

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.

"v3n0mbyt3_"

TryHackMe — Operation Slither room. The first step was ...

... v3n0mbyt3_ Answer in lowercase Answer format: What they value the flag? Answer format: --:--
***** *** ***** * Stuck on ...

Threads
https://www.threads.com › @v3n... · Tłumaczenie strony

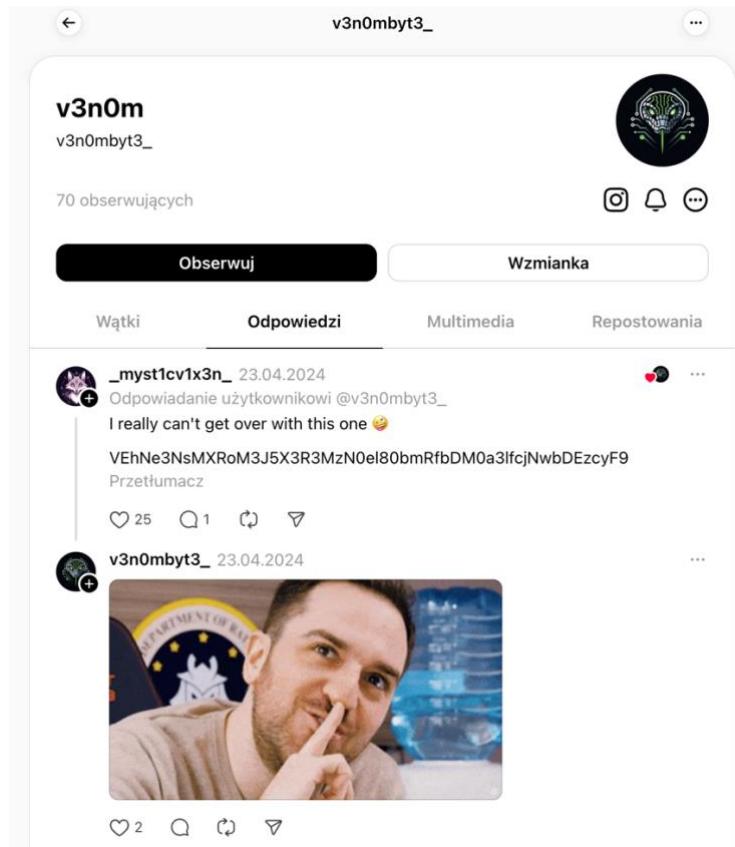
v3n0m (@v3n0mbyt3_) • Threads, Say more

65 Followers • 0 Threads. See the latest conversations with @v3n0mbyt3_.

Picture 1: v3n0mbyt3_ profile on Threads.

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

Igor Buszta
ROOM: OPERATION SLITHER



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.

Decode from Base64 format
Simply enter your data then push the decode button.

VEhNe3NsMXRoM3J5X3R3MzN0el80bmRfbDM0a3lfcjNwbDEzcyF9

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
THM{sl1th3ry_tw33tz_4nd_l34ky_r3pl13s!}
```

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:

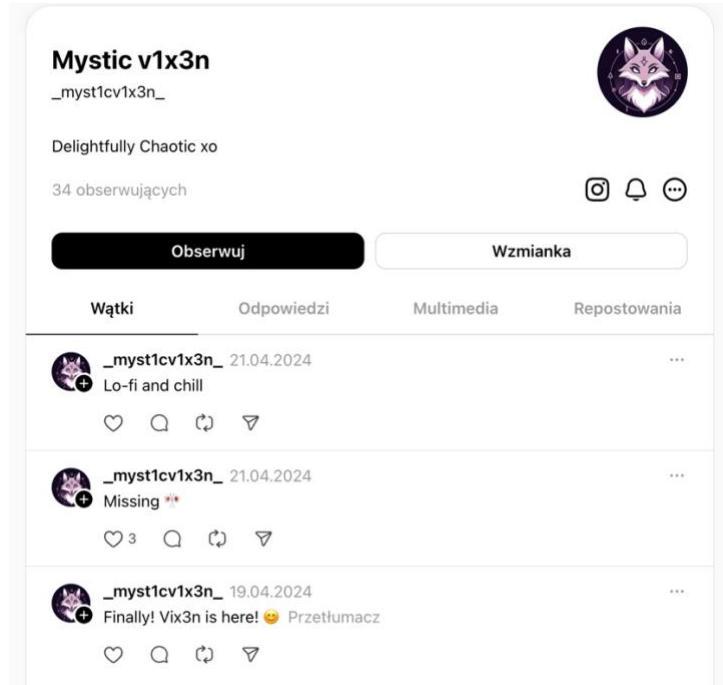
HIDDEN CONTENT

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.

Igor Buszta
ROOM: OPERATION SLITHER

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



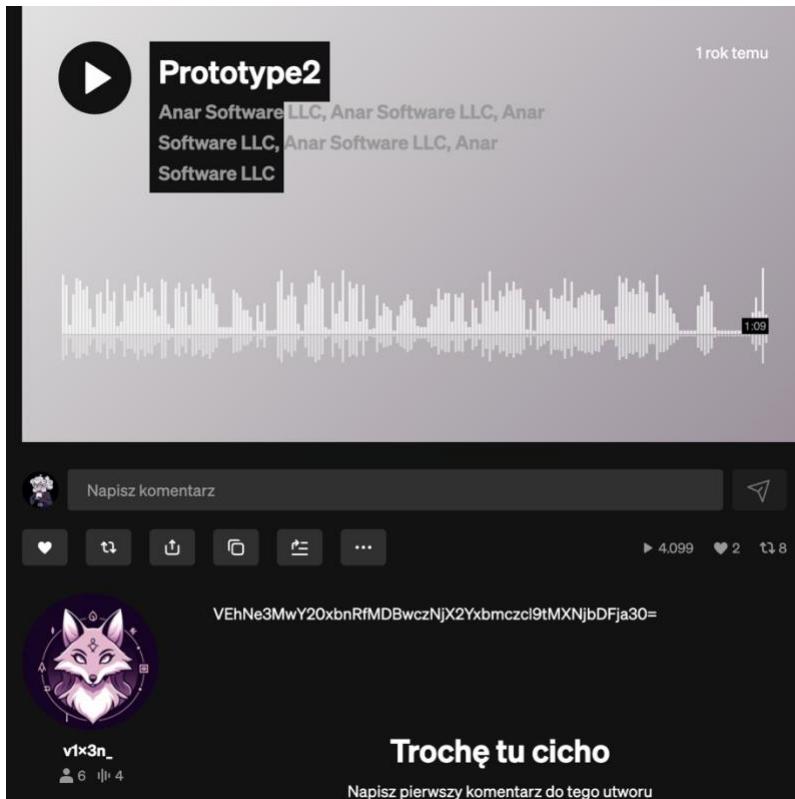
Picture 5: Instagram reel published on sidekick's profile.

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

The image shows a screenshot of a SoundCloud track page. The track is titled "Prototype1" by the user `v1x3n_`. The page includes a play button, a waveform, and a fan art image of a fox-like character with a stylized face. The track was posted one year ago. Below the track information, there is a comment section with three comments. The first comment is from the user `v1x3n_` and says "Napisz komentarz". The second comment is from the user `GG` and says "Odpowiedz". The third comment is from the user `Użytkownik SOLO` and says "0:19 • 8 dni temu". The page also features a "FANI" section, a "Zajmij to miejsce" button, and various interaction buttons like "Avatar", "Polub", "Obserwuj", and "Odtwórz".

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

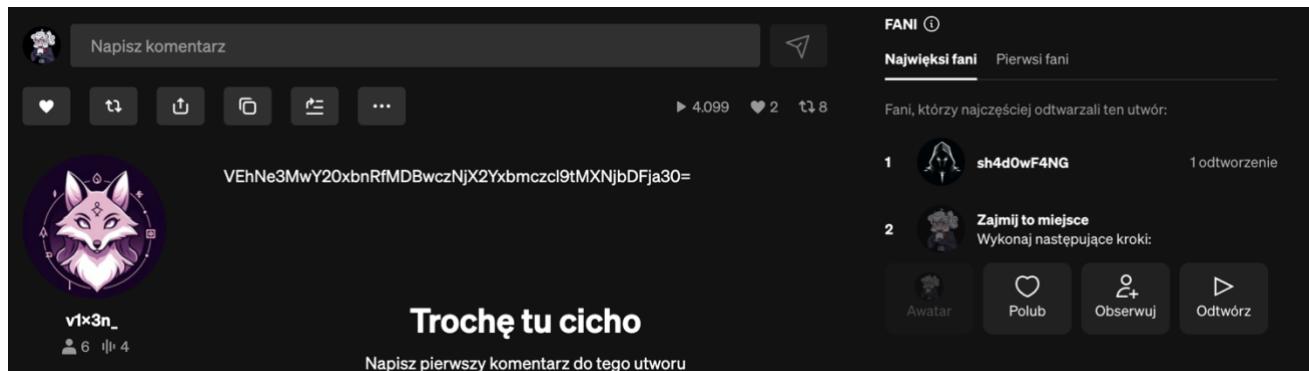
Accepting all types of crypto

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.

The screenshot shows a Google search result for the query "sh4d0wF4NG". The top result is a GitHub repository named "sh4d0wF4NG/red-team-infra". The repository has 8 stars and 9 commits. It contains several files: .gitignore, README.md, python_scripts, and terraform_scripts. The repository was created 2 years ago and has 1 branch and 0 tags.

Picture 9: Last Operator's github.

Now let's look at the code.

The screenshot shows the GitHub repository "red-team-infra" with 9 commits. The commits are:

File	Description	Date
.gitignore	Created new gophish script	2 years ago
README.md	Initial repo	2 years ago
python_scripts	ongoing work with python automation	2 years ago
terraform_scripts	Grouped terraform scripts	2 years ago
sh4d0wF4NG and sh4d0wF4NG	Grouped terraform scripts	d61e82c · 2 years ago

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.

The screenshot shows a GitHub commit history with 4 files changed. The changes are:

- ec2_gophish.tf**: +20 -1281 lines changed.
Content:

```
11 + wget https://go.dev/dl/goi.19.13.linux-amd64.tar.gz -O /opt/goi.19.13.linux-amd64.tar.gz
12 + rm -rf /usr/local/go && tar -C /usr/local -xzf /opt/goi.19.13.linux-amd64.tar.gz
13 + git clone https://github.com/gophish/gophish.git /root/gophish
14 +
15 + EOF
16 +
17 + tags = {
18 +   Name = "gophish_instance"
19 +
20 }
```
- terraform.tfstate**: -745 lines changed.
Content:

This file was deleted.
- terraform.tfstate.backup**: -536 lines changed.
Content:

This file was deleted.

Picture 11: sh4d0wF4NG's commits.

We can see 2 deleted files that we can recover.

The screenshot shows a terminal window with the file 'terraform.tfstate' open. The file contains JSON-like data with several fields, including 'version', 'terraform_version', 'serial', 'lineage', and an 'outputs' section containing a 'shadow-password' entry with a value that appears to be encoded.

```
... @@ -1,745 +0,0 @@
1   - {
2     - "version": 4,
3     - "terraform_version": "1.6.6",
4     - "serial": 36,
5     - "lineage": "f09bb25f-e5e7-1579-ce76-95fe4bc1aa7",
6     - "outputs": {
7       - "shadow-password": {
8         - "value": "VEhNe3NoNHJwX2Y0bmd6X2wzNGszZF9ibDAwZHlfchD9"
9       - "type": "string"
}
```

Picture 12: Recovered file.

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

The screenshot shows a web-based tool for decoding Base64 data. The input field contains the string 'VEhNe3NoNHJwX2Y0bmd6X2wzNGszZF9ibDAwZHlfchD9'. The character set is set to 'UTF-8'. The 'Live mode OFF' option is selected. The 'DECODE' button is highlighted in green. The output field shows the decoded result: 'THM[sh4rp_f4ngz_l34k3d_b100dy_pw]'.

Decode from Base64 format
Simply enter your data then push the decode button.

```
VEhNe3NoNHJwX2Y0bmd6X2wzNGszZF9ibDAwZHlfchD9
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set: UTF-8

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
THM[sh4rp_f4ngz_l34k3d_b100dy_pw]
```

Picture 13: Decoded flag.