ZAIUX
framework

An advanced and customized Command-and-Control software designed for authorized Red Team operations

ZAIUX Framework comes with a vast set of out-of-the-box evasive techniques, leaving the Red Team only the duty to perform the offensive operations in a safe and under-the-radar environment.

Key Features

Automatically unhook User-Land Callbacks
Prevent some EDR products from tracing Syscalls and loaded modules by disabling callbacks monitoring routines such as ProcessInstrumentation and LdrRegisterDllNotification

Indirect Syscalls + Dynamic SSN Resolution on-the-fly
Change the return address of the Syscall instruction in ntdll.dll memory region and automatically resolve Syscalls' System Service Numbers

LoadLibrary Proxy
LoadLibrary() is proxied to through legitimate Windows APIs and memory regions, in order to keep a clean stack whenever a new library is loaded

Inline Execution
Run .NET, COFF and EXE inside the memory of the current process, bypassing detection by avoiding any kind of fork n' run operation

Return Address Spoofing
Spoof the return address of the thread before going to sleep, without calling Sleep() or NtDelayExecution()

Sleep Obfuscation
Prevent Memory Scanners from identifying the payload in memory during sleep cycles

Patchless AMSI & ETW Evasion via Hardware Breakpoints

AMSI and ETW Bypass is carried out through Hardware-Breakpoints, avoiding any Byte-Patching in ntdll.dll or amsi.dll

Automatically free the Shellcode's memory region

Release the operator from the need to free the memory region initially allocated for the shellcode

Other Technical Specs

- Token Impersonation
- Multiple Shellcode Injection techniques
- Situational Awareness built-in features
- File-Transfer capabilities
- Provided Implant types: Shellcode, DLL, EXE (Fully written in C and Assembly)
- Malleable Profiles
- Designed for Red-Teams (Multi-Player)
- More...

Ethical Hacking, Artificial Intelligence and Machine Learning
cleverly combined by an expert team who offers
cutting edge software solutions and services to mitigate Cyber Risk

ZAIUX® framework is a “Made in Italy” solution
developed by Pikered | Milano | pikered.com