EDR: The Great Escape

by Silvio La Porta & Antonio Villani

TRAINING DESCRIPTION

Engaging in red-team activities within enterprise networks often involves encountering and bypassing endpoint protection solutions, specifically Endpoint Detection and Response (EDR) systems. These EDRs are intricate and sophisticated systems designed to monitor and defend against various threats, including unauthorized access attempts by red team operators seeking to infiltrate the target network. This course aims to provide a comprehensive understanding of the architecture of modern EDRs and their underlying Antivirus (AV) systems. It delves deeply into the complexity of modern EDRs, their structure, including the components responsible for real-time monitoring, data collection, and threat analysis. The course also explores how internal Antivirus (AV) systems operate within the EDR framework, their role in threat detection, and their interaction with other security components. In addition to examining detection mechanisms employed by EDRs, participants will learn about evasion techniques. This includes tactics and strategies to evade detection by EDRs, such as bypassing signature-based scans, disguising malicious behavior, and exploiting potential vulnerabilities in EDR configurations. 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 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. This Class is complementary to our main training covering techniques not present in the main class. This course is valuable not only for red team operators but also for blue team professionals. Blue team members can gain insights into

how their detection systems may be bypassed, helping them enhance their security measures and stay one step ahead of potential threats. This course equips security professionals with a deep understanding of modern EDRs and their AV systems, enabling them to better simulate advanced threat scenarios, improve their evasion detection skills, and contribute to the overall enhancement of security within enterprise networks.

TRAINING OUTCOMES

> Be able to recognize, implement and deal with stealthy malware/backdoors evasion techniques and tradecrafts.
> Be able to modify malware components to protect them against reversing efforts.
> Familiarize with the .NET advanced obfuscation system.
> Be able to build custom obfuscators and to recognize some pattern left by some obfuscation transforms.
> Learn tradecraft used by attackers to prevent and effectively impair defensive incident responders from analyzing their tools, payloads, and backdoors.

ABOUT THE TRAINER

Dr. Silvio La Porta is CEO and Co-Founder at RETooling defining and developing Threat Actor emulation platform enabling red team to recreate a realistic 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 environments. 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 Co-Founder at RETooling and spent the past years analyzing high level implants for top tier customers, providing detailed implementation information to support cyber-defense and cyber threat intelligence teams. Now, he uses his experience in the reverse-engineering of multi-stage implants re-implementing it to improve RETooling attack emulation products. 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 its PhD he also worked in the field of malware research and digital forensic.

WHAT TO BRING

> Virtualization capable CPU(s)
> Minimum 8GB of RAM (for running one guest VM)
> Minimum 80 GB free disk space
> Host CPU intel (ARM is not supported)
> Host OS Windows 10 64-bit
> Debugging Tools for Windows (Ida Pro, WinDBG). Decompiler recommended.
> SysInternals Tool Suite
> Virtualization Software (VMWare, VirtualBox)
> Guest OS Windows 10 64-bit Version 20H2

> System Administrator access required on both host and guest OSs

WHAT WILL BE PROVIDED

> ~500 page printed lecture materials
> Custom VMs with laboratories that will remain to the student forever
  - All the laboratories will be both dev and reverse version

PARTICIPANT SKILL SET

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

CLASS SYLLABUS

MODULE 1

> The shortest Intro
> Give a shout to the Alpaca
> The reference architecture
> Minifilter drivers
  - Architecture, altitute
  - pre/post operation Callbacks
  - Self-protection
> Kernel to user dll injection
  - APC injection
  - Hooking library
  - Hook detection / Unhooking strategies
  - Show the openedr implemenetation
  - Look at a couple of proprietary DLL s
> Unhooking the watchers in all the possible ways
  - Restore the original ntdll
  - Patch the hooked ntdll in memory
  - The right ways of using call gates
  - Indirect syscall
> Labs:
  - Unhook
  - Disable self-protection

MODULE 2

> Using ROP to do good or better bad things…
  - Write your ROP injector
> Protected Processes and Protected Process Light
  - Internals: Core kernel data structures
  - Anti-Malware and ELAM
> Mastering ETW and get the forbidden feed
  - Providers, Consumers, Sessions
  - User-space provider bypass
  - The Threat Intelligence Provider
> Labs:

- Using ROP to minimize the presence in ETW logs

MODULE 3

> Primer on the Windows Filtering Platform
> File Scanners
> Memory Scanners
  - Moneta
  - PE-sieve
  - Other memory scanner tools
> Smashing the stack for fun and evasions
  - Stack spoofing
  - Sleep Obfuscation
> Local Privilege Escalation
  - SID, UAC, DACL, PPL, PP
  - Abuse WinSxS
  - Handle stealer
> Labs
  - LPE and get Admin
  - Create your stack spoof

MODULE 4

- Notification callbacks
  - Process, Threads, Objects
  - OpenEDR implementation
  - Vendor specific implementations?
  - Weaponize vulnerable signed drivers to bypass EDR detections
- .NET internals
  - C# file format and internals
  - C# Interoperability C++ (IJW)
  - Obfuscate and make hard to reverse your C# stage0
- Lab .NET obfuscation