

EICAR 18th Annual Conference
11 May to 12 May 2009
with a pre-conference program on
9 May and 10 May 2009

Abstracts of Industry Presentations

Sébastien Tricaud & Philippe Saadé
INL Paris France

Applied Parallell Coordinates for Logs and Network Traffic Attack Analysis

Abstract: By looking on how computer security issues are handled today, dealing with numerous and unknown events is not easy. Events need to be normalized, abnormal behaviours must be described and known attacks are usually signatures. Parallel coordinates plot offers a new way to deal with such a vast amount of events and event types: instead of working with an alert system, an image is generated so that issues can be visualized. By simply looking at this image, one can see line patterns with particular colour, thickness, frequency, or convergence behaviour that gives evidence of subtle data correlation. This paper first starts with the mathematical theory needed to understand the power of such a system and later introduces the Picviz software which implements part of it. Picviz dissects acquired data into a graph description language to make a parallel coordinate picture of it. Its architecture and features are covered with examples of how it can be used to discover security related issues.

Damien Aumaitre, Christophe Devaux, Julien Lenoir
Sogeti/ESEC, Paris France

Discovering a botnet from russia (with love)

Abstract: A botnet refers to the network of infected computers remotely controlled. Botnet's owners take advantage of the huge amount of hosts (and thus mass power) to generate illegal profit by performing spam or adware campaigns, Denial of services attacks or data theft. This article is an analysis of a multi-tasks botnet found in the wild. Everything began when an infected laptop was sent to our lab for a forensic analysis. The system was infected by many malwares. After a quick analysis, we decided to focus on one of it by curiosity. We soon realized that our infected machine was enrolled in a botnet and we decided to study the whole botnet. In a first part, we show how we have analysed and reverse engineered the malware itself and all the binaries it dropped. This analysis covers the infection, the machine exploitation and the network topology of zombies computers. From there we were able to draw the network map of the botnet and its control servers. We could also see the evolution of the malware features and improvement of protections layers. In the second part, we analysed the business model of this botnet. We gathered information about the "botnet manager", how he manages the botnet like a company. We have discovered its costs and profit sources, the developers' recruiting process and how this malware is potentially linked with others malwares and others criminal organizations.

David Harley
ESET, England

Execution Context in Anti-Malware Testing

Abstract: Anti-malware testing methodology remains a contentious area because many testers are insufficiently aware of the complexities of malware and anti-malware technology. This results in the frequent publication of comparative test results that are misleading and often totally invalid because they don't accurately reflect the detection capability of the products under test. Because many tests are based purely on static testing, where products are tested by using them to scan presumed infected objects passively, those products that use more proactive techniques such as active heuristics, emulation and sandboxing are frequently disadvantaged in such tests, even assuming that sample sets are correctly validated.

Recent examples of misleading published statistical data include the ranking of anti-malware products according to reports returned by multi-scanner sample submission sites, even though the better examples of such sites are clear that this is not an appropriate use of their services, and the use of similar reports to generate other statistical data such as the assumed prevalence of specific malware. These problems, especially when combined with other testing problem areas such as accurate sample validation and classification, introduce major statistical anomalies.

In this paper, it is proposed to review the most common mainstream anti-malware detection techniques (search strings and simple signatures, generic signatures, passive heuristics, active heuristics and behaviour analysis) in the context of anti-malware testing for purposes of single product testing, comparative detection testing, and generation of prevalence and global detection data. Specifically, issues around static and dynamic testing will be examined. Issues with additional impact, such as sample classification and false positives, will be considered - not only false identification of innocent applications as malware, but also contentious classification issues such as (1) the trapping of samples, especially corrupted or truncated honeypot and honeynet samples intended maliciously but unable to pose a direct threat to target systems (2) use of such criteria as packing and obfuscation status as a primary heuristic for the identification of malware.

Babu Nath Giri

McAfee Avert Labs, Bangalore, India

Malware in Men - will you be protected?

Abstract: Computers continue to increase their influence in many aspects of today's society, and that trend shows no signs of slowing down. We see computers in almost all walks of life, from satellites to cell phones, and from cars to coffee machines. Years ago people entered computers to operate and repair them; today, in contrast, computers are starting to enter humans.

As computers become faster, smaller, and wireless, wearable or implanted devices are gaining in popularity. These very portable computers are particularly useful in the area of medicine. Implantable devices such as pacemakers and hearing aides save and improve lives. Wearable devices—particularly consumer electronics such as MP3 players—have been popular for several years. Today we have MP3 jackets, head-mounted displays, and wrist-worn PCs. The comfort and mobility of these devices is compelling; however, because these are still computers, we also face the problems of the security and stability of these devices.

One excellent study on the security and privacy of implantable devices was done by Daniel Halperin et al (Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S.Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel, 2008). We've also read a fine study on the security issues of some popular consumer electronics, such as MP3 players and video streaming devices, by T. Scott Saponas et al. (T. Scott Saponas, Jonathan Lester, Carl Hartung, and Tadayoshi Kohno 2006). The two studies demonstrate that these devices are vulnerable to malicious attacks. In this paper we will look at the big picture of wearable and implanted devices with security in mind. We will also discuss the possibility of such malware arising in the future.

Christophe Devine & Nicolas Richaud

Thales – France

A study of anti-virus' response to unknown threats

Abstract: This study presents the evaluation of twelve anti-virus products with regards to programs not known from the signature files that show different kinds of malicious behavior. In practical terms, a set of twenty-one tests implementing various actions were developed; they cover key-logging, injection of code into other processes, network evasion, rootkit-like behaviour and exploitation of software vulnerabilities. The test programs were then run against each anti-virus program, and results were collected and consolidated. It was shown that all products tested here show deficiencies in at least one area, and some in all areas. For example, eleven anti-virus programs out of twelve still do not detect one code injection technique, which has been known for more than five years. Programs that spy on the user, such as recording the microphone, are not detected at all. Finally, this study provides recommendations to anti-virus vendors to enhance the capabilities of their products to detect malware, and improve safeguards against known attack techniques.

Magnus

Kaspersky Lab, Germany

Kalkuhl

From Virtual to physical

Abstract: Nowadays the worst thing that malware does is robbing someone's bank account, stealing confidential data, deleting files or DDoSing certain servers - but within the next 10 years things are going to be worse. The more that people depend on computers and robotics the stronger are the impacts that malware will have on their life - not only in terms of financial aspects, but with serious physical consequences for the victim's life. This presentation is about what could happen - and how security companies as well as the rest of the society could help to reduce the risks. Some of the scenarios may look a bit utopian at first glance, but that's due to the nature of future - we will all know better when we're finally there.

Franck Legardien
Hauri Labs , Seoul, Korea

Integrating Anti-steganography into Anti-virus Software.

Abstract: We all have thousands of pictures, mp3, and video files on our hard drives, most of them were collected from the web. Each of these files may or may not contain hidden data, these data may be harmless, or they may represent a potential threat, for example if the hidden data is the bytecode of a virus that embeds a virtual machine interpreter and that loads it's program from a carrier file. Or a virus might hide your own files into other files and ask you to pay a ransom to recover the original file. Or you may simply want to know whether files that reside on your hard drive contain hidden data or not.

For all these reasons, there is a need to have a tool that permits to provide two features:

- Hidden data detection
- Hidden data extraction (and if possible and necessary, decryption and decompression).

Until now anti-steganography tools have been built using an opposite paradigm comparing to antivirus scanners: antivirus will basically look for patterns that permit to identify a given malware, meanwhile anti-steganography tools generally consider a possible carrier file, and try to determine whether this file contains hidden data or not using file format specifications and statistics.

Thus, the approach proposed in this paper consists in an anti-steganography scanner that behaves almost like an antivirus: it is based on signatures and uses heuristics as well when necessary. And the most important thing is that this scanner is integrated into the antivirus itself so that you can process both virus threat and steganography threat at the same time.

In this paper we study the implementation of a free software called "Exosteg" that is integrated into an antivirus. Exosteg permits anyone to add its own detection and extraction algorithm using a simple plug-in system.

First we will explain the overall software architecture of Exosteg and what this architecture permits. Then we will try to show that anyone with a little programming skill can become the author of new plug-ins that will permit new threat analysis, the plug-in architecture will be presented in this step. The next step will consist in showing some real life examples permitting to show and explain the full cycle "detection/extraction/decryption," furthermore, results of performance benchmarks will be provided to evaluate the efficiency of the approach. Then to finish we will determine what such a tool does not permit to do, and what could and should be improved in the future.

Alexandre Gazet & Jean-Baptiste Bédrune
Sogeti/ESEC

Applied evaluation methodology for anti-virus software

Abstract. This paper presents an evaluation methodology dedicated to anti-virus software evaluation. The proposed methodology draws its inspiration from a French security assessment proposed by the Central Information Systems Security Division (DCSSI): the CSPN (Certification de Sécurité de Premier Niveau - First Level Security Certification). It is thought to be operational. We first define the notion of anti-virus software. Then, in accordance with this definition we propose a target of security, to which the anti-virus software should comply, taking into consideration the concept of test simulability.

Ferenc Leitold

Veszprog Ltd - College of Dunaújváros – Hungary

Checkvir Realtime Anti-malware testing and Certification

Abstract: A unique antimalware testing and certification procedure has been developed under the aegis of CheckVir Lab. This testing procedure can provide actual comparative test results of antimalware solutions automatically for the IT user community on the web. These are ready some minutes after the new version of a particular version of an antimalware solution is released. This realtime automatic testing is based on a set of dedicated PCs continuously checking the possible updates and they are dealing with executing the predefined testing procedures as well: Malware knowledge (detection, disinfection), False positive test, Speed test (in infected environment, in clean environment), Container (packers, obfuscators, e-mail clients storage files, embedded files).

Ramagopal Prashanth, Mohandas, Rahul, Thomas Vinoo
McAfee – Avert Labs, Bangalore, India

The Rise of Autorun-Based Malware

Abstract: Most people associate today's computer viruses and other prevalent malware with the Internet. But that's not where they started. Lest we forget, the earliest computer threats came from the era of floppy disks and removable media. With the arrival of the Internet, email and network-based attacks became the preferred infection vector for hackers to spread malicious code—while security concerns about removable media took a back seat. Now, however, our attention is returning to plug-in media.

Over the years, floppy disks have been replaced by portable hard drives, flash media cards, memory sticks, and other forms of data storage. Today's removable devices can hold 10,000 times more data than yesterday's floppy disks. Not only can they store more data, today's devices are "smart"—with the ability to run portable software programs or boot operating systems.

Seeing the popularity of removable storage, virus authors realized the potential of using this media as an infection vector. And they are greatly aided by a convenience feature in operating systems called autorun, which launches the content on a removable disk without any user interaction.

This paper traces the advancements in autorun-based malware. We also discuss methods to proactively detect and stop malware that spreads via removable drives, using a combination of traditional anti-virus and cloud-computing techniques.

Andy Hayter, George Japak, Leo Pluswick

ICSA Labs, Verizon Business, USA

Accrediting a Testing Lab under the Auspices of the International Standards Organization

Abstract: There are anti-malware testing labs and then there are certified anti-malware testing labs. How is it possible to receive assurance that the lab testing anti-malware solutions follows reproducible process and procedures, qualifies and certifies the analyst performing the tests and maintains detailed records? The International Standards Organization (ISO) standards 9001:2000 and 17025 were established to provide such assurance.

ISO 9001 defines the quality policy as a formal statement from management, closely linked to the business and marketing plan and to customer needs. The quality policy is a must understood and followed at all levels within the certified organization. Each employee must have measurable objectives to work towards. This entails detailed record keeping of processes and procedures. Regular internal and external independent audits validate adherence. This can be a very difficult exercise in the face of constantly changing world of malware and the associated anti-malware products. ISO 17025 is the primary standard used by testing and calibration laboratories. This standard was established in 2000, has much in common with ISO 9001, but adds in the concept of competence to the equation. There are two main areas of requirements for labs testing security solution. ISO 17025 management requirements are primarily related to the operation and effectiveness of the quality management system within the laboratory. Technical requirements address the competence of staff, methodology and test/calibration equipment. Would you allow just anyone to process a medical blood test without the assurance that they are properly certified to prepare samples, operate the equipment and report the results? The same standard applies to security solution testing, otherwise how are you assured that the company and analyst performing test on anti-malware software is competent to perform the test and adhering to documented processes and procedures. This paper will look at how testing and certification programs accredited under ISO 9001 and 17025 standards provide assurance to both the developer of anti-malware solutions and the end-point consumer, and that the lab issuing the certification meets the rigorous standards set by the International Standards Organization.

Anoirel S. Issa

Symantec, MessageLabs UK

Raw assault on a Poly/MetaMoRPhic engine

Abstract: Poly or metamorphic engines have some essential components that help them build highly obfuscated code. A single engine is able to produce unique variants that can reach millions. This means that a self replicating polymorphic virus is able to produce millions of new mutants from itself.

To achieve this when designing such engine, the author has to choose one or many registers and sacrificing them as garbage. This is an important point for us as we will be essentially exploiting this fact through this paper. The use of junk registers technique can produce an extremely obfuscated poly/metamorphic code when combined with some others features. Therefore trying to attack such a code directly by tracing its instruction flow could cause one being held indefinitely in a psychiatric hospital without "droit de parole". However, this does not mean that AV researchers are disarmed and are hopelessly watching things happening. Analysis can be performed whatever the difficulty presented by the level of "morphicity" of the generated code.