THREATHUNTING ACADEMY : EVASION

COURSE OVERVIEW:

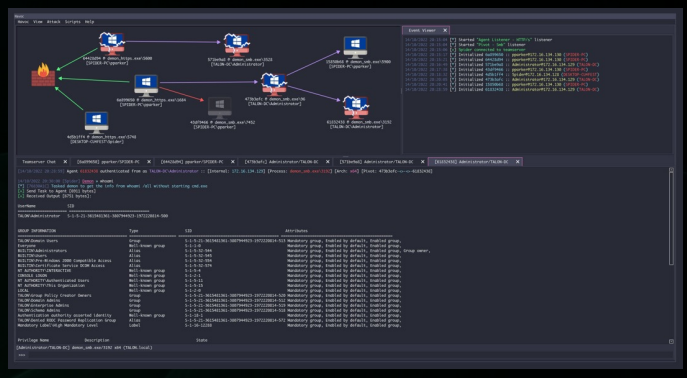
“Threathunting academy : Evasion” is a practical training program that combines offensive and defensive cybersecurity techniques to teach advanced evasion methods. Through hands-on labs, participants will learn how adversaries operate and how to counter their tactics effectively.

What makes this training truly unique is the translation of complex technical matter into a logical step-by-step approach of combining theory and practice, which significantly lowers the pre-requisite level of knowledge normally required for trainings such as these.

We focus on properly explaining how adversaries compromise environments by implementing **evasion** techniques, in order to teach students the proper analytical skills and timely responses when their security tooling (i.e. EDR) flags an event as suspicious.

Quickly spotting actual suspicious activity and knowing how to investigate are the most underrated skills for SOC Analysts, Security Engineers and **Blue Teamers**.

For a beginning **Red Teamer**, this training will show how their payloads can be detected and how to improve their tradecraft when performing engagements.



(Havoc C2 Framework)

BUSINESS TAKEAWAYS:

- Gain a clear understanding of adversary tactics, techniques, and procedures (TTPs) like privilege escalation, code execution, persistence, memory injection and evasion.
- Deal with and better understand alerts from various security tooling
- Build and customize a **C2 framework** (Havoc C2) to simulate real-world attacks and implement evasion techniques such as AMSI/UAC bypasses, ETW patching, and static signature evasion.
- Develop a **custom evasive shellcode loader** by applying techniques learned during the course.
- Analyze adversary behavior, identify threats, and use the right tools for **detection and response**.
- Understand the strengths and limitations of AV/EDR/SIEM solutions and how they integrate into a security operations center (SOC).

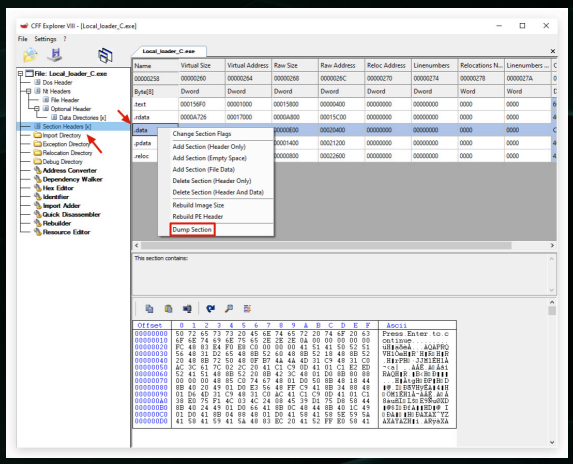
WHO SHOULD ATTEND:

- **Security practitioners**, system administrators, and architects wanting to deepen their understanding of adversary behavior.
- **SOC analysts**, incident response, and threat hunting team members looking to detect and respond to sophisticated attacks.
- **Security engineers** aiming to improve interpretation and response to AV/EDR/NDR alerts.
- **Red team operators** interested in bypassing defenses with evasion techniques and custom shellcode.
- **Forensic analysts** seeking to uncover adversary techniques through reverse engineering and shellcode analysis.
- Organizations planning to establish an in-house or managed (**MXDR**) SOC or evaluating SIEM/EDR vendors to understand their functionality , applications and limitations.

THREATHUNTING ACADEMY : EVASION

The course starts with setting up your own C2 Framework (**Havoc C2**), using the built-in payload generator to demonstrate how adversaries compromise systems. From there we'll walk through several evasion techniques such as **AMSI** and **UAC** bypasses, **ETW** patching and static **signature evasion** – using of the shelf open-source code, that will be modified by students to bypass detections. Each step of the way the techniques used will be explained, and implemented in hands-on labs. We will cover **blue** and **red teaming** tradecraft as we continue by building a custom evasive shellcode loader, incorporation techniques learned along the way.

The custom developed tooling will then be integrated into the Havoc C2 framework, demonstrating how to extend the capabilites of existing C2 frameworks. At each stage we'll show how to analyze the TTPs implemented, in order to fully understand adversary behaviour, which tools to use for anlysis and where to start when analyzing malicious files.



(Analyzing shellcode)

TRAINING SCHEDULE

DAY 1

- **Introduction**
- **Overview of C2 frameworks**
- **Privilege Escalation techniques**
- **Windows Defender Internals**

DAY 2

- **AMSI & CLR**
- **WIN32API & Functions**
- **Building an evasive shellcode loader**
- **Malware Analysis Lab**

DELIVERED BY

Luk Schoonaert has a proven track record as a hands on **CISO** and strategic advisor, specializing in **threat hunting**, **detection engineering**, and mitigating advanced threats. Recognized for driving innovation, building high-performing teams, and delivering actionable security solutions for global organizations.

Pieter-Jan Blaton is a life-time cybersecurity veteran with deep levels of understanding ranging from network, endpoint, SIEM/SOAR, UEBA and other security technologies. He currently works as a **Senior SOC Analyst** and is a master at troubleshooting.

Both have taught Threathunting academy courses before and have hands-on experience with building and managing next-generation automated SOCs.

FORMAT

- Instructor-led hands 2 day technical training
- Maximum of 15 seats to keep teacher-student interaction at the highest level
- Custom in-house private training available as of 10 seats

PREREQUISITES

- Familiarity with Windows and Linux is a plus. No coding skills required.

HARDWARE REQUIREMENTS

Students need to bring their own laptops with the following minimum system requirements :

- Windows 10 /11 or recent MacOS
- A recent web-browser (Chrome would be preferred)
- As we are running everything in the cloud, nothing needs to be installed on the student machines .

COURSE MATERIALS

- Students will receive all training materials including code and tools.