

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Search

Sign in

Sign up

BC-SECURITY / Empire

Public

forked from

EmpireProject/Empire

<> Code

Issues61

Pull requests6

Discussions

Actions

Projects

Wiki

Security

Insights

main

Go to file

<> Code

This branch is 1934 commits ahead of EmpireProject/Empire:master.

vinnybod

Merge pull request #750 from B...

ee6526b · 2 months ago

3,443 Commits

.github	attempt to fix docker action (EmpirePro...	3 months ago
docs	Added route4me logo to docs	3 months ago
empire	Update starkiller version to v2.8.2	2 months ago
setup	5.10 updates (EmpireProject#784)	9 months ago
.dockerignore	Python 3.12 (#716)	last year
.gitignore	Remove starkiller submodule (#595)	last year
.gitmodules	Added Threadlessinject module (Empire...	4 months ago
.pre-commit-config.yaml	Add FURB, SLF, RET to Ruff (EmpireProj...	4 months ago
.python-version	Python 3.12 (#716)	last year
CHANGELOG.md	Merge branch 'main' into release/5.11.5	2 months ago
Dockerfile	5.10 updates (EmpireProject#784)	9 months ago
LICENSE	Update LICENSE (#27)	4 years ago
README.md	Added AC3 sponsor logo (#746)	2 months ago
changelog	use changelog.md format (#309)	2 years ago
conftest.py	Agent checkins (#618)	last year
empire.py	New ruff rules (EmpireProject#839)	5 months ago
poetry.lock	Add FURB, SLF, RET to Ruff (EmpireProj...	4 months ago
ps-empire	Updated to startup and install (Empire...	8 months ago
pyproject.toml	Prepare release 5.11.5 private	2 months ago
pytest.ini	Python 3.12 (#716)	last year

README

BSD-3-Clause license

About

Empire is a post-exploitation and adversary emulation framework that is used to aid Red Teams and Penetration Testers.

bc-security.gitbook.io/empire-wiki/

hacktoberfest

empire

c2

redteam-infrastructure

Readme

BSD-3-Clause license

Activity

Custom properties

4.2k stars

103 watching

576 forks

Report repository

Releases77

v5.11.5

Latest

on Sep 22

+ 76 releases

Sponsor this project

BC-SECURITY BC Security

Sponsor

Learn more about GitHub Sponsors

Packages

No packages published

Languages

PowerShell93.4%

Python6.0%

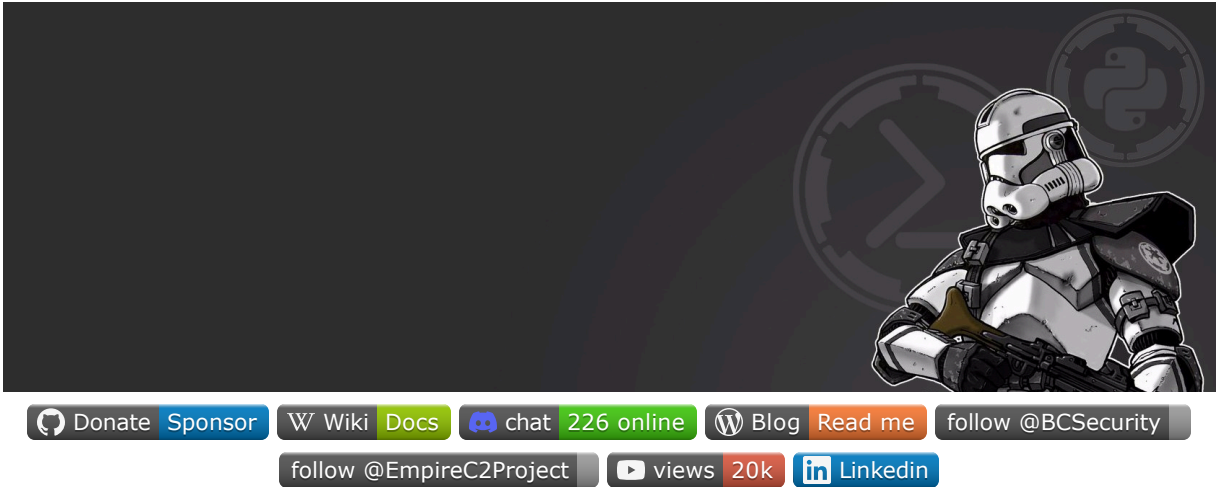
C#0.6%

Shell0.0%

Objective-C0.0%

HTML0.0%

Page 1 of 4



## Empire

Empire is a post-exploitation and adversary emulation framework that is used to aid Red Teams and Penetration Testers. The Empire server is written in Python 3 and is modular to allow operator flexibility. Empire comes built-in with a client that can be used remotely to access the server. There is also a GUI available for remotely accessing the Empire server, [Starkiller](#).

### Features

- Server/Client Architecture for Multiplayer Support
- Supports GUI & CLI Clients
- Fully encrypted communications
- HTTP/S, Malleable HTTP, OneDrive, Dropbox, and PHP Listeners
- Massive library (400+) of supported tools in PowerShell, C#, & Python
- Donut Integration for shellcode generation
- Modular plugin interface for custom server features
- Flexible module interface for adding new tools
- Integrated obfuscation using [ConfuserEx 2](#) & [Invoke-Obfuscation](#)
- In-memory .NET assembly execution
- Customizable Bypasses
- JA3/S and JARM Evasion
- MITRE ATT&CK Integration
- Integrated Roslyn compiler (Thanks to [Covenant](#))
- Docker, Kali, ParrotOS, Ubuntu 20.04/22.04, and Debian 10/11/12 Install Support

### Agents

- PowerShell
- Python 3
- C#
- IronPython 3

### Modules

- [Assembly Execution](#)
- [BOF Execution](#)
- [Mimikatz](#)
- [Seatbelt](#)
- [Rubeus](#)
- [SharpSploit](#)
- [Certify](#)
- [ProcessInjection](#)
- And Many More

### Sponsors



## Release Notes

Please see our [Releases](#) or [Changelog](#) page for detailed release notes.

## Quickstart

When cloning this repository, you will need to recurse submodules.

```
git clone --recursive https://github.com/BC-SECURITY/Empire.git
```

Check out the [Installation Page](#) for install instructions.

Note: The `main` branch is a reflection of the latest changes and may not always be stable. After cloning the repo, you can checkout the latest stable release by running the `setup/checkout-latest-tag.sh` script.

```
git clone --recursive https://github.com/BC-SECURITY/Empire.git
cd Empire
./setup/checkout-latest-tag.sh
./ps-empire install -y
```

If you are using the sponsors version of Empire, it will pull the sponsors version of Starkiller. Because these are private repositories, you need to have ssh credentials configured for GitHub. Instructions can be found [here](#).

## Server

```
# Start Server
./ps-empire server

# Help
./ps-empire server -h
```

## Client

```
# Start Client
./ps-empire client

# Help
./ps-empire client -h
```

Check out the [Empire Docs](#) for more instructions on installing and using with Empire. For a complete list of changes, see the [changelog](#).

## Starkiller



[Starkiller](#) is a web application GUI for PowerShell Empire that interfaces remotely with Empire via its API. Starkiller can be ran as a replacement for the Empire client or in a

mixed environment with Starkiller and Empire clients. As of 5.0, Starkiller is packaged in Empire as a git submodule and doesn't require any additional setup.

## Contribution Rules

See [Contributing](#)

## Contributors

A special thanks to the following contributors for their help with Empire:

[@harmj0y](#) [@sixdub](#) [@enigma0x3](#) [@rvrsh3ll](#) [@killswitch\\_gui](#) [@xorrior](#) [@Cx01N](#)  
[@Hubbl3](#) [@Vinnybod](#)

## Official Discord Channel

Join us in [our Discord](#) with any comments, questions, concerns, or problems!

