TryHackMe Room Write-up

Title: Operation Slither

Description: Follow the lead and find who’s behind the operation.

Author: Igor Buszta

The Leader

Description: *We got access to a hacker forum and found the info of our company on sale! All the info we have is in this post. Find any information related to the leader of the Sneaky Viper group.*

Full user database TryTelecomMe on sale!!!

As part of Operation Slither, we've been hiding for weeks in their network and have now started to exfiltrate information.

This is just the beginning. We'll be releasing more data soon. Stay tuned!

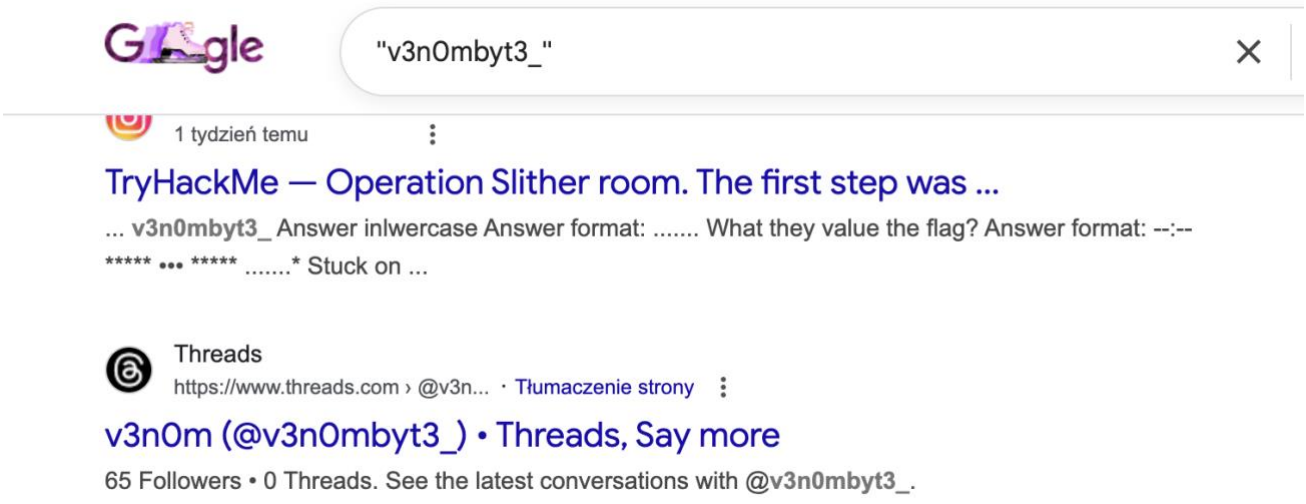
*@v3n0mbyt3_*

Objective: Aside from Twitter / X, what other platform is used by v3n0mbyt3

What is the value of the flag?

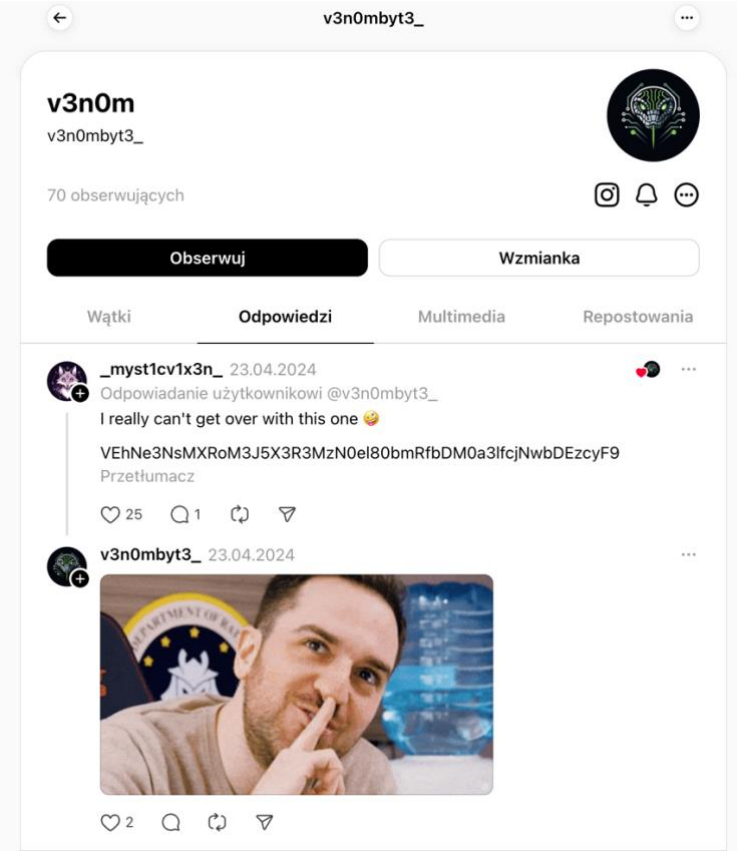
Tools: Browser

We have his full nickname, so all we have to do is to use Google to find all sites where his nickname is mentioned. Use quotation marks to limit search results to those where there is wanted string.



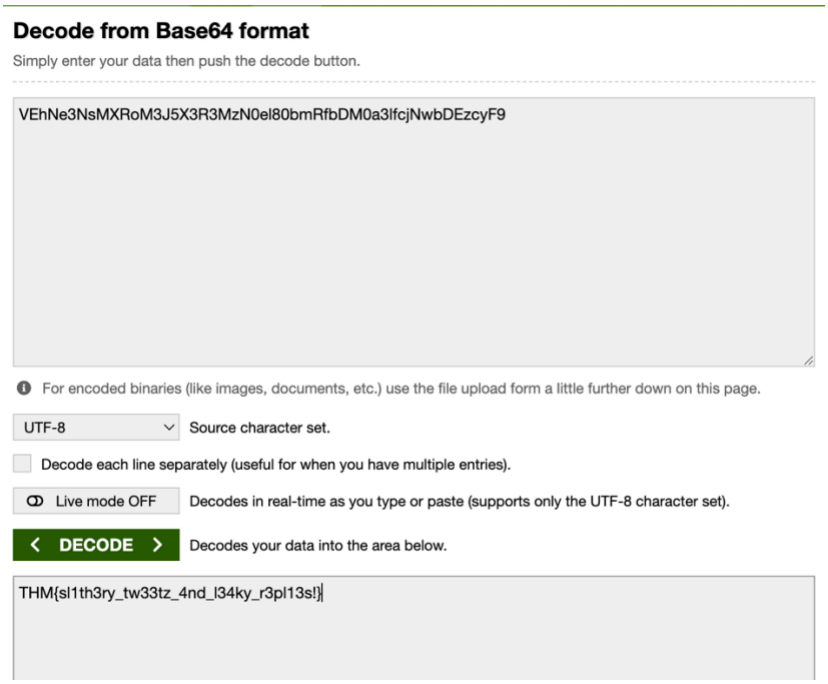
Picture 1: v3n0mbyt3_ profile on Threads.

We have our platform. Let’s visit his profile and search for flag.



Picture 2: Replies from v3n0m's profile.

We find this interesting message being mentioned by another user. It seems like it's encoded. Most of the CTFs encode message with base64, so let's see if it's used again in this room.



Picture 3: Online base64 decoder with flag.

The Sidekick

Description: *A second message has been made public! Our accountt in their forum was deleted, so we couldn't get the operator's handle this time. Follow the crumbs from the first task and hunt any information related to the second operator of the group.*

60GB of data owned by TryTelecomMe is now up for bidding!

Number of users: 64500000 Accepting all types of crypto

For takers, send your bid on Threads via this handle:

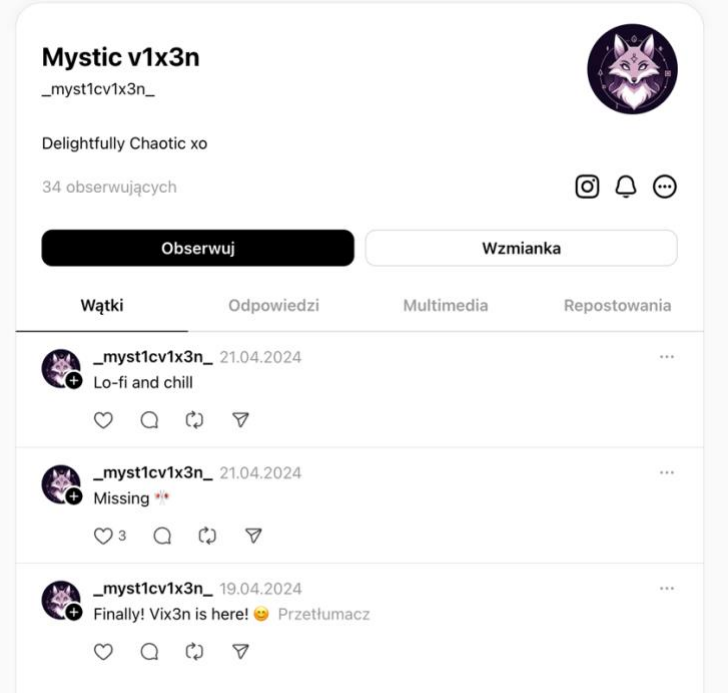
HIDDEN CONTENT

You must register or log in to view this content

Objective: What is the username of the second operator talking to v3n0mbyt3 from the previous platform?
What is the value of the flag?

Tools: Browser

The first task is already completed. We've seen this other profile on Threads.

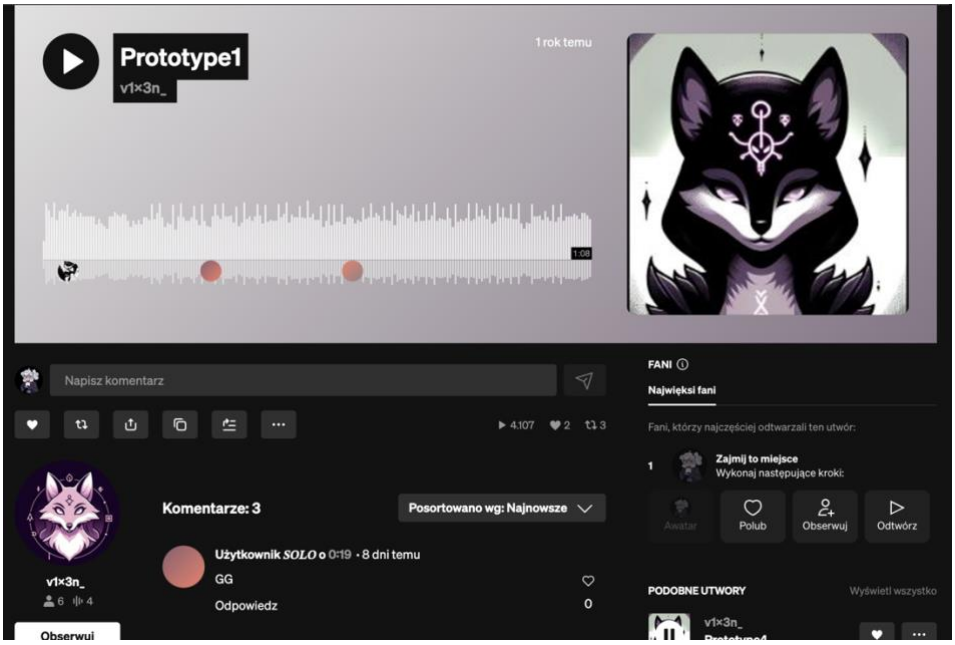


Picture 4: Sidekick's profile on Threads.

Oh, his Instagram profile is linked. Let's visit and search for flag there (let's ignore all the comments and look for ourselves!).

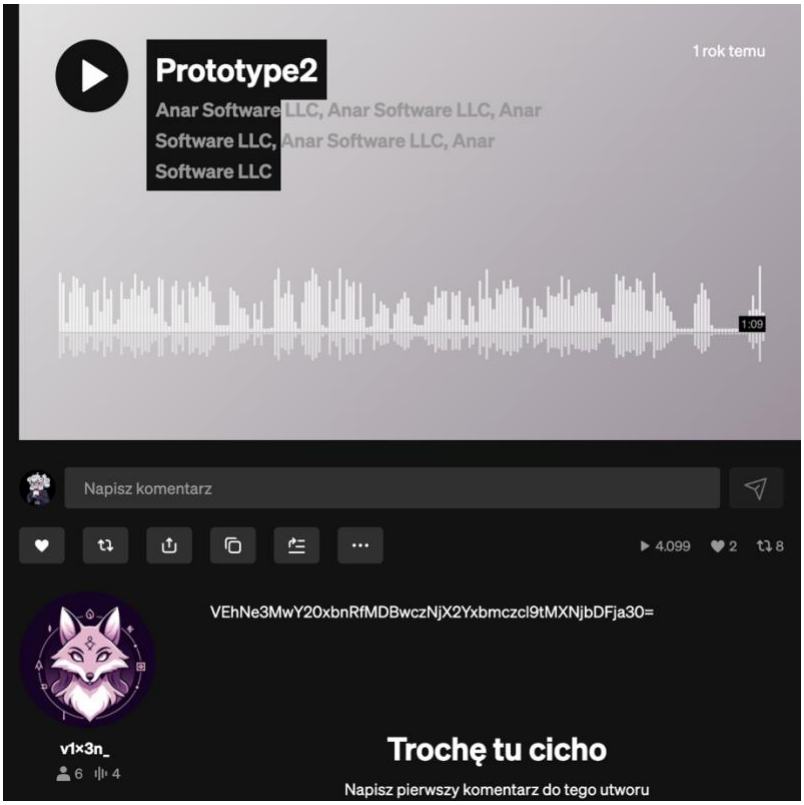
Picture 5: Instagram reel published on sidekick's profile.

All the other posts are empty, but here we've found a link to his profile on Soundcloud.



Picture 6: Sidekick's Lo-Fi song.

If you look to the right, there are 4 songs in total published by the Sidekick.



Picture 7: Prototype2 song with flag in description.

There's a flag in Prototype2's description.

The Last Operator

Description: *A new post is up. Hunt the third operator using past discoveries and find any details related to the infrastructure used for the attack.*

FOR SALE

Advanced automation scripts for phishing and initial access!

Inclusions:

- Terraform scripts for a resilient phishing infrastructure

- Updated Google Phishlet (evilginx v3.0)

- GoPhish automation scripts

- Google MFA bypass script

- Google account enumerator

- Automated Google brute-forcing script

- Cobalt Strike aggressor scripts

- SentinelOne, CrowdStrike, Cortex XDR bypass payloads

PRICE: $1500

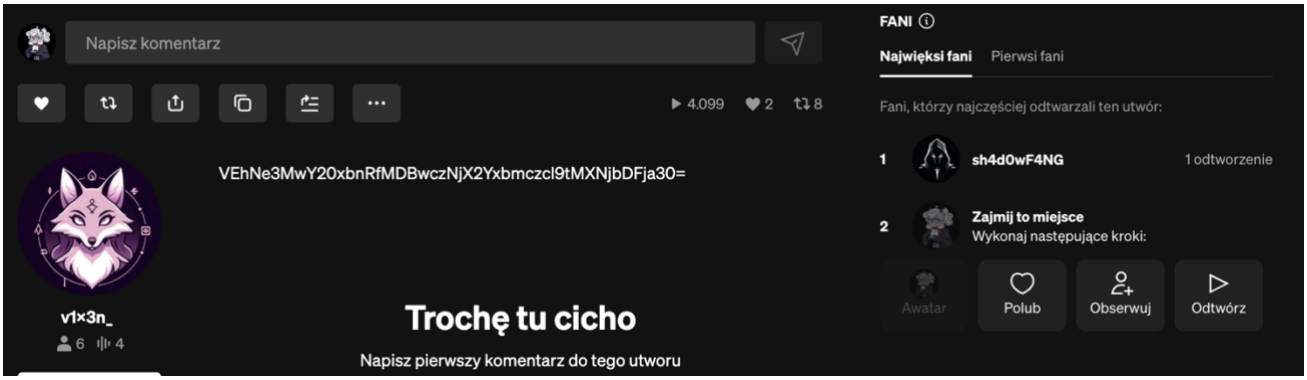
Accepting all types of crypto

Contact me on REDACTED@protonmail.com

Objective: What is the handle of the third operator? What other platform does the third operator use? What is the value of the flag?

Tools: Browser

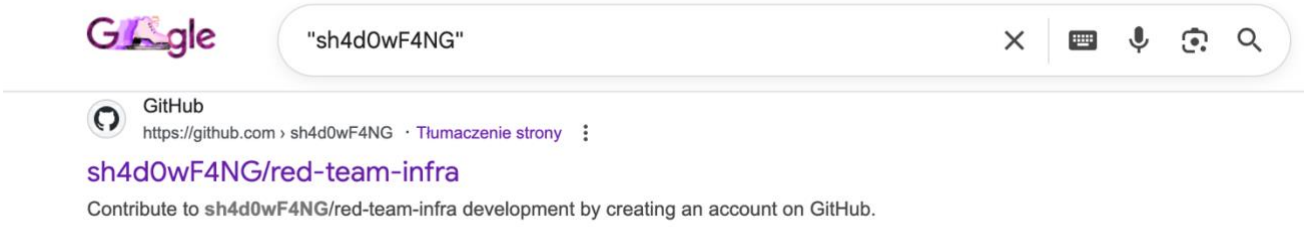
Let's go back to where we last finished.



Picture 8: Prototype2's description and listeners.

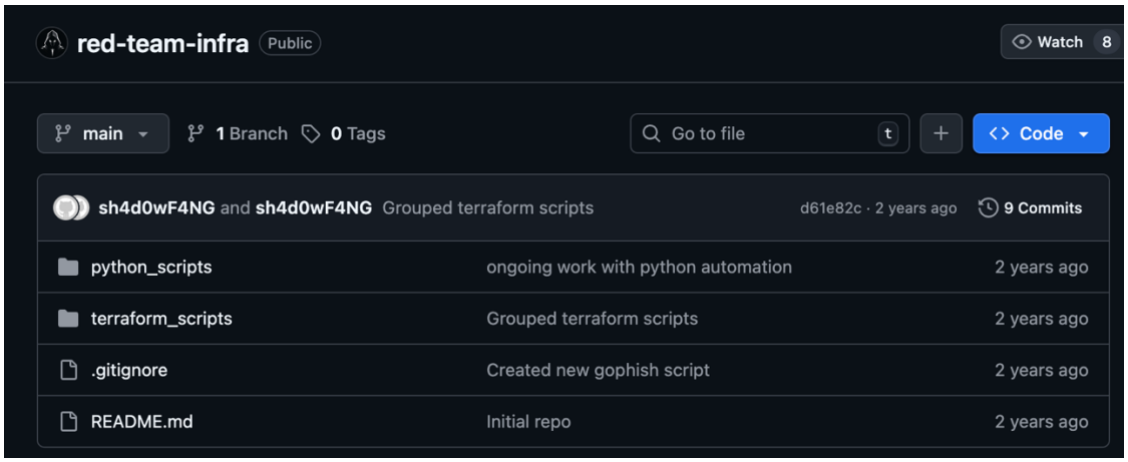
There's one user, sh4d0wF4NG, who played this song once. This must be our Last Operator.

We once again use search browser to look for other platforms he's on.



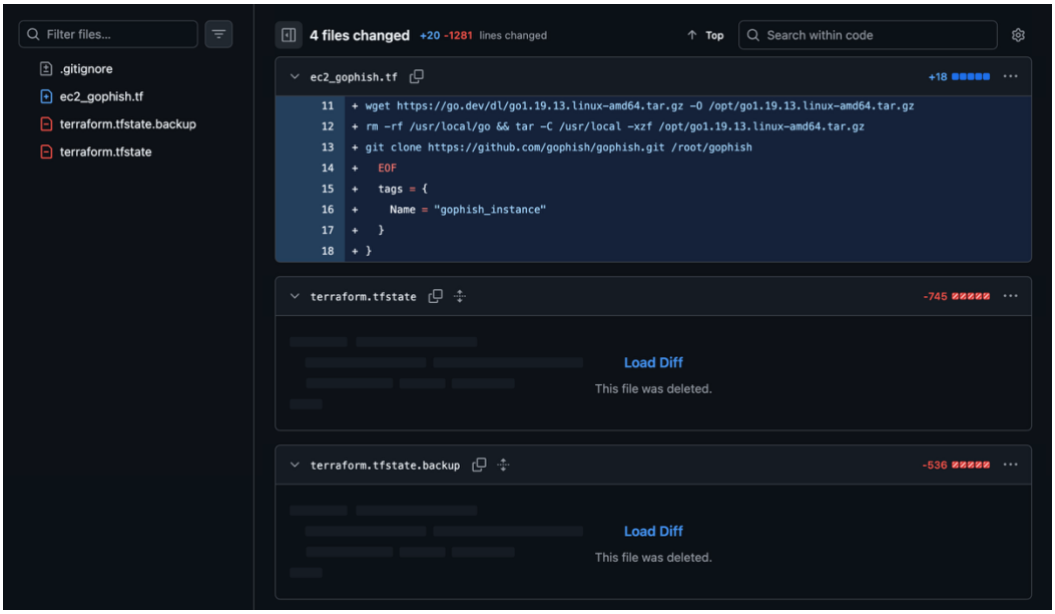
Picture 9: Last Operator's github.

Now let's look at the code.



Picture 10: Last Operator's repo.

I did go through all the scripts, but found nothing. But as we can see, there were 9 commits. Let's see what he changed in his code.



Picture 11: sh4d0wF4NG's commits.

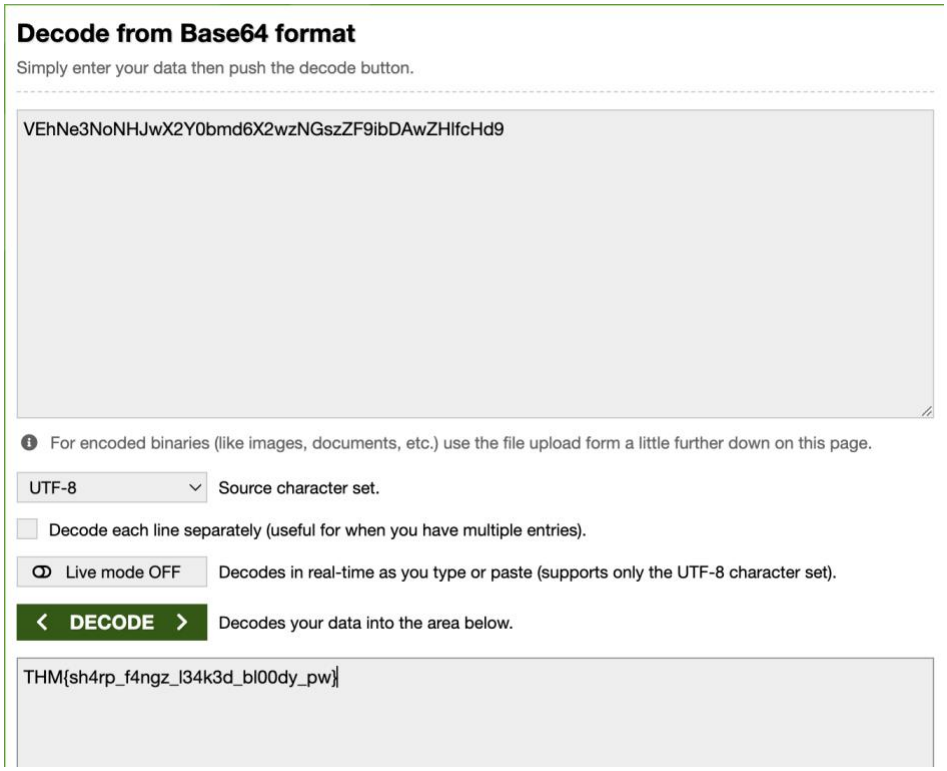
We can see 2 deleted files that we can recover.

terraform.tfstate -745

```
@@ -1,745 +0,0 @@
- {
-   "version": 4,
-   "terraform_version": "1.6.6",
-   "serial": 36,
-   "lineage": "f09bb25f-e5e7-1579-ce76-95fe4bcb1aa7",
-   "outputs": {
-     "shadow-password": {
-       "value": "VEhNe3NoNHJwX2Y0bmd6X2wzNGszZF9ibDAwZHlfcHd9"
-       "type": "string"
```

Picture 12: Recovered file.

There's shadow password with interesting value, probably encoded with base64. Let's decode it real quick.



Picture 13: Decoded flag.