

main



Go to file

<> Code ▼

## About

Abusing Reddit API to host the C2 traffic, since most of the blue-team members use Reddit, it might be a great way to make the traffic look legit.

reddit

hacking

cybersecurity

pentesting

pentest

c2

redteam

 [Readme](#)

 GPL-3.0 license

 Activity

☆ 253 stars

 7 watching

43 forks

Report repository

## Releases

No releases published

Sponsor this project

# RedditC2

Abusing Reddit API to host the C2 traffic, since most of the blue-team members use Reddit, it might be a great way to make the traffic look legit.



⚠ [Disclaimer]: Use of this project is for **Educational/ Testing purposes only**. Using it on **unauthorised machines is strictly forbidden**. If somebody is found to use it for **illegal/ malicious intent**, author of the repo will **not** be held responsible.

## Requirements

Install **PRAW** library in python3:

```
pip3 install praw
```



## Quickstart

See the [Quickstart guide](#) on how to get going right away!

## Demo

📺 reddit\_c2\_demo.mp4 ▾

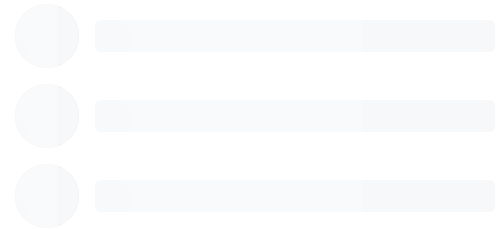
💖 Sponsor

[Learn more about GitHub Sponsors](#)

### Packages

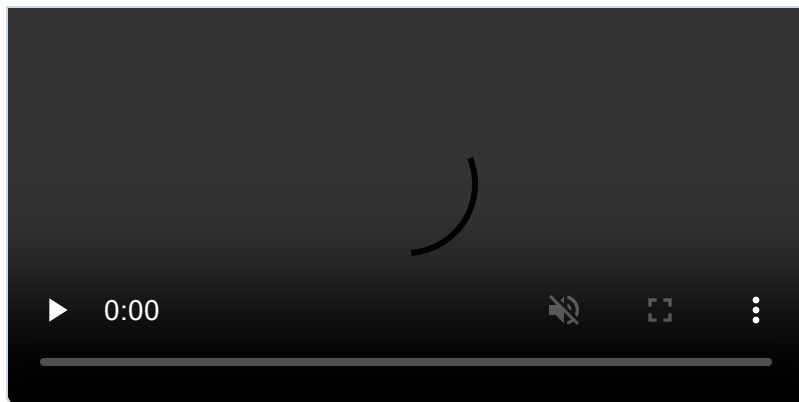
No packages published

### Contributors 3



### Languages





## Workflow

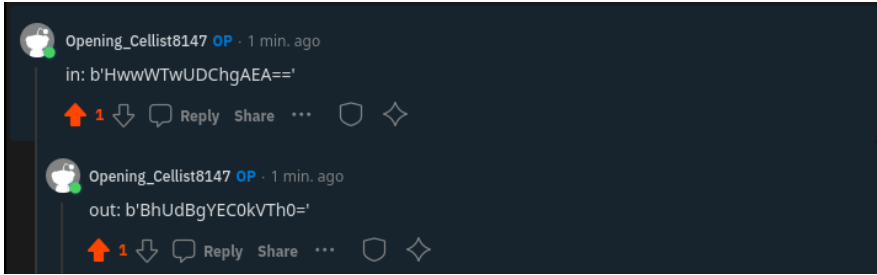
### Teamserver

1. Go to the specific Reddit Post & post a new comment with the command ("in: ")
2. Read for new comment which includes the word "out:"
3. If no such comment is found, go back to step 2
4. Parse the comment, decrypt it and read it's output
5. Edit the existing comment to "executed", to avoid reexecuting it

### Client

1. Go to the specific Reddit Post & read the latest comment which includes "in:"
2. If no new comment is detected, go back to step 1
3. Parse the command out of the comment, decrypt it and execute it locally
4. Encrypt the command's output and reply it to the respective comment ("out:" )

Below is a demonstration of the XOR-encrypted C2 traffic for understanding purposes:



## Scanning results

Since it is a custom C2 Implant, it doesn't get detected by any AV as the behaviour is completely legit.

 **ANTISCAN.ME**

Filename: RedditAgent.exe  
MD5: 8e7c0b33222f0c36329df32ec380ffeb  
Scan date: 30-11-2022 11:37:29

 **Detection** 0/26

 Ad-Aware Antivirus Clean	 Eset NOD32 Antivirus Clean
 AhnLab V3 Internet Security Clean	 Fortinet Antivirus Clean
 Alyac Internet Security Clean	 IKARUS anti.virus Clean
 Avast Internet Security Clean	 F-Secure Anti-Virus Clean
 AVG Anti-Virus Clean	 Malwarebytes Anti-Malware Clean
 Avira Antivirus Clean	 Panda Antivirus Clean
 Webroot SecureAnywhere Clean	 Kaspersky Internet Security Clean
 BitDefender Total Security Clean	 McAfee Endpoint Protection Clean
 BullGuard Antivirus Clean	 Sophos Anti-Virus Clean
 ClamAV Clean	 Trend Micro Internet Security Clean
 Dr.Web Security Space 11 Clean	 Windows Defender Clean
 Emsisoft Anti-Malware Clean	 Zone Alarm Antivirus Clean
 Comodo Antivirus Clean	 Zillya Internet Security Clean

ANTISCAN.ME - NO DISTRIBUTE ANTIVIRUS SCANNER

## TO-DO

☒ Teamserver and agent compatible in Windows/Linux

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



© 2024 GitHub, Inc.