Do you still believe that nobody can make a Win 7 system become useless despite using a “powerful” antivirus?

DAVID Baptiste (ESIEA Laval - France)

Abstract
Do you really believe that such a threat is not possible? Imagine a massive denial of service on your computer. You click on any application and nothing happens, your computer becomes as useless as stone. But do not be worry, the antivirus is here and protects you from anything. According to the AV company, he will solve the problem since he can detect even unknown threats... Unless ... unless the antivirus itself cannot no longer do anything too!

You have just got an invincible virus in your system which has spilled out itself on your hard drive. A trigger is scheduled to start when the session begins and when the virus is executed absolutely nothing can stop it. Anyway, it is enough to give nightmares to many antivirus vendors... All of this is performed under Windows 7 in user mode with an attack which is not discriminating about the protection system installed. The work of an expert, do you think? Well you are going to be very surprised! This talk aims at presenting how sophisticated yet simple algorithmics and a pinch of mathematics is enough to bypass almost every antivirus, regardless of the privileges given to the user.

With demos!

Real-world physical attacks and countermeasures

Damien Aumaître (Sogeti - France) – Christophe Devine (Sogeti – France)

Abstract
Once physical access to a computer has been obtained, compromising the system is often a matter of hours, or even minutes. Several attack vectors will be presented; those include USB "U3" pendrives, bootkits and Direct Memory Access. Then, we will demonstrate how to put them into practise to successfully obtain full control of the target. Finally, we'll propose practical countermeasures for hardening computer systems with regards to known attack methods.

With demos !

Algorithm of computing entropy map as a new method of malware detection

Zdenek Breitenbacher (AVG Technologies – Czech Republic)

Abstract
It is evident that traditional approach to malware detection, based on typical binary signatures, cannot cover modern polymorphic malware. It is necessary to find another ways, which would not rely on binary signatures, but would be still precise enough. Our goal was to develop an algorithm, which would be able to transform polymorphic data into some easy to compare patterns. Such algorithm has to ignore binary variety in compared data and has to emphasize parameters which are still the same or similar for each member of a particular polymorphic family.

The keyword is entropy. It is well known that entropy of encrypted or compressed data is higher than entropy of well organized data, like program code or even text. So what about to compute entropy of each smallest part of the file and compare the entropy evolution throughout the file instead of searching for any binary signature?

We are going to introduce a new algorithm, which can transform binary data into precise entropy map. You will see that although particular members of a polymorphic family are different in binary, they have very similar or even identical entropy map. So such an entropy map, which is sufficiently detailed and easy to compare, now serves as a very good replacement of traditional binary sequences.

The algorithm of computing entropy map will be described in details, utilizing many images and charts. Although for practical purposes we usually assign one entropy value to each 16 subsequent bytes, you will see that it is easy to assign an entropy value to each particular byte in the examined file. This way we can get transformed data which reminds pure mathematical derivation.

Although this presentation is focused on the method itself, we are going to bring several examples from daily praxis to show, how this entropy map can speed up a process of polymorphic malware analysis and how it can help the malware analyst to create reliable definition.

Returning trust against user

Jean-Paul Fizaine (ESIEA – France) – Jonathan Dechaux (ESIEA – France)

In office software, the execution of macros is disabled with the default installation. Whenever a document is opened, the office application is displaying an alert to warn of the presence of macros embedded in the document. Moreover additional security mechanism exist (trusted macro, digital signature…), whose purpose is to prevent malicious macro to be executed and to enable those that the user wants only. Those features are supposed to provide enough security provided that there are well implemented. But in some cases, the software architecture exhibits

a few security holes with respect to their internal design. Consequently an attacker can efficiently exploit those security holes and thus turn the trust in the application security against the user. In this talk we show that we can go through or even bypass all those security mechanisms by using suitable malware algorithmics while exploiting that wrong sense of security. This approach enables to yield very powerful attacks.

The Perseus lib: Open Source Library for TRANSEC and COMSEC Security

Eric Filiol (ESIEA – France) – Eddy Deligne (DCNS – Toulon/ESIEA – France)

In this talk we present the Perseus library which enables to protect any kind of protocol/traffic against passive eavesdropping and thus protects the privacy while preserving and ensuring the national security needs of nation states. Any flows protected by Perseus cannot be broken unless having considerable resources (time and supercomputing power). Moreover any Perseus-protected data looks like non-encrypted data and thus evade detection based on pure COMSEC contents. Perseus thus can receive a lot of applications that will be described in this talk.

Smart cards Workshop

Vincent Guyot (ESIEA – France)

This 3-hour tutorial/workshop aims at practically introducing smart cards technology. Each participant will work on a smart card development kit (card reader + card; such kit can be bought at cost price on site as well for those interested). They will first develop one or more application for smart card by using a special SDK developed at ESIEA by Vincent Guyot. The programming language is JAVA.
Since the number of seats is limited (max 30) interested participants are strongly advised to register in advance. The remaining seats will be given onsite on "first come first served" basis.

---

sAVEX a new way to bypass Antivirus protection

Alan Zacardelle (Dimension Data – France)

Since decades, Antivirus Editors are faced to the growth rate of malware. They strive to detect, prevent and remove them and be more efficient in their detection and mitigation analysis, but attacks are also getting more and more sophisticated as new technologies and new needs come on markets. Because an antivirus is obviously installed on every system and gives the first end user defence, the only way for the attacker to succeed with malware's infection is to be "undetectable" during the attack by the system's antivirus software protection. The "undetectable" malware can live on the infected system as long as its code signature is not implemented in the next Antivirus updates. It is a historical battle between malwares and Antivirus products.

A lot of presentations and proof of concepts have shown how it was possible to disable antivirus (ie: iAWACS 2009/2010) but this paper will present new ways to bypass antivirus protection without disabling it. It will show also a way to keep the malware persistant and let it stay "undetectable"

Workshop on PLC

Xavier Carcelle (/tmp/lab – France)

"Crashcourse: Securing a PLC Networks"

New Threat Grammars

Geoffroy Gueguen (Universite de Rennes/ESIEA – France) – Eric Filiol (ESIEA- France)

Formal grammars have been used to model viral mutations. Indeed, any metamorphic virus can be represented by a formal grammar. We will see how we can define a particular class of viruses: the k-ary viruses, by using a special type of grammars: the two-level grammars, also known as the van Wijngaarden grammars. This enables to define a new kind of sophisticated malware.

PWN2KILL Challenge

Anthony Desnos (ESIEA – France) and Eric Filiol (ESIEA – France)

Five candidats have registered up to now.

Invited talks to come.

A few workshops to be added