Industrial Intrusion — OSINT 1 Walkthrough

🕵️‍♂️ OSINT 1 — Tracing a Phishing Campaign

Tags: #TryHackMe #OSINT #Phishing #CyberThreatIntel #DigitalForensics #CTF #Infosec

Scenario

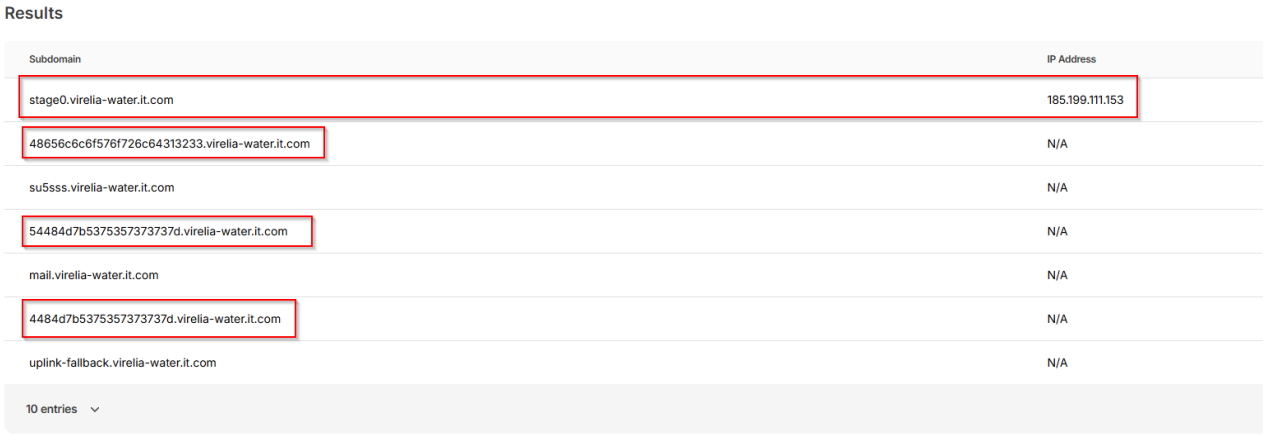
> *“Hexline, we need your help investigating the phishing attack from 3 months ago. We believe the threat actor hijacked our domain **virelia-water.it.com** and used it to host their infrastructure during the campaign.”*

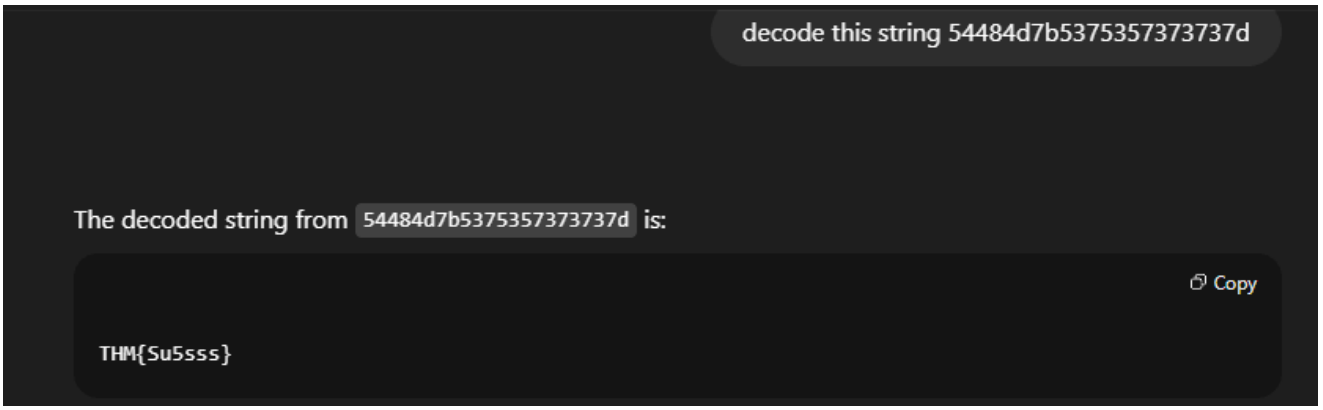
Objective: Identify subdomains tied to virelia-water.it.com and extract any critical infrastructure details from them.

Approach:

1. Recon via Subdomain Enumeration: First step, as always, was to enumerate subdomains of the target. For this, I relied on web-based tools like Shodan and Pentest-Tools, which quickly brought up a handful of relevant subdomains. The most interesting one was 54484d7b5375357373737d.virelia-water.it.com. This subdomain’s odd format stood out to me immediately — it looked like a hexadecimal string.
2. Decoding the Hex String: A quick conversion of this hex string revealed it to be the flag I was after. It's a common technique in red teaming to find such obfuscations and break them down. In this case, the decoded flag was: Flag: THM{Su5sss}
3. Tools Used:

- Shodan
- DNSDumpster
- Pentest-Tools Subdomain Finder





First flag that i found was

```
THM{Su5sss}
```