

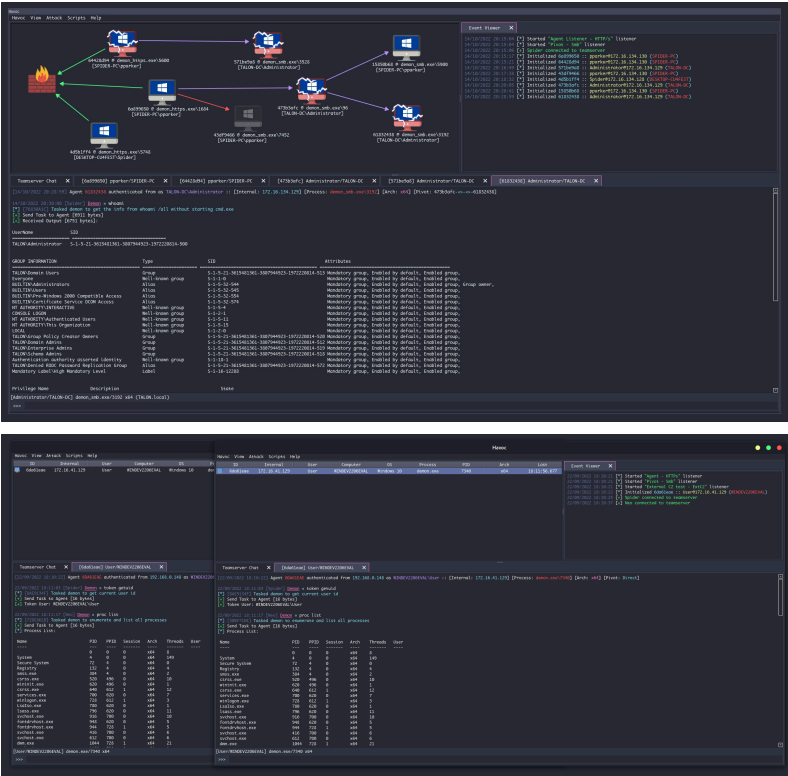
makefile

README GPL-3.0 license



Havoc

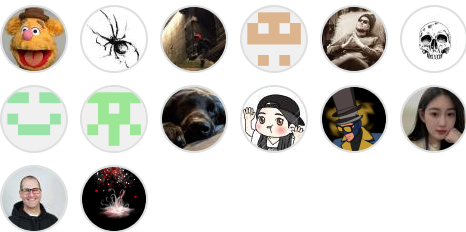
Havoc is a modern and malleable post-exploitation command and control framework, created by [@C5pider](#).



Packages

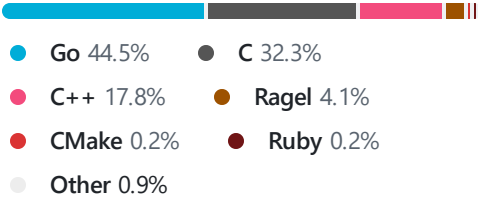
No packages published

Contributors 34



+ 20 contributors

Languages



⚠ Havoc is in an early state of release. Breaking changes may be made to APIs/core structures as the framework matures.

Support

Consider supporting C5pider on [Patreon](#)/[Github Sponsors](#). Additional features are planned for supporters in the future, such as custom agents/plugins/commands/etc.

Quick Start

Please see the [Wiki](#) for complete documentation.

Havoc works well on Debian 10/11, Ubuntu 20.04/22.04 and Kali Linux. It's recommended to use the latest versions possible to avoid issues. You'll need a modern version of Qt and Python 3.10.x to avoid build issues.

See the [Installation](#) docs for instructions. If you run into issues, check the [Known Issues](#) page as well as the open/closed [Issues](#) list.

Features

Client

Cross-platform UI written in C++ and Qt

- Modern, dark theme based on [Dracula](#)

Teamserver

Written in Golang

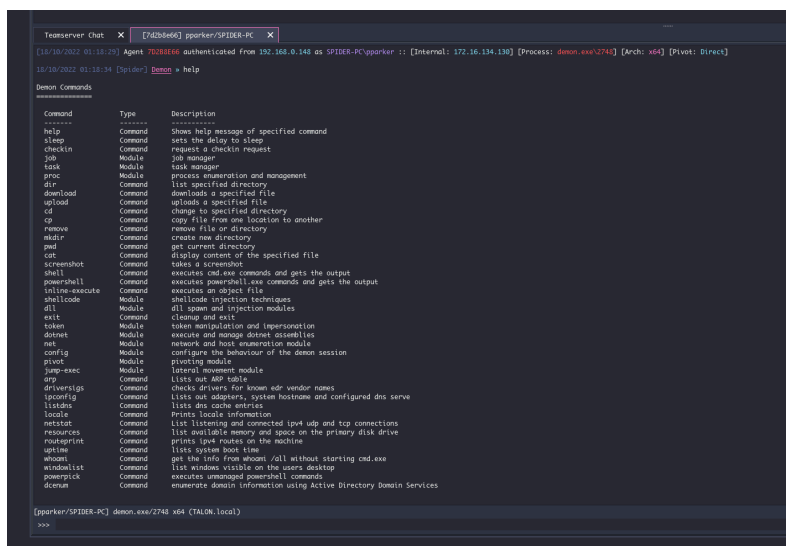
- Multiplayer
- Payload generation (exe/shellcode/dll)
- HTTP/HTTPS listeners
- Customizable C2 profiles

- External C2

Demon

Havoc's flagship agent written in C and ASM

- Sleep Obfuscation via [Ekko](#), Zillean or [FOLIAGE](#)
- x64 return address spoofing
- Indirect Syscalls for Nt* APIs
- SMB support
- Token vault
- Variety of built-in post-exploitation commands
- Patching Amsi/Etw via Hardware breakpoints
- Proxy library loading
- Stack duplication during sleep.



```
Termserver Chat X [762b6d66] pparker/SPIDER-PC X
[18/10/2022 01:18:29] Agent 762b6d66 authenticated from 192.168.0.148 as SPIDER-PC/pparker :: [Internal: 172.16.134.130] [Process: demon.exe/2743] [Arch: x64] [Pivot: Direct]
18/10/2022 01:18:34 [Spider] Demon > help

Demon Commands
=====
Command      Type      Description
-----
cd.exe       Command   Shows help message of specified command
help         Command   Shows help message of specified command
sleep        Command   sets the delay to sleep
checkin      Command   request a checkin request
job          Module    job manager
task         Module    task manager
proc         Module    process enumeration and management
dir          Command   list specified directory
download     Command   downloads a specified file
upload       Command   uploads a specified file
cd           Command   change to specified directory
cp           Command   copy file from one location to another
rm           Command   remove file or directory
mkdir        Command   create new directory
pwd          Command   get current directory
cat          Command   display content of the specified file
screenshot   Command   takes a screenshot
shell        Command   executes cmd.exe commands and gets the output
powershell   Command   executes powershell.exe commands and gets the output
inline-execute Command   executes an object file
shellcode    Module    shellcode injection techniques
dll          Module    dll spawn and injection modules
exit         Command   cleanup and exit
token        Module    token manipulation and impersonation
dotnet       Module    execute and manage dotnet assemblies
net          Module    network and host enumeration module
config       Module    configure the behaviour of the demon session
privat       Module    pivoting module
jump-exec    Module    lateral movement module
arp          Command   lists arp table
driversigs   Command   checks drivers for known edr vendor names
spconfig     Command   lists net adapters, system hostname and configured dns serve
listads     Command   lists dns cache entries
locale       Command   Prints locale information
netstat      Command   list listening and connected ipv4 udp and tcp connections
resources    Command   list available memory and space on the primary disk drive
routeprint   Command   prints ipv4 routes on the machine
uptime       Command   lists system boot time
whoami       Command   get the info from whoami /all without starting cmd.exe
windowlist   Command   list windows visible on the users desktop
powercat     Command   executes unmanaged powershell commands
dcom         Command   enumerate dcoms information using Active Directory Domain Services

[pparker/SPIDER-PC] demon.exe/2743 x64 (TALON: local)
>>>
```

Extensibility

- [External C2](#)
- Custom Agent Support
 - [Talon](#)
- [Python API](#)
- [Modules](#)

Community

You can join the official [Havoc Discord](#) to chat with the community!

Contributing

To contribute to the Havoc Framework, please review the guidelines in [Contributing.md](#) and then open a pull-request!

Note

Please do not open any issues regarding detection.

The Havoc Framework hasn't been developed to be evasive. Rather it has been designed to be as malleable & modular as possible. Giving the operator the capability to add custom features or modules that evades their targets detection system.

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.