GitHub - 0xTriboulet/Revenant: Revenant - A 3rd party agent for Havoc that demonstrates evasion techniques in the context of a C2 framework

By 0xTriboulet

Archived: 2026-04-05 16:30:27 UTC

Revenant is a 3rd party agent for Havoc written in C, and based on Talon. This implant is meant to expand on the Talon implant by implementing covert methods of execution, robust capabilities, and more customization.

Setup

This project aims to be a self-contained Havoc C2 implant. The goal end-user functionality is as follows:

*****NOTE*** As of August 2023, Havoc 0.6 broke support for 3rd party agents. @C5pider intends to bring the functionality back in a future release, but for the time being use Havoc 0.5 available here: https://github.com/0xTriboulet/Havoc_0.5**

HAVOC (DEV) HAS BEEN PATCHED TO SUPPORT 3RD PARTY AGENTS: https://github.com/HavocFramework/Havoc/tree/dev

> 1. Download repo
> 2. Unzip Revenant.zip
> 3. pip install black
> 4. startup Havoc (./havoc server --profile ./profiles/havoc.yaotl -v --debug & ./havoc client)
> 5. Go to root folder
> 6. python Revenant.py
> 7. ???
> 8. PROFIT

> **x86 and Win 7 Compatability:**
>
> - Disable NativeAPI
>
> > Note: Revenant uses NtCreateUserProcess to deliver NativeAPI functionality.
> > NtCreateUserProcess is not supported by x86 or Win 7

Commands

> - **pwsh** - executes commands through powershell.exe -> pwsh ls
> - **shell** - executes commands through cmd.exe -> shell dir
> - **download** - downloads file to loot folder -> download C:\test.txt
> - **upload** - uploads file to desired folder -> upload /home/test.txt C:\temp\test.txt
> - **exit** - kills current implant -> exit

Options

> - **Sleep** - Set sleep in seconds
> - **Polymorphic** - Enable/Disable polymorphism at build and run time
> - **Obfuscation** - Obfuscate strings with XOR
> - **Arch** - x86/x64
> - **Native** - Use NativeAPI where implemented
> - **AntiDbg** - Leverage antidebug checks at initialization
> - **RandCmdIDs** - Randomize command IDs
> - **Unhooking** - GhostFart/Perun's Fart method to unhook, exec command, then rehook

> Note: RandCmdIDs randomizes the CmdIDs in the output executable. Revenant does **NOT** store these random CmdIDs; these will only work with the active session. If you want a reusable executable, do **NOT** enable this option.

TODO:

> - Add exec-assembly
> - Add cd, ls, whoami commands
> - Decrease entropy

Source: https://github.com/0xTriboulet/Revenant