Modern Malware OPSEC & Anti-Reverse Techniques Implementation and Reversing

Introduction

The course will present an in-depth description of the techniques implemented in modern malware to evade defenders and security products (such as AV, IPS, IDS, EDR), and how attackers design and operate their implants in order to ensure a prompt redeployment after a detection or a public disclosure by researchers or security vendors.

The course will also cover real-world scenarios that impair (effectively slow-down or dissuade) reverse engineering efforts and make the job of first responders tougher. The techniques will be demonstrated in two ways: first, by reversing real malware samples, and then by re-implementing an improved version of the malware code. The training is designed from an attacker's point of view, teaching red-teams how to make their implants stealthier, but it will also teach defenders how to deal with the anti-reversing and the OPSEC techniques demonstrated in class.

The course focuses primarily on Windows malware and on the analysis, tweaking and re-purposing of real malware samples. Participants will be provided with plenty of custom code to facilitate the understanding of complex malware techniques.

As part of the course, theory sessions will be followed by exercises where participants will reverse and re-implement specific parts of real malware in order to fully understand the hidden corners of all the techniques involved. The 50% of the course will be dedicated to hands-on labs that will show how to translate the theory principles into practice.

Labs are designed to provide flexibility in terms of complexity and include bonus tracks to ensure that you always feel engaged and have something interesting to explore and learn.

Almost all labs are provided in dual versions (reverse and development). Students can choose which version to approach.

To develop and test the techniques described during the theory sessions, students will be provided with the source-code of our training agent and its corresponding C2.

Key Learning objective

Be able to recognize, implement and deal with stealthy malware/backdoors techniques and tradecrafts.
Be able to modify malware components and pre/post build tools to protect them against reversing efforts.
Familiarize with the latest advances in code and DLL injection techniques and customize reflective loader.
Be able to build custom obfuscators and to recognize some pattern left by some obfuscation transforms.
Learn tradecrafts used by attackers to prevent and effectively impair defensive incident responders from analyzing their tools, payloads, and backdoors.

Who should Attend

Developers and Reverse engineers who want to understand the tradecraft from a different point of view, red-team members who want to go beyond using third-party implants, and researchers who want to develop anti-detection techniques of real malware/apt.

Prerequisites

Programming experience (C, C++, Python, .NET, and PowerShell)
Be familiar with assembly language and Debuggers (IDA pro, WinDBG)

Hardware/Software requirements

Laptop Requirements:
Virtualization capable Intel CPU(s) (ARM CPUs are not supported)
Minimum 8GB of RAM (for running one guest VM)
Minimum 80 GB free disk space

Software Requirements:
Host OS Windows 10 64-bit
Debugging Tools for Windows (Ida Pro, WinDBG). Decompiler recommended.
SysInternals Tools
Virtualization Software (VMWare, VirtualBox)
Guest OS Windows 10 64-bit
System Administrator access required on both host and guest OSs

Course Agenda

- ❑ Module 1
    1. Warm up (refresh basic concepts)
    2. DynLoader
        - ❑ Dynamic APIs resolution
        - ❑ Import by hash
        - ❑ PEB walk
        - ❑ Syscall direct invocation
        - ❑ API Custom implementation
    3. Obfuscation I
        - ❑ Obfuscation techniques
        - ❑ Opaque predicates, MBA, VM obfuscators
- ❑ Module 2
    1. Obfuscation II
        - ❑ Source level obfuscation
        - ❑ Intermediate representation obfuscations (LLVM)
    2. Bring your own Loader
        - ❑ Windows Loader
        - ❑ Alternative Loaders
    3. Injection I (Advanced Reflective Loader)
        - ❑ Wide used injection techniques
        - ❑ Reflective Loader deep analysis
        - ❑ Customize RL
- ❑ Module 3
    1. Injection II (Exotic Injection)
        - ❑ Uncommon injection techniques
        - ❑ Hooks
        - ❑ Implement an *exotic* injector
    2. Anti-Debug
        - ❑ Debugging internals
        - ❑ Breakpoint detection (HW and SW)
        - ❑ Anti-tampering
    3. Persistence
        - ❑ COM/DLL Hijacking
        - ❑ WMI persistence

- ❑ Module 4
  1. Anti-VM
     - ❑ Artifact detection
     - ❑ Instruction and timing detection
     - ❑ Build an anti-vm module
  2. Multi Lang Module
     - ❑ Run managed code from unmanaged
     - ❑ AMSI
     - ❑ Execution Guardrails
     - ❑ IPC
  3. Final Lab

BIO

Dr. Silvio La Porta is CEO and Co-Founder at RETooling defining and developing Threat Actor emulation platform enabling red team to recreate a realist attack scenario. Previously he was a Senior Cyber Security Architect designing security products and researching advanced detection technology for complex malware/APT. Silvio previously was a lead research scientist with EMC Research Europe based in the Centre of Excellence in Cork, Ireland. His primary research focus areas were real-time network monitoring and data analysis in smart grids to detect malware activity in SCADA systems and corporate networks. He was also leading Security Service Level Agreement (Sec-SLA) and end user security/privacy protected data store projects for hybrid Cloud environment. He is a frequent speaker in professional and industry conferences. Before joining EMC, Silvio worked as a Malware Reverse Engineer in Symantec's Security Response team in Dublin, Ireland. Silvio holds a PhD in Computer Network Security from the University of Pisa, Italy.

Dr. Antonio Villani is the Co-Founder of RETooling. He is working full-time on the development of red-team and adversary emulation capabilities for his company. Previously he spent most of his time in the blueteam, reversing high level implants for top tier customers and providing detailed information to support cyber-defense and cyber threat intelligence teams. Now he analyzes complex implants to gain a deep understanding of the TTPs used by threat actors and to provide a high-quality reimplementation of them. As a researcher he published in top tier conferences and journals, and he participated in European research projects in the field of cyber resilience and data security. During his PhD he worked in the field of malware research and digital forensics.