Yui Kee Computing Ltd.

Newsletter

August 2007

Contents

Spam Arms Race set for Next Escalation

<web-link for this article>

An interesting paper at USENIX 2007 (Spamscatter: Characterizing Internet Scam Hosting Infrastructure) that analyses spam and the servers involved in hosting their scams has prompted exaggerated claims that spam's Achilles' Heel has been found in some of the computing press. Unfortunately, we face intelligent adversaries who can be expected to quickly change their strategy.

The paper demonstrates the *spamscatter* technique for identifying scam infrastructure, using approximate image comparison to bypass obfuscation techniques used by spammers and thus identify clusters of servers associated with individual campaigns. The results of using the technique show that, while spammers use large numbers of spam relays to send messages, most spam campaigns use just one server as the further contact point for the scam, and, in many cases, multiple campaigns share one host. The authors suggest, "This practice provides a potentially convenient single point for network-based interdiction either via IP blacklisting or network filtering". Furthermore, claims journalist Matthew Broersmaas, as it is the scam that collects money from the customers/victims, this interdiction cuts the economic lifeblood for the spam, suggesting that spam might be combated in this way.

Unfortunately, the most likely result of IP blacklisting or network filtering the scam hosts will be the development of distributed, fault-tolerant clusters of scam servers. We know the bad guys have the technical capability, they have already used it for sending spam, they have just not had a reason to bother before now.

A better approach might be to use these techniques to trace the scammers and put them behind bars. Ultimately, they might still start using distributed clusters, but jail-time is a lot stronger deterrent than loosing a server; it could really change the criminal's view of the risk/benefit trade-off.

More Information

Study finds spam's Achilles heel
UCSD Computer Scientists Shed Light on Internet Scams
UC-San Diego computer scientists shed light on Internet scam
Spamscatter: Characterizing Internet Scam Hosting Infrastructure; David S. Anderson et al
UC San Diego Computer Scientists Shed Light on Internet Scams
UC-San Diego computer scientists shed light on Internet scams
Computer scientists shed light on Internet Scams
Study finds weak link in spam business
Study Finds Spam's Achilles Heel

Submitting Virus Samples

<web-link for this article>

We recently received an email that started, "As incredible as it meight be, there is no simple way to report a new virus to either of the major vendors (nod32, symantec, mcaffee, etc, etc). So i just found your email on the wild list." This is incredible, because we know all the major vendors provide ways for people to submit samples. Unfortunately, the message contained a brief description of what the supposed virus did, but no sample.

So, let us clarify how to report a possible new virus to an anti-virus developer in the most effective way:

1. **Have you updated your anti-virus software?** Check whether the latest available update for your anti-virus software detects and/or disinfects the suspected virus.
2. **You need to provide a sample.** The developer examines new viruses (or other malware) to understand how they work, how to detect them and how to remove them. A report of a new virus without a sample is almost useless, it will not result in a virus definition that can detect and remove the virus. If you do not know how to collect a sample, contact your technical support or your anti-virus vendor's technical support, they can help you.
3. **Choose a report method**. Some anti-virus software includes an integrated feature to help you submit samples, and all the major vendors have instructions on their websites (see links below).
4. **Don't make multiple submissions**. The major anti-virus developers all share virus samples, because they recognise that viruses are like a public health issue, and that, by giving samples to their commercial competitors, the customers they are protecting are their own. Submit your sample to your own anti-virus vendor, if it is a new virus, they will send it to the others.
5. **Include relevant information**. Say why you suspect these files, what you observed when the incident occurred, and your system information: operating system and version, anti-virus software type, version and virus definitions date/version, and the name and version of any software that seemed to be involved. Include the report of your anti-virus software, if there is one.
6. **Don't Panic**.

Is that clear? Here are those submission links:

More Information

F-Secure Support pages: How to send samples
Sophos: Sample Submission Form
Symantec Security Response: Submit Virus Samples
Trend Micro - Submission Wizard

McAfee Threat Center: Submit a Sample

German Government Shoots Self in Anti-Hacking Foot

<web-link for this article>

Ignoring warnings about the consequences from security experts, and the example of the British Government in amending the Police and Justice Bill, the German Government has brought §202c StGB into force, criminalising the creation and distribution of a wide range of security-related tools. Possession or use of dual-use tools, such as nmap or nessus, will be punished with up to one year in jail, and a fine.

Apparently, possession and use of such tools with the intent only to use them where authorised will be illegal, making it difficult for German System Administrators to test whether their systems are vulnerable.

Developers of such tools, and researchers who wish to publish exploits will also fall foul of the law, and there have been several announcements concerning this:

The KisMAC (wireless network discovery tool) developers are moving to the Netherlands.

Phenoelit (developers of a number of interesting tools) have closed their German site, though their US site remains open.

Stefan Esser, (PHP Security researcher), has withdrawn all of the exploit code that originally accompanied his Month of PHP Bugs project.

So, those that can will move their operations out of Germany. Some researchers may stop, a blow to security research. Testing the security of a system in Germany legally will be tricky, and the criminals will still be able to target German systems from outside. It is difficult to see a positive effect of this law.

More Information

Germany enacts 'anti-hacker' law
German Security Professionals in the Mist
Germany says: Good-bye KisMAC!
http://blog.php-security.org/archives/91-MOPB-Exploits-taken-down.html
Chaos Computer Club
Phenoelit
Phenoelit US
Police and Justice Bill - dual use "hacker tools" - has the Government finally seen sense ?
The new “Hacker-paragraph” §202c StGB!
Hollow chocolate bunnies from hell is closed

Wal-Mart Selects SSH Tectia Solution to Secure Data-in-Transit

<web-link for this article>

Wal-Mart Stores, Inc. (NYSE: WMT) and SSH Communications Security (HEX: SSH1V), a leading global provider of secure file-transfer and end-to-end communications security solutions for the enterprise, have announced that Wal-Mart has selected the SSH Tectia® solution to enable secure remote access and secure end-to-end data file transfer throughout the retail leader’s extensive global computing network. The SSH Tectia client/server solution secures sensitive company data-in-transit, delivering strong robust encryption, support for heterogeneous computing platforms and multiple authentication technologies, along with

enhanced SFTP (Secure File Transfer Protocol) capabilities. SSH Tectia provides an ideal alternative to prohibit unsecured file transfers and Telnet sessions.

Wal-Mart also selected SSH Tectia Manager, a comprehensive communications security management platform, to manage the enterprise-wide SSH Tectia security solution. SSH Tectia Manager enables powerful pre-configuration, deployment, and maintenance operations on an enterprise-wide scale, and performs auditing functions to help maintain regulatory compliance in a cost-effective manner.

"With the size and complexity of our environment, it was important to find a solution that could be utilized on all platforms," said Kerry Kilker, Wal-Mart vice president of information security. "The centralized management of SSH Tectia Manager will enable us to quickly deploy, easily maintain and simplify configuration management in our environment. That is where we expect to see the most return on investment with this technology."

"SSH Tectia is the best-of-breed solution for securing file transfers and data-in-transit end-to-end in large heterogeneous enterprise networks," said George Adams, president and CEO, SSH Communications Security, Inc. "SSH Tectia provides the strongest level of enterprise security for low overall costs, which complements Wal-Mart's highly effective business model. We are very pleased that Wal-Mart has chosen SSH Tectia after rigorous testing, to secure sensitive company information, while using Tectia's architecture and central management to meet their growing needs, today and in the future."

More Information

SSH delivered its largest ever order to Wal-Mart Stores, Inc. USA

How to Bias a Survey

<web-link for this article>

Computerworld Hong Kong and Symantec have recently been heavily promoting their InfoSecurity 2007 survey, which aims to, "help provide some insight to what security standards and benchmarks companies should aim for to safeguard their business". Unfortunately, the resulting insight is likely to be biased.

The survey, hosted by SurveyMonkey does not work for users of Mozilla Firefox, the supplied link just redirects to the site home page. The site works fine in the most commonly used browser, Internet Explorer, but it is probable that Firefox users have a distinctly different view of security from IE users.

Also, some of the questions in the survey do not consider all possible responses, for example, the question, "When do you plan to roll out Windows Vista throughout your enterprise?" does not have choices such as, "never", "we use Macs", or "we are intending to abandon Microsoft operating systems for an alternative". Again, a systematic bias is introduced.

The results of the survey will, no doubt, be interesting, but it should be bourne in mind that the results will reflect only part of the security landscape of Hong Kong businesses.

How Safe is Your Organisation from Trojans?

<web-link to this article>

This video demonstrates that many organisations are still open to a literally Classic exploit.

Note: the headline should read Greeks, instead of Trojans, but these guys were Australian, anyway.

Malware Detection and Lawful Spyware

<web-link for this article>

There has been debate about whether security software should detect trojans installed by law-enforcement for surveillence purposes sin, at least, 2001, when the "FBI Magic Lantern" trojan made the news. The two issues that arise if security companies deliberately do not detect Police spyware are:

any trojan used legitimately by the Police could be taken and used by criminals for other purposes

there would be a risk of law-enforcement mis-using the trojan, silently extending surveillence to larger segments of the population

CNET News has recently asked thirteen security companies about their policies and actions. They have also published the verbatim responses.

More Information

Will security firms detect police spyware?
Security firms on police spyware, in their own words
Sophos voices concern about FBI's Magic Lantern e-bug

HKCS Forms CIO Board

<web-link for this article>

Hong Kong Computer Society (HKCS) has announced the establishment of a new division of the society, the HKCS CIO (Chief Information Officers) Board. This division was officially established on the 20th of June 2007 with 7 founding members all of whom hold positions as Chief Information Officers or Heads of Information Technology in prominent Hong Kong companies.

The CIO Board is a group focused on sharing information between CIOs. Membership will be restricted in order to ensure the quality and relevance of member's submissions. The Board aims to encourage members to learn from each other through round-table discussions and open best practice sharing.

The CIO Board also plans to organise seminars, surveys and study groups to research and consolidate the volume of knowledge each member brings to the group. It plans to address a wide range of topics facing the Hong Kong ICT industry, including compatibility, education, knowledge retention and IT integration between Hong Kong and Mainland China.

The primary objectives of the new division are to provide a platform for (CIOs/HoITs) to share insights, views, issues and experiences amongst themselves. Also it aims to enhance the professionalism and competency of CIOs and HoITs in Hong Kong. Furthermore, to collect common views on matters of common interests related to ICT and to consolidate such views and submit them to relevant parties, to establish a knowledge-base on best practices of CIO and IT management and to contribute to the training and development of potential CIOs/IT managers in Hong Kong. Other objectives are to exchange and share experience with fellow CIOs/HoITs based in Mainland China and around the region and to assist CIOs to develop and mentor the next generation of IT leaders.

Membership to the HKCS CIO Board is restricted to individuals who head up IT, IS, MIS or Computer Services departments and can be obtained through nomination by existing members and approval by the CIO Board Executive Committees.

Activities for CIO Board members will be held on a bi-monthly basis.? Members will be sharing their best practices, latest technologies and developments. At the first meeting of the

CIO Board, the Chairman and members of the Executive Committee were elected. Members also came up with a long list of topics and issues to be addressed in future meetings.

Membership List

- Chairman: Mr. Daniel Lai, MTR Corporation Limited
- Mr. Joe Locandro, CLP Power
- Mr. Raymond Cheng, HSBC
- Mr. Raymond Chu, Hong Kong Housing Authority
- Mr. Peter Smith, HKCSL
- Ms. Susanna Shen, Towngas
- Mr Andre Greyling, Hospital Authority
- Mr Alfred Wong, HKEx
- Mr David Nicholls, Hutchison Whampoa
- Mr Edward Nicol, Cathay Pacific
- Mr Michael Leung, China Construction Bank
- Mr Michael Ma, AIG
- Mr Joseph Lai, Airport Authority
- Mr Paul Liu, Chong Hing Bank Ltd.
- Mr. Sunny Lee, Hong Kong Jockey Club
- Mr Timothy Tang, Hutchison Port Holding

Four charged in Hubei Province over Fujacks Worm

<web-link for this article>

Four men, Li Jun, Wang Lei, Zhang Shun and Lei Lei, have been charged with damaging Internet information systems in Xiantao City over their alleged roles in creating and spreading the Fujacks worm, also known as worm.whboy and "Panda burning joss sticks".

Fujacks spread, mainly on Chinese-language systems, though this was not a limitaion of the worm, during January 2007. Anti-virus company Sophos detected about 35,000 different websites that were hosting variants of Fujacks. It has backdoor capability, and can be used for stealing personal information including the account names and passwords of online game players and users of chat software, such as QQ

The alleged author, Li Jun, is said to have made over 100,000 yuan (US$12,500) selling to worm to twelve clients. Police also announced in February that they would release a removal tool for the worm, written by Li Jun, though this was criticised by security experts.

If convicted, the gang of four could face five years or more in prison. The arrests were said to be the first the Chinese Police had made in connection with a major internet virus.

More Information

Chinese Police Release Fix by Fujacks Suspect
Four charged over Panda cyber worm
Gang of four charged in Chinese joss-stick worm case
China charges four in Panda worm outbreak
Panda joss-stick virus rears its head on 3500 websites
W32/Fujacks-B (Sophos)

New Sony Rootkit Incident

<web-link for this article>

F-Secure reports that the software supplied with the Sony MicroVault USM-F uses rootkit techniques to hide a directory from the operating system. This could allow malware to install

and run itself undetected by some anti-virus software. The Microvalut USM-F is a flash USB drive with fingerprint reader.

From their analysis, F-Secure believes that the MicroVault software hides this folder to somehow protect the fingerprint authentication from tampering and bypass. It is obvious that, for secure authentication, user fingerprints cannot be in a world writable file on the disk, but the method used is open to exploitation by malware. F-Secure contacted Sony before going public with the case, but received no reply from them.

More Information

Double Whammy! Another Sony Case (And it's Not BioShock)
Deja vu: Sony uses rootkits, charges F-Secure

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/