README GPL-3.0 license

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:

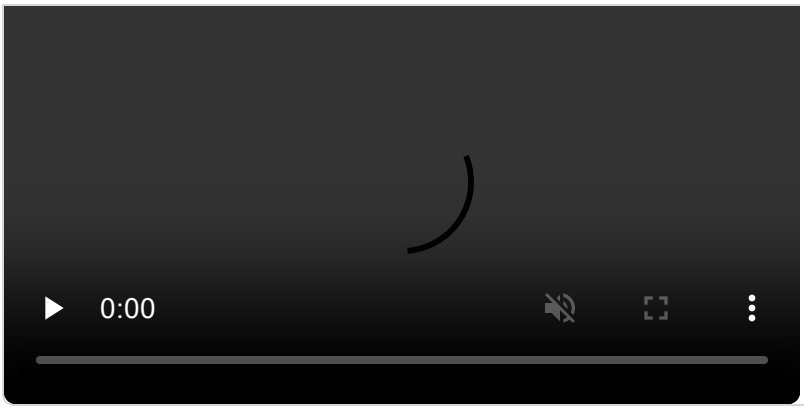
```
pip3 install praw
```

Quickstart

See the Quickstart guide on how to get going right away!

Demo

reddit_c2_demo.mp4



Workflow

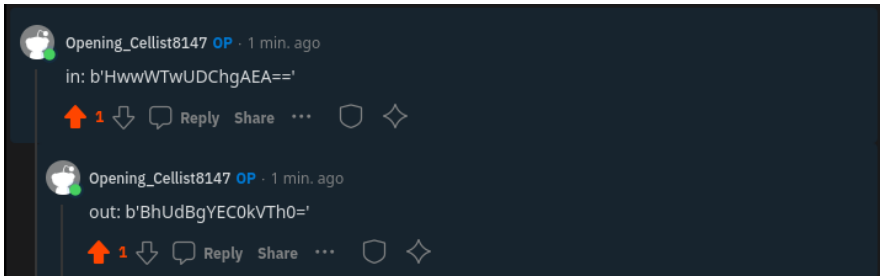
Teamserver

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 bevahiour is completely legit.

TO-DO

- [x] Teamserver and agent compatible in Windows/Linux