MALWARE ON STEROIDS

A Malware Development Training Program for Windows

Dark Vortex LLP

Table of Contents

Day 1

- Course Overview
- Development VM Setup
- Command and Control Architecture
    - Malware Lifecycle
    - Payload Handling
- Windows Internals
    - Windows OS architecture
    - Process & Thread Internals
    - Debugging with Windbg
    - PE & DLL Structure
    - Writing Reflective DLL Loader
    - Windows Memory Protections
    - Windows System Programming
    - Windows Access Security Tokens
    - Impersonating Process Tokens

Day 2

- Windows Socket Programming
  - Reverse Shells in C
  - Bind Shells in C
- Anonymous Pipes
- Named Pipes
- SpyC2 – Building your own CnC
- C2 Methodology
  - Asynchronous HTTP Callbacks
  - C2 Authentication
  - Comm Encryption
  - Sleep & Jitter
  - C2 Round Robins
  - URI Handling
- Malware Functions
  - Enumerating users, groups and hosts
  - Enumerating Process
- Memory Dumping Techniques
  - MiniDumpWriteDump
  - PssCreateSnapshot
  - In-memory Memory Dumps
- Process Injections
  - Building Evasive Loaders
    - Reflective DLL

    - C# Reflection
    - PowerShell Reflection
  - Injections using WinAPI Calls
  - Injections using NTAPI Calls
  - Thread Hijacking and APCs
  - Injection Evasion Tactics
  - Hiding Memory Artefacts
- Macros, Droppers and Stagers
- Stageless Payloads

Day 3

- Shellcoding
  - Introduction to x64 Intel Assembly
  - Position Independent Shellcodes
  - Position Independent Code in C
  - In-Memory Object File Execution
- Sandbox Evasion
- Code Obfuscation and AMSI Evasion
- PowerShell one liners, HTA, LOLBINS
- MS Build, MWC Executions
- Named Pipe Executions
  - Building your own PS Exec in C
- OPSEC Considerations

Target Audience

- Red Team members
- Penetration Testers
- Blue Teamers
- Threat Hunters

This intense three-day training program is designed for security professionals who want to enhance their skills by digging more deeper than the usual Red Team. This course will give you brief introduction towards the Windows Internals and how to manipulate them for offensive tasks. You will learn to build your own Command and Control Centre and different types of payloads which support code injections, dropper and stagers in ASM and C.

Requirements

- A laptop with 16GB RAM to support 2 VMs running at the same time.
- Basic Understanding of operating system architecture
- Basic understanding of programming concepts
- Experience with or knowledge of pointers, addresses in C and multi-threading/processing in Python3
- Strong will to learn and creative mindset.

What all do you get in the end

- 3 days of rigorous training program
- Course PDF and content materials
- Source code for payloads and a python3 C2 built during your training program

For any queries, contact paranoidninja@0xdarkvortex.dev