

---

## Tangled WinExec

This repository is for investigation of Windows process execution techniques. Most of PoCs are given a name corresponding to the technique.

### Projects

- **BlockingDLL** : This toolset is for testing blocking DLL process. See README.md.
- **CloneProcess** : This directory is for process forking and reflection. See README.md.
- **CommandLineSpoofing** : This PoC performs Command Line Spoofing. This technique may not work for Windows 11.
- **DarkLoadLibrary** : PoCs in this directory are for testing Dark Load Library which is released by @\_batsec\_. See README.md
- **GhostlyHollowing** : This PoC performs Ghostly Hollowing.
- **Misc** : This directory is for helper tools to development PoCs in this repository.
- **PhantomDllHollower** : This PoC performs Phantom DLL Hollowing. See README.md.
- **PPIDSpoofing** : This PoC performs PPID Spoofing.
- **ProcessDoppelgaenging** : This PoC performs Process Doppelgänger. Due to kernel protection improvement for Microsoft Defender, this technique does not work for recent Windows OS (since about 2021, maybe). So if you want to test this technique in newer environment, must be stop [Microsoft/Windows Defender Antivirus Service](#). See the issue for hasherezade's repository.
- **ProcessGhosting** : This PoC performs Process Ghosting. Due to kernel protection, this technique does not work for newer Windows from 22H2.
- **ProcessHerpaderping** : This PoC performs Process Herpaderping. Due to file lock issue, if you choose a fake image file smaller than you want to execute, file size shrinking will be failed and corrupt file signature for herpaderping process. To take full advantage of this technique, fake image file size should be larger than you want to execute. Due to kernel protection, this technique does not work for newer Windows from 22H2.
- **ProcessHollowing** : This PoC performs Process Hollowing. Unlike the original, the PE image is parsed into a new memory area instead of using [ZwUnmapViewOfSection](#) / [NtUnmapViewOfSection](#).
- **ProcMemScan** : This is a diagnostic tool to investigate remote process. See README.md.

- 
- **ProtectedProcess** : This toolset is for testing Protected Process. See README.md.
  - **ReflectiveDLLInjection** : This toolset is for testing Reflective DLL Injection. See README.md.
  - **sRDI** : This directory is for tool to sRDI (Shellcode Reflective DLL Injection). See README.md.
  - **TransactedHollowing** : This PoC performs Transacted Hollowing.
  - **WmiSpawn** : This PoC tries to spawn process with WMI. The processes will be spawn as child processes of [WmiPrvSE.exe](#). Supports local machine process execution and remote machine process execution. The usage can see README.md.

**NOTE** : Currently ProcessHollowing code does not works for Debug build. To test it, use Release build. See this issue.

## Reference

### Blocking DLL

- Preventing 3rd Party DLLs from Injecting into your Malware
- Staying Under the Radar - Part 1 - PPID Spoofing and Blocking DLLs
- PPID Spoofing & BlockDLLs with NtCreateUserProcess

### Command Line Spoofing

- Hide Artifacts: Process Argument Spoofing
- The return of the spoof part 2: Command line spoofing

### Dark Load Library

- GitHub - bats3c/DarkLoadLibrary
- Bypassing Image Load Kernel Callbacks

### Phantom DLL Hollowing

- Masking Malicious Memory Artifacts – Part I: Phantom DLL Hollowing
- GitHub - forrest-orr/phantom-dll-hollower-poc

---

## **PPID Spoofing**

- Access Token Manipulation: Parent PID Spoofing
- Parent PID Spoofing (Mitre:T1134)
- How to Detect Parent PID (PPID) Spoofing Attacks
- Parent Process ID (PPID) Spoofing
- The return of the spoof part 1: Parent process ID spoofing

## **Process Doppelgänger**

- Lost in Transaction: Process Doppelgänger
- Process Injection: Process Doppelgänger
- Process Doppelgänger – a new way to impersonate a process

## **Process Ghosting**

- What you need to know about Process Ghosting, a new executable image tampering attack
- Process Ghosting Attack

## **Process Herpaderping**

- GitHub - jxy-s/herpaderping
- Process Herpaderping
- Process Herpaderping (Mitre:T1055)

## **Process Hollowing**

- Process Injection: Process Hollowing
- Process Hollowing and Portable Executable Relocations

## **Ghostly Hollowing and Transacted Hollowing**

- GitHub - hasherezade/transacted\_hollowing

---

## Protected Process

- [Unknown Known DLLs](#)
- [Unreal Mode : Breaking Protected Processes](#)
- [The Evolution of Protected Processes – Part 1: Pass-the-Hash Mitigations in Windows 8.1](#)
- [The Evolution of Protected Processes Part 2: Exploit/Jailbreak Mitigations, Unkillable Processes and Protected Services](#)
- [Protected Processes Part 3 : Windows PKI Internals \(Signing Levels, Scenarios, Root Keys, EKUs & Runtime Signers\)](#)
- [Windows Exploitation Tricks: Exploiting Arbitrary Object Directory Creation for Local Elevation of Privilege](#)
- [Injecting Code into Windows Protected Processes using COM - Part 1](#)
- [Injecting Code into Windows Protected Processes using COM - Part 2](#)
- [Do You Really Know About LSA Protection \(RunAsPPL\)?](#)
- [Bypassing LSA Protection in Userland](#)
- [Debugging Protected Processes](#)
- [The End of PPLdump](#)
- [Protecting Windows protected processes](#)
- [Relevance of Security Features Introduced in Modern Windows OS](#)
- [Bypassing LSA Protection \(aka Protected Process Light\) without Mimikatz on Windows 10](#)
- [Debugging the undebuggable and finding a CVE in Microsoft Defender for Endpoint](#)
- [Sandboxing Antimalware Products for Fun and Profit](#)
- [GitHub - elastic/PPLGuard](#)
- [GitHub - gabriellandau/PPLFault](#)
- [PPLdump Is Dead. Long Live PPLdump \(Video\)](#)
- [PPLdump Is Dead. Long Live PPLdump \(Slide\)](#)

## Reflective DLL Injection

- [GitHub - stephenfewer/ReflectiveDLLInjection](#)

---

## **sRDI**

- sRDI – Shellcode Reflective DLL Injection
- GitHub - monoxgas/sRDI
- An Improved Reflective DLL Injection Technique

## **Acknowledgments**

Thanks for your research:

- Tal Liberman (@tal\_liberman)
- Eugene Kogan (@EuKogan)
- hasherezade (@hasherezade)
- Gabriel Landau (@GabrielLandau)
- Forrest Orr (@\_forrestorr)
- Stephen Fewer (@stephenfewer)
- batsec (@\_batsec\_)
- Nick Landers (@monoxgas)