Medium

Sign up Sign in

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

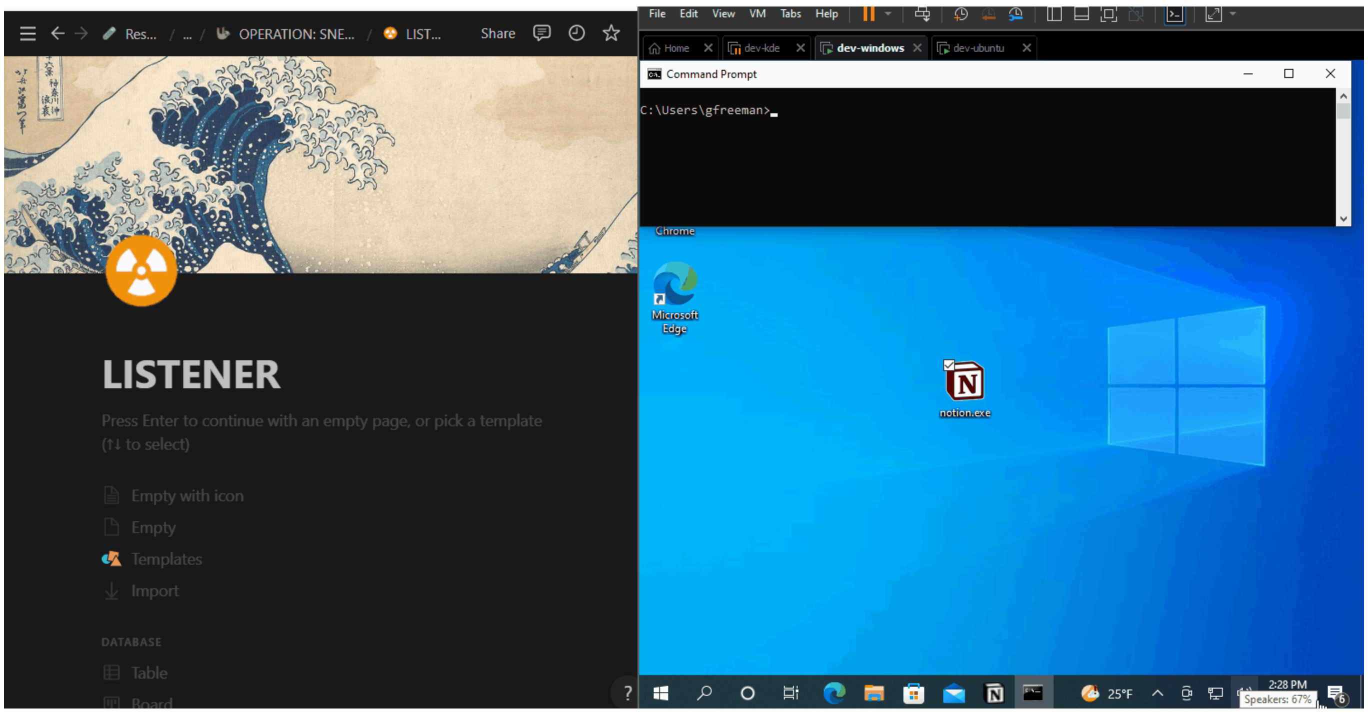
We Put A C2 In Your Notetaking App: OffensiveNotion

A Red Teaming Science Fair Project

HuskyHacks · Follow

6 min read · Feb 27, 2022

140 2



LISTENER

Press Enter to continue with an empty page, or pick a template (↑↓ to select)

Empty with icon
Empty
Templates
Import
DATABASE
Table
Board

```
C:\Users\gfreeman>_
```

tl;dr: We realized you can use the Notion developer API to build a C2 platform. We wrote a cross-platform agent in Rust. It runs on Linux and

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

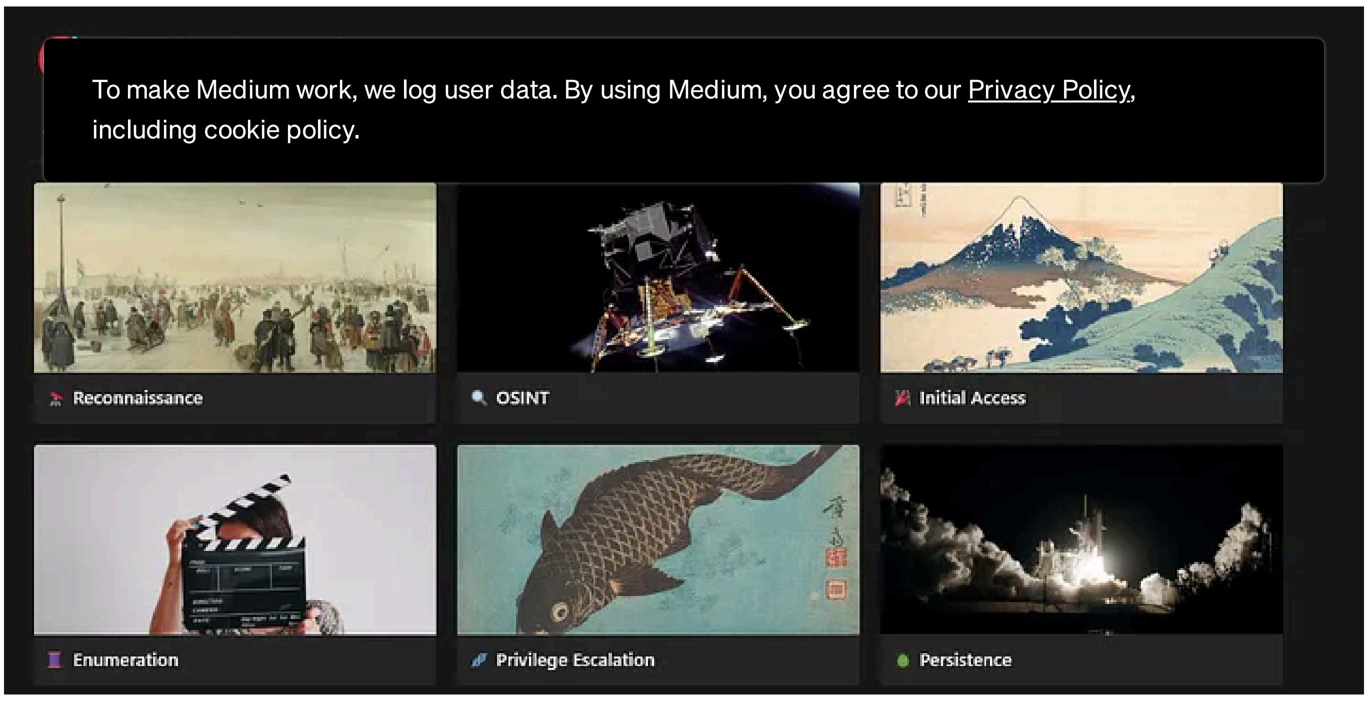
- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Sign up for free

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Try for 5 $/month


To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

An example of one of my notebooks within Notion

One of the features of the Notion platform is the Notion developer API. This API allows you to perform web requests that can add and change data within your Notion notebook. This is accomplished via a standard set of API web request methods. This allows you to create pages, add blocks to pages, and do just about anything else that you can do with the Notion app itself.

This is a story about how we (mttaggart and HuskyHacks) built an entire C2 platform around the Notion developer API.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

The long and short of it was that after speaking to the Notion developers, they informed me that this was intended functionality for the platform. Unlimited S3 AWS phishing links! Sweet!

This was the genesis of our interest in Notion for red team operations.

Shortly after this, Taggart examined the Notion developer API. Taggart is an absolute wizard when it comes to web application shenanigans, so I watched on in awe as he formed a Python script to programmatically read blocks, evaluate their contents, perform some kind of command as a result of those contents, and post the results to a specified Notion page in his notebook. We topped it off with my personal favorite feature: the command was evaluated if and only if there was a 🎯 emoji at the end. This led to a code snippet that I believe deserves to be in the Smithsonian as a relic of landmark technology:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

… then could we make a C2 that uses the Notion platform to control an ag

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

Narrator: Yes, indeed, they could.

Coding began in mid January. The first attempt was to make an agent in Nim.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

The “Listener” page with multiple agent sessions.

As of the end of February 2022, OffensiveNotion is in version 1.0.0 “Iron Age.” We call it this because every time we thought of a cool feature to implement, having drawn inspiration from other C2s we love like Cobalt Strike and Empire, we’d try to remind ourselves that we were still in the Stone Age of this project’s development. We settled on a core set of features for the evolution into the Iron Age. Someday we’ll hit the Space Age and send a rocket ship to Alpha Centauri to achieve the Space Race victory condition.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

challenge to work through. In short, we needed to focus on granting robust
co
he

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

Learning how to do this in Rust was a doozy for me! In Taggart's words, "Rust is the old school martial arts instructor that used to hit my legs with a pole when my stance was not low enough." I went several rounds with the Rust compiler night after night during this project and I can say that is 100% true. But I have no doubt it has made me into a better developer.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

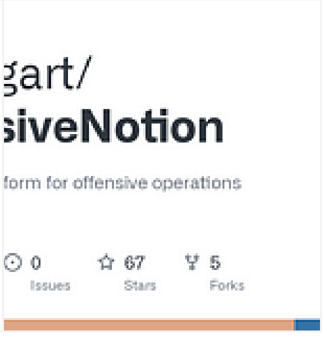
Nothing to see here, blue teamers. Move along.

We wrote a whole section of the wiki on OPSEC. Check it out here if you’re interested:

7. OPSEC Considerations · mttaggart/OffensiveNotion Wiki

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or...

github.com



In short, this is a LOTS (living off trusted sites) goldmine and makes for incredibly sneaky C2 capacities.

Closing Thoughts

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Thank you for reading! We hope you enjoyed this article

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

*n

edit 2/27: typo

edit 2/28: embeds instead of links

Hacker Cybersecurity Infosec Red Team

140 2

Written by HuskyHacks

60 Followers

Follow

Recommended from Medium

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Tech & Tools

Medium's Huge List of

To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

Staff Picks

755 stories · 1416 saves

Natural Language Processing

1788 stories · 1391 saves

Alexander Nguyen in Level Up Coding

The resume that got a software engineer a $300,000 job at Google.

1-page. Well-formatted.

✦ Jun 1 25K 483

Sanskar Kalra

Game of Active Directory: Pentesting Strategies for Real-...

Introduction

Aug 16 3 1

AbhirupKonwar in OSINT Team

Bug Hunting Recon Methodology | Part2 | LegionHunter

backdoor

Setting Up Mythic C2: A Guide to Evading Advanced Detection...

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app