






































 Files

 ce04369









 Go to file


- >  APC_Injection
- >  API_Hammering
- >  API_Hooking
- >  Anti_Analysis
- >  Anti_Debug
- >  Binary_Info
- >  Block_DLL_Policy
- >  Callback_Code_Execution
- >  Compile_Encrypt_String
- >  Create_DLL
- >  Create_Driver
- >  Create_UEFI
- >  Early_Bird_APC_Injection
- >  Enable_All_Tokens
- >  Encryption_Shellcode
- >  Enumeration_Processes
- >  Execute_Command
- >  Extract_Wifi
- >  Hells_Halos_Tartarus_Gate
- >  IAT_Camouflage
- >  IAT_Obfuscation
- >  LdrLoadDll_Unhook
- >  Local_Function_Stomping_Injection
- >  Local_Mapping_Injection
- >  Local_PE_Injection
- >  Local_Payload_Execution
- >  Local_Thread_Hijacking
- >  Minidump-rs
- >  Module_Overloading
- >  Module_Stomping
- >  NTDLL_Unhooking
- >  Named_Pipe_Client_Server
- >  Obfuscation
- >  PPID_Spoofing
- >  Parsing_PE
- >  Patch_AMSI

 joaoviictorti refactor: rename folder

bf05ce1 · 9 months ago

 History

Name	Last commit message	Last commit date
 ..		
 src	refactor: rename folder	9 months ago
 .gitignore	refactor: rename folder	9 months ago
 Cargo.lock	refactor: rename folder	9 months ago
 Cargo.toml	refactor: rename folder	9 months ago
 README.md	refactor: rename folder	9 months ago

README.md

Self Deletion

made with

Rust

platform

windows


- [Overview](#)
- [Usage](#)


Overview







This project focuses on the self-deletion technique, which allows the binary itself to be deleted during execution. This functionality is particularly useful in scenarios where it is detected that the binary is under analysis, either through debugging or execution in a Virtual Machine (VM)

Usage

You can run with cargo run or the compiled binary directly:

cargo run

target/release/self_deletion.exe

- >  Patch_ETW
- >  Payload_Execution_Control
- >  Payload_Execution_Fibers
- >  Payload_Placement
- >  Process_Argument_Spoofing
- >  Process Ghosting