mttaggart / OffensiveNotion Public

Notifications Fork 125 Star 1.1k

Code Issues 13 Pull requests Actions Projects Wiki Security Insights

main Go to file Code

mttaggart Merge pull request #139 from m4nbat/m4nb... c12d028 · last year 548 Commits

| | | |
|---|---|---|
| .github | Okay _actually_ fix the mac build | 2 years ago |
| agent | Update deps | last year |
| utils | removing macos from build args for no... | 2 years ago |
| .gitignore | comment in gitignore | 2 years ago |
| CODE_OF_CONDUCT.md | Update CODE_OF_CONDUCT.md | 2 years ago |
| CONTRIBUTING.md | Fix uncomemented line | 2 years ago |
| Dockerfile | fix on dockerfile glob to match one cha... | 2 years ago |
| LICENSE | prompt for AMSI for web delivery, smal... | 2 years ago |
| OffensiveNotion-SigmaRule.yaml | Update OffensiveNotion-SigmaRule.yaml | last year |
| README.md | Update README.md | 2 years ago |
| main.py | Fix launch default | 2 years ago |
| requirements.txt | adding requirements.txt for main.py | 2 years ago |
| rules.yara | Add Yara rules | 2 years ago |

README Code of conduct MIT license

# OffensiveNotion

## Notion (yes, the notetaking app) as a C2.

A collaboration by:

MTTAGGART HUSKYHACKS

Documentation | Pull Requests | Issues

RELEASE: TOLEDO V1.5.0 PRS WELCOME LICENSE MIT

## About

Notion as a platform for offensive operations

Readme
MIT license
Code of conduct
Activity
1.1k stars
16 watching
125 forks
Report repository

## Releases 7

v1.5.0: "Dragon Well" Latest
on Apr 7, 2023

+ 6 releases

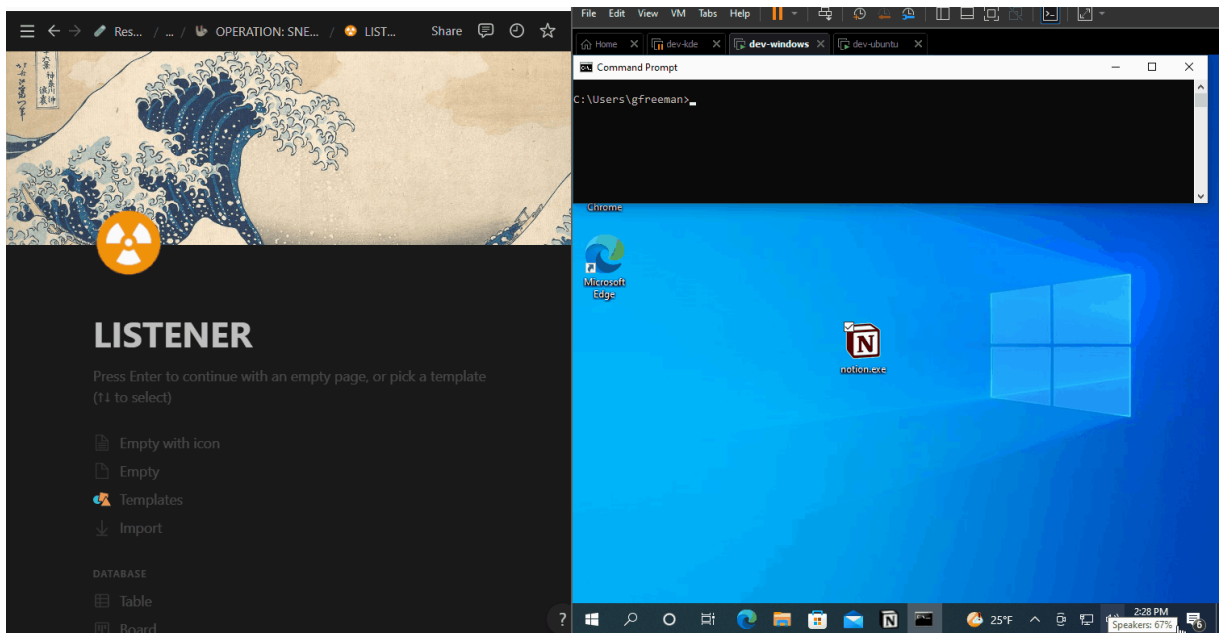
## Packages

No packages published

## Contributors 5

## Languages

Rust 79.3% Python 17.3% YARA 2.1% Dockerfile 1.3%




## Wait, What?

Yes.

## But Why?

What started as a meme grew into a full project. Just roll with it.

## Read more!

Here's our blog post about it: We Put A C2 In Your Notetaking App: OffensiveNotion

# Features

- 📡 A full-featured C2 platform built on the Notion notetaking app.
- 🚧 Easy setup: set up your Notion developer API account, drop the Agent to the target, run and enjoy!
- 🖥️ Cross-platform agent built in Rust that compiles for Linux, Windows, and macOS with the same code base. Includes a Python setup/controller script to simplify the process.
- ☢️ A range of capabilities including port-scanning, privilege escalation, asynchronous command execution, file download, and shellcode injection, all controlled from the comfort of a Notion page!
- 📜 Document as you go! The agent identifies special syntax to run commands, so feel free to use the rest of the Notion page to document your operation.
- 🤝 Collaborative by design! Notion allows for multiple people to edit and view your notes. Your listener page can handle multiple agents and you can invite your red team friends to your page. Congratulations, that's a teamserver!
- 📱 Mobile C2! Use the Notion application from your mobile device to issue commands to your agents from anywhere in the world.
- 🦹 Stealth! C2 comms ride over the Notion API natively. Your C2 traffic looks like someone is using Notion for its intended purpose.

# Quickstart

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

# Documentation

Please see the Wiki for setup, usage, commands, and more!

# Thanks & Acknowledgements

> This project has been a blast for me! I learned a ton about Rust and how the mechanics of a C2 work. So thank you to my co-creator @mttaggart for helping

> me along the way. None of this would have been possible without your technical acumen and creativity.
>
> Thank you to Joe Helle (@joehelle) for the POC steps for the fodhelper UAC bypass.
>
> Thank you to all of the great red team devs who came before me, too numerous to list them all, who have created some of my favorite tools. I'm continually inspired by the red dev innovation in our field.
>
> -Husky

> As a fairly new security person, I had no idea I'd end up working with such a fantastically talented, kind, and reliable partner and hacker as @HuskyHacks. It's been a true privilege to build this alongside him.
>
> I want to thank the Taggart Tech community for supporting us along the way and always offering helpful feedback. This would not be possible without you all.
>
> -Taggart

## Contributors

The dev team would like to thank the following contributors for their work on OffensiveNotion:

| Contributor | Contribution |
| --- | --- |
| @MEhrn00 | Execution guardrails for domain name/joined status 🚀 |
| @hitcxy | Improved shell encoding 🚀 |

---

| Legend |
| --- |
| 🚀 - Issue/PR submitted and code landed |
| 💡 - Cool ideas |
| 🤔 - Consultation/Inspiration |
| 🦎 - Bug submission/fix |

## Disclaimer

There is no way to make an offensive security relevant research tool and release it open source without the possibility of it falling into the wrong hands. This tool is only to be