Reverse Engineering of Malicious Software Training

Introduction

- Review of best practices in digital investigation
- Overview of different malware families
- Infection vectors
- Persistence and propagation mechanisms

Analysis Lab

- Virtual vs. physical labs
  - Advantages of virtualization
  - Virtualization solutions
- Network segregation
  - Virtual and shared networks
  - Virtual machine containment
  - Precautions and best practices

Monitoring Machine Activity

- Network
- File system
- Registry
- Services

Introduction to Behavioral Analysis

- Diversity of systems

Setting Up a Behavioral Analysis Ecosystem

- Ecosystem configuration
- Definition of standard configurations
- Virtualization of guest machines
  - VMware
  - VirtualBox
- Installation of CAPEv2 and VirtualBox

Practical Application

- Submitting malware
- Analysis process
- Result analysis and reporting

Improvement via API

- Development opportunities and enhancements

Dynamic Malware Analysis

- Precautions
  - Working within virtual machines
  - Network configuration
- Analysis tools
  - OllyDbg
  - Immunity Debugger
- Debugging analysis
  - Step into / Step over
  - Software and hardware breakpoints
  - Key system functions to monitor
  - Pseudo-random domain name generation (C&C)
  - Best analysis practices
- Anti-analysis mechanisms
  - Debugger detection
  - Detection of reverse engineering tools
  - System exploit techniques

Analysis of Malicious Documents

- PDF Files
  - Introduction to the PDF format
  - Specific characteristics
  - JavaScript integration and possibilities
  - Examples of malicious PDFs
  - Analysis tools: OLE Tools, hex editor
  - Payload extraction and analysis
- Office Files (DOC/DOCX)
  - Introduction to DOC/DOCX formats
  - Specific characteristics
  - Macros
  - Linking and Embedding Objects (OLE)
  - Analysis tools: OLE Tools, hex editor
  - Malicious code extraction and analysis
- APK Files
  - Introduction to APK format
  - Analysis tools: jadx, Frida, Genymotion, MobSF
  - Bypassing emulator protections
  - Understanding application behavior

Nous contacter:
Doussou Formation
Email: info@doussou-formation.com
http://doussou-formation.com