 (Chinese) country code.

AVAR 2008 Call For Papers

<web-link for this article>

The Eleventh Association of anti-Virus Asia Researchers International Conference will be held at the Taj Palace Hotel, New Delhi on 10th-12th December 2008. President of AVAR, Allan Dyer, said, "This is probably the first time an International Anti-Virus conference has been held in India. I am delighted that Kailash Katkar and Quick Heal Technologies Pvt. Ltd. are dedicating their time and resources to hosting the conference and I am looking forward to meeting everyone in New Delhi."

The AVAR 2008 Conference Committee is now seeking submissions from those wishing to present at the AVAR 2008 Conference to be held on 10-12 December 2008 in New Delhi, India.

This call for papers invites the submission of full papers and abstracts on all subjects relevant to anti-malware and anti-spam that may include, but are not restricted to:

- ✓ Analysis of malware trends
- ✓ Non-Windows malware
- ✓ Botnets
- ✓ Fast-flux network threats
- ✓ Rootkits
- ✓ The roles of ISPs, ASN's
- ✓ Wireless security
- ✓ Honeypot
- ✓ Sandbox
- ✓ Unpackers/emulators
- ✓ Reverse engineering

- ✓ Vulnerabilities and Software Bugs
- ✓ Cyber Terrorism
- ✓ Spam and Phishing
- ✓ Mobile threats
- ✓ Online Games malware
- ✓ Attack scenarios - how to handle them
- ✓ Obfuscation methods
- ✓ Network-based malware control (IDS/IPS)

Speakers from government, defense, ISPs, CERTs, universities, the commercial sector, and anywhere the security of networked computers is involved are encouraged to submit.

Authors wishing to give a presentation must provide the following information to the AVAR 2008 Conference Organizing Committee on or before 15th July 2008.

- ✓ name and affiliation
- ✓ contact email and physical address
- ✓ a short biography of qualification and/or experience(100 words)
- ✓ paper title
- ✓ abstract (maximum 500 words)

The above information should be submitted by e-mail in Plain text, Rich text or Adobe PDF format to avar2008@aavar.org.

Following the close of the call for papers all submissions will be anonymized before being reviewed by a selection committee. Authors will be notified of the status of their paper by email. Authors are required to submit the completed papers on selection no later than 30th September 2008.

Presentations must not exceed 40 minutes including 5 minutes for questions.

The official language of the conference is English. Speakers should indicate their audio-visual and computing equipment requirements for presentation of papers.

The speakers are exempted from the conference registration fee and are entitled to attend all sessions of the two-day conference, lunch on 11-12 December 2008 and banquet on 11 December 2008.

AVAR 2008 Conference Organizing Committee also invites suggestions for particular speakers you would like to hear from at AVAR 2008 Conference. Please send speaker nominations, along with details of why you would like to hear the speaker to avar2008@aavar.org.

More Information

AVAR 2008 New Delhi
AVAR 2008 New Delhi Call For Papers
Tenth AVAR Conference in Seoul Discusses Changing Threats

Pen. Testing Microsoft

<web-link for this article>

Microsoft security strategist Katie Moussouris told delegates at the the ToorCon security conference in Seattle that Microsoft will not to sue or press charges against ethical hackers who responsibly find security flaws in its online services. This has been reported as the first time a

major company has made such a pledge. However, Microsoft's manager for security response communication, Bill Sisk later claimed this was not a change in position, "Microsoft did not announce anything new at ToorCon Seattle regarding its position on responsible disclosure, but we did mention our industry leading online services acknowledgment, which went public in July of 2007. Because we will not pursue legal action against researchers who report vulnerabilities to us responsibly, we hope to encourage those who want to help us protect customers to feel free to do so without fear of repercussions."

Regardless of whether this was the first announcement of the policy, this is the first time the policy has attracted media attention. Cautious white hats will want to check the details of the policy before launching their attacks. The cynical might speculate why Microsoft has no budget for professional penetration testing.

More Information

Microsoft: Finding flaws on our website is OK
Microsoft Picks New Song for Hacker Slow Dance
Microsoft denies its pledge not to sue security researchers is new

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: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/