Malware Nights

Organized by Agent Technology Center, Department of Computer Science, CVUT

Sebastian Garcia. ***sebastian.garcia@agents.fel.cvut.cz***

Malware Nights Seminar

The Malware Nights is a **seminar** for learning and experiencing the most advanced concepts of **Malware Network Forensic**s. It is designed to be very intensive and totally **practical**, allowing the students to grasp the most deep concepts of the discipline. Every step of the course is done on-site by the students, allowing a hands-on experience of how to work on network security, how does malware work in the network, how malware attacks web pages and how malware can be analyzed and detected.

The goal of the seminar are to allow students to:

- Learn about network traffic analysis.
- Learn about web attacks and how malware performs them.
- Learn how to execute malware, capture and analyze the traffic.
- Learn how to create better malware traffic protection measures.

The pedagogy of the seminar is based on Constructivism, specially the Accommodation theory, by which **learning comes from experiencing and failing**. Another pillar of the seminar is the **active learning** theory, or **learning by doing**, by which students discover and learn by their own means.

Class Plan

The seminar has **four classes**. Each will be **three hours long** in a laboratory, where students try each example and idea. After a short introduction to know why students are here, we will talk about why we do this job, the ethics related, how important is network security and the analysis of network traffic.

The only requirements for the students are to bring a **laptop** and a running virtual machine of the **Kali Linux** distribution[1]. There are no restrictions about the knowledge students must have prior the course, but a familiarization with linux and network protocols will speed up the course.

First Class: Network Security and the Malware Trails.

The main goal of the first class is to develop a common ground on the knowledge about **network security** among the students. We will start with basics analysis and we will move to more complex tasks on recognition.

The minimal topics covered are:

- How network protocols work. A reminder.
- Analysing network traffic, what to see.
- Basic tools: Wireshark, tcpdump, ngrep, etc.
- Security considerations of network traffic: outside the protocols.
- How does the security of network traffic impact us? Pros and cons.
- Port scanning, web crawling and attacks in the network. Can you recognize them?.
- Attacking each other and discovering the traffic.

  By the end of this class students must be able to work easily with network analysis tools and to recognize protocols and security indicators.

[1] https://www.kali.org/downloads/

Second Class: Web Attacks and Malware Abuse

The main goal of the second class is to understand **how web attacks take place**, the impact of the attacks, how the attacks work and how these **techniques are abused by malware** to accomplish their tasks. It is very important to know how to attack in order to understand how to defend. The class will have special security measures to make the attacks.

The minimal topics covered are:

- Motivations to study web attacks, case studies of real malware.
- How does HTTP and HTML work in principle. Looking at the big picture.
- How to do common attacks: SQL Injection, XSS, vulnerability exploiting, code injection and inclusion vulnerabilities.
- Trying the attacks and understanding their network fingerprint.
- Why malware need to attack web pages?
- Why attacking one web page is not the same as the web abuse of malware?
- Common protection solutions and tools.

By the end of the second class students should be able to do basic web attacks, understand the techniques, know malware attack techniques and recognize the traffic from most of these actions.

Third Class: Malware Execution. The Real Thing

The main goal of the third class is to introduce students to the discipline of **malware execution** and analysis. Teaching about real malware is the only way of learning how to stop it[2].

To accomplish these tasks we will create a safe laboratory environment. It will use a special connection to allow the execution of malware inside the university, in such a way that it is not possible to abuse it to attack the University or to make DDoS attacks or send SPAM. In particular the students will be routed through our malware capture facility project laboratory[3], which is under strong control policies.

The minimal topics covered are:

- The environment of malware execution. Techniques and ethics.
- What does malware eat?
- Why to execute real malware?
- Downloading and selecting malware samples.
- Executing malware.
- Monitoring malware traffic and execution.
- Basic Analysis of malware traffic.

By the end of the third class students should be able to execute their own malware binaries, analyze the traffic and understand the repercussions.

Fourth Class: Botnets and Malware Traffic Analysis

The main goal of the fourth class is to analyze the network traffic of the malware samples and start to see and develop **theoretical behavioral models** of how the malware is working. We will focus on **differentiating malware traffic from normal** traffic, which are the differences and similarities and how can we exploit them to better detect malware.

The minimal topics covered are:

- Deep analysis of the malware traffic.
- Support information tools: flows, web logs, etc.
- Analysis of all the data in order to extract more information.
- Identification of malware patterns and behavioral characteristics.
- Detection ideas of malware patterns.

By the end of the fourth class students should be able to recognize the patterns in malware traffic and design probable detection methods for protection.

Registration

Registration is done by email to
sebastian.garcia@agents.fel.cvut.cz

Send an email with your name, affiliation (if you have one) and a one-liner of why you want to attend the seminar.

[2] http://www.csl.sri.com/users/neumann/cacm223.pdf
[3] http://mcfp.felk.cvut.cz

Conclusion

We expect this seminar to help train students in the **malware network security and analysis** area. There will be a final and optional homework consisting in the development of tools to implement some of the ideas about detection. This homework will give us another indicator of the capabilities of the students for future consideration.