**Analyzing Potential Command and Control Communication using ELK**

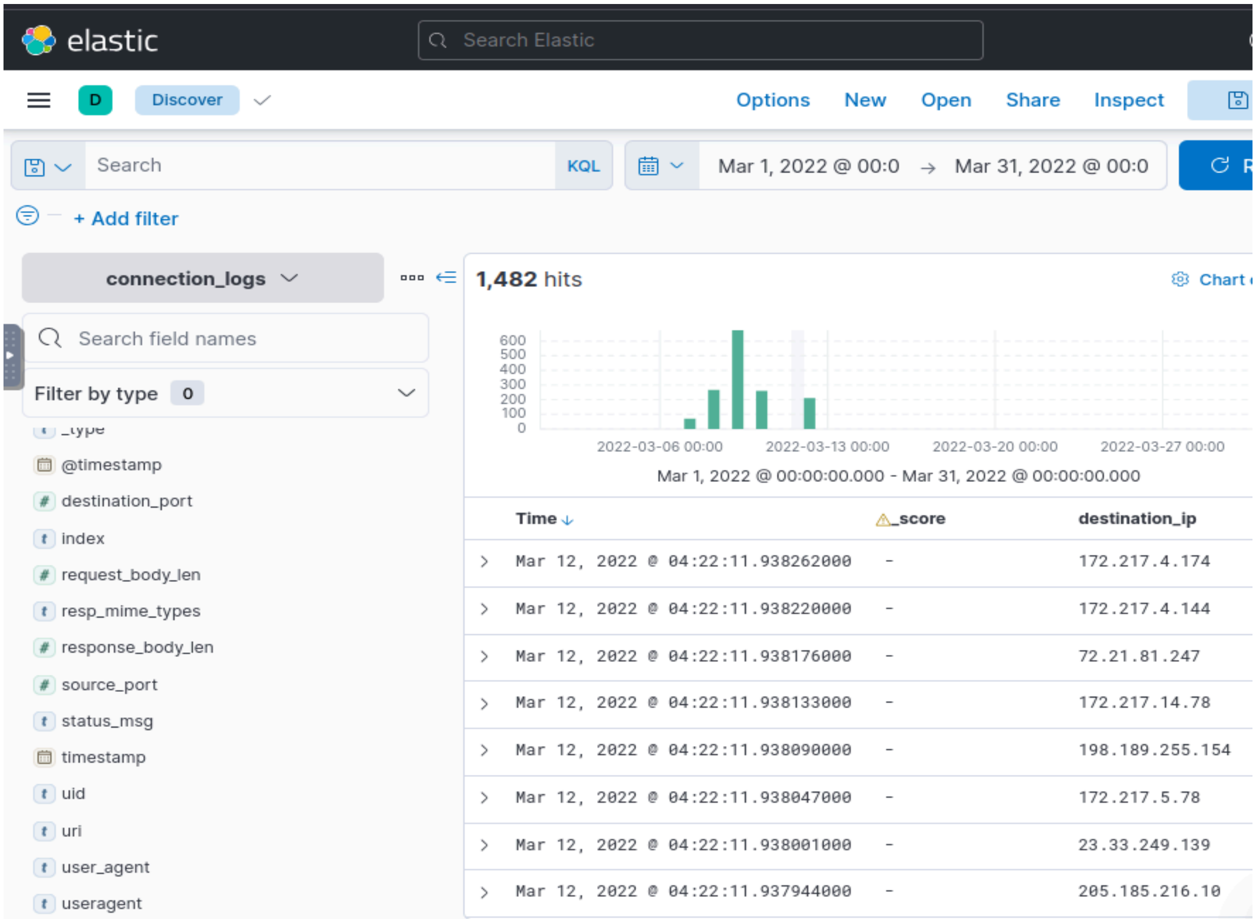
In this project, I conducted an investigation using the ELK stack (Elasticsearch, Logstash, and Kibana) to analyze network logs related to a potential Command and Control (C2) communication detected by an Intrusion Detection System (IDS). The task was part of a TryHackMe scenario in which an alert flagged suspicious activity from a user's system in the HR department.

## Objective:

To examine HTTP connection logs (connection_logs), identify suspicious activity, and uncover critical details about the C2 communication.

## Key Steps and Findings:

1. **Log Analysis:**
    - Used Kibana to filter and analyze a week-long dataset of connection logs indexed under `connection_logs`.
    - Identified 1,482 events logged in March 2022.



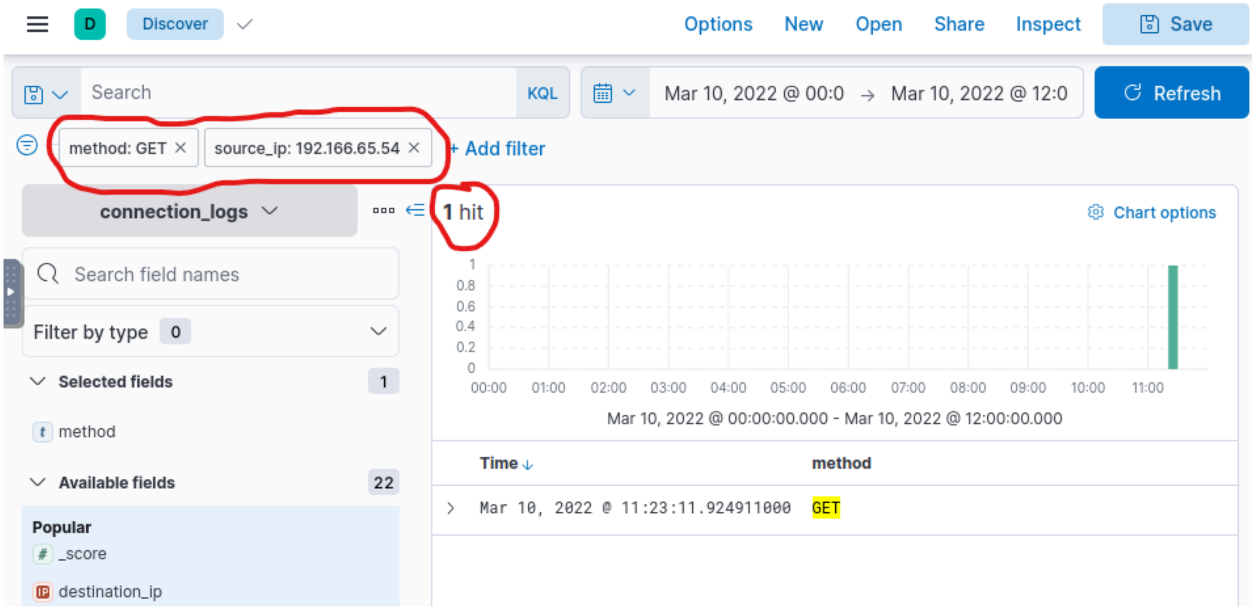
_type
@timestamp
destination_port
index
request_body_len
resp_mime_types
response_body_len
source_port
status_msg
timestamp
uid
uri
user_agent
useragent

1,482 hits

Mar 1, 2022 @ 00:00:00.000 - Mar 31, 2022 @ 00:00:00.000

| Time ↓ | ⚠_score | destination_ip |
|---|---|---|
| Mar 12, 2022 @ 04:22:11.938262000 | - | 172.217.4.174 |
| Mar 12, 2022 @ 04:22:11.938220000 | - | 172.217.4.144 |
| Mar 12, 2022 @ 04:22:11.938176000 | - | 72.21.81.247 |
| Mar 12, 2022 @ 04:22:11.938133000 | - | 172.217.14.78 |
| Mar 12, 2022 @ 04:22:11.938090000 | - | 198.189.255.154 |
| Mar 12, 2022 @ 04:22:11.938047000 | - | 172.217.5.78 |
| Mar 12, 2022 @ 04:22:11.938001000 | - | 23.33.249.139 |
| Mar 12, 2022 @ 04:22:11.937944000 | - | 205.185.216.10 |

2. **Suspected IP Identification:**
   - Found the user's source IP (`192.166.65.54`) by filtering for source_IP and method = GET. *Note: I spotted this because this other source IP had only 1 hit which stood out compared to the rest of traffic. This user was interacting with a known malicious C2 server (`104.23.99.190`), verified using AlienVault threat intelligence.



Mar 10, 2022 @ 00:0 → Mar 10, 2022 @ 12:0

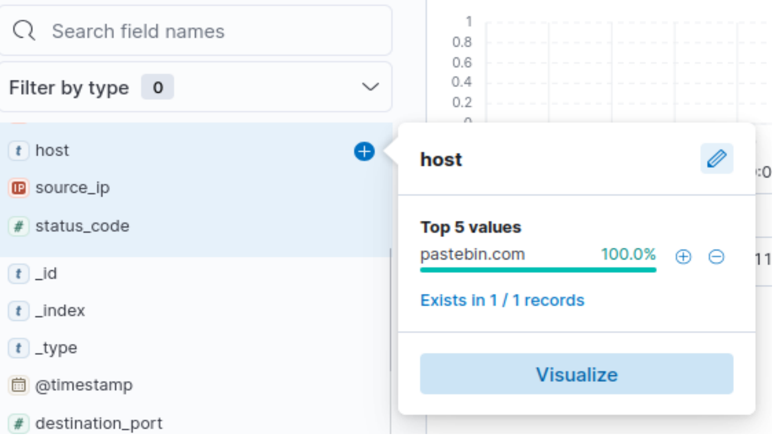
method: GET ×   source_ip: 192.166.65.54 ×

1 hit

Mar 10, 2022 @ 00:00:00.000 - Mar 10, 2022 @ 12:00:00.000

| Time ↓ | method |
|---|---|
| Mar 10, 2022 @ 11:23:11.924911000 | GET |

3. **Malicious Activity Tracking:**
   - Determined that the compromised system used a legitimate Windows binary (`bitsadmin`) to download a file from the C2 server. *Note: This user is likely using an agent to do this so I looked at the user_agent and host field to find clues for a possible domain name.
   - Discovered a connection to a well-known file-sharing site (`pastebin.com`), used as a C2 platform.



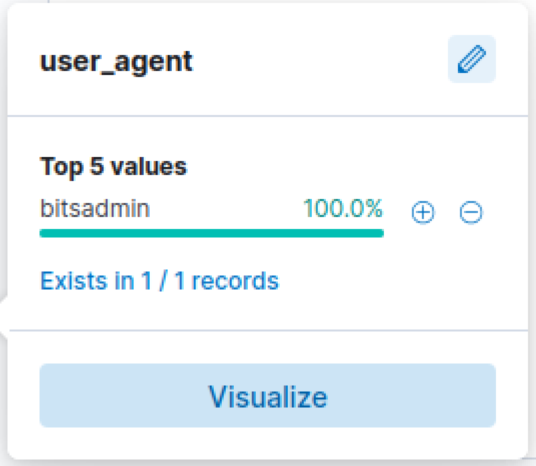
host
source_ip
status_code
_id
_index
_type
@timestamp
destination_port

**host**

**Top 5 values**

pastebin.com 100.0%

Exists in 1 / 1 records



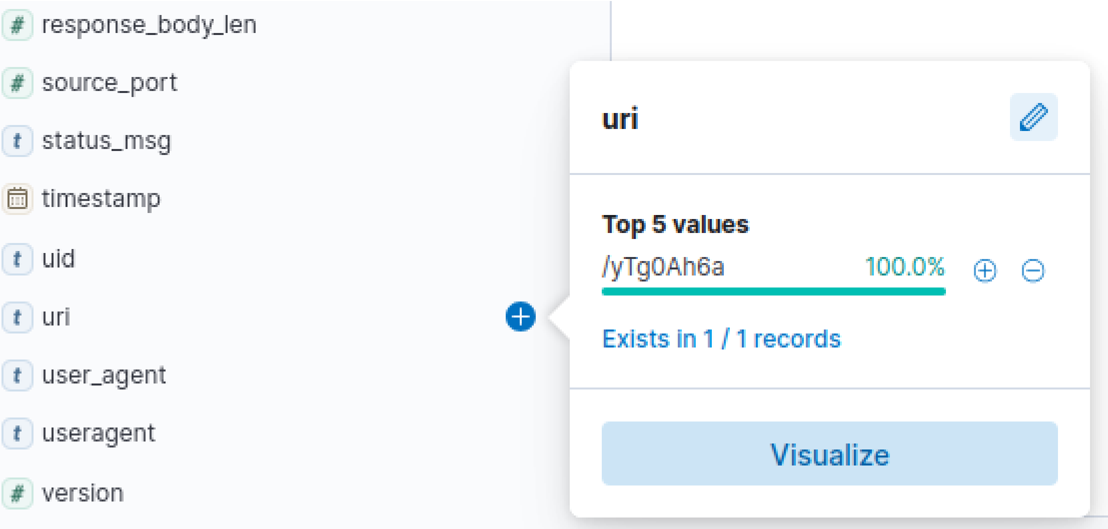
**user_agent**

**Top 5 values**

bitsadmin 100.0%

Exists in 1 / 1 records

4. **C2 URL and File Details:**
   - Extracted the full C2 URL: `pastebin.com/yTg0Ah6a`.
   - Identified a malicious file accessed (`secret.txt`) containing a secret code in the format `THM{_____}`.



response_body_len
source_port
status_msg
timestamp
uid
uri
user_agent
useragent
version

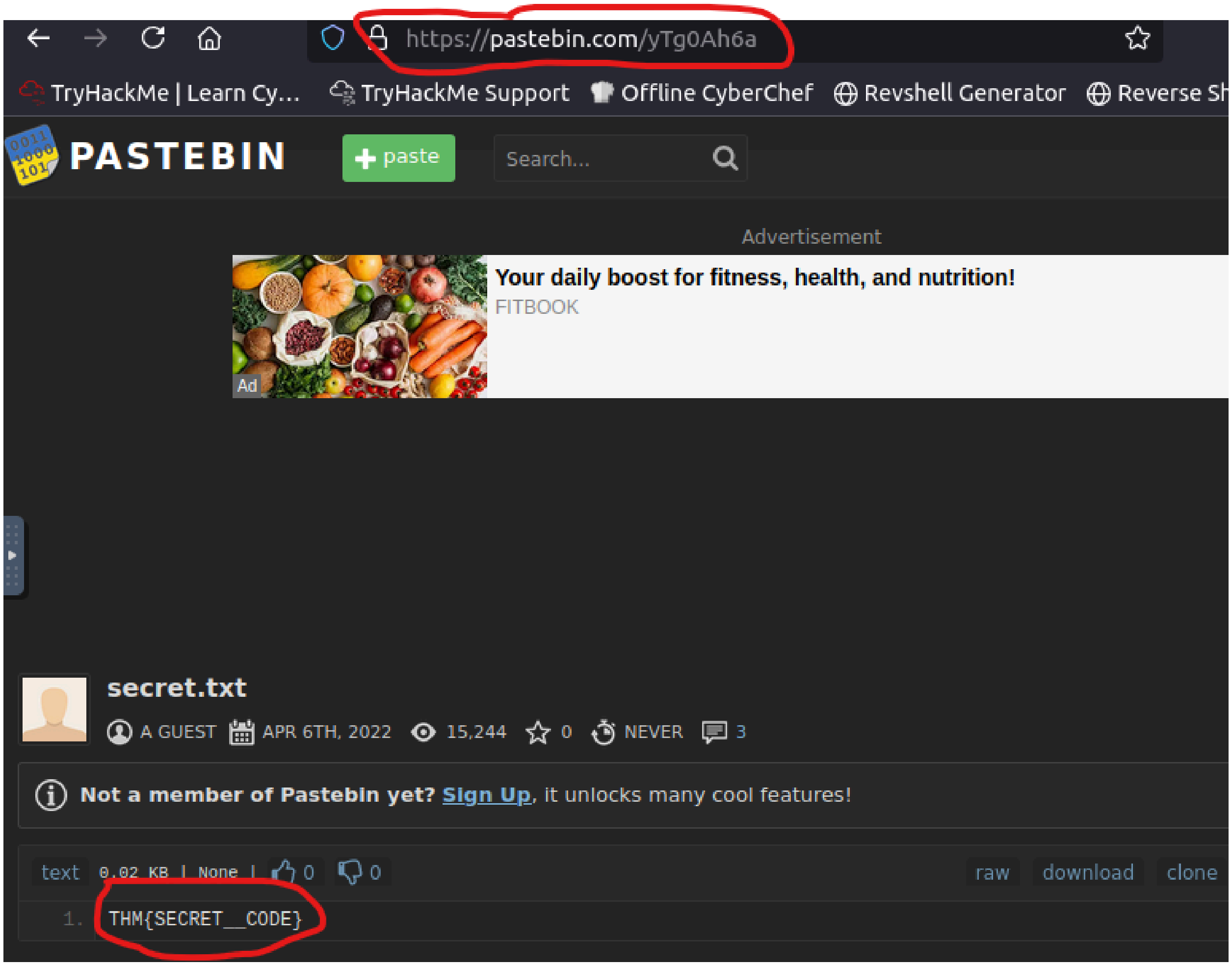
**uri**

**Top 5 values**

/yTg0Ah6a 100.0%

Exists in 1 / 1 records

5. **Final Artifact:**
    - Recovered and validated the secret code embedded in the accessed file.



secret.txt

A GUEST APR 6TH, 2022 15,244 0 NEVER 3

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.02 KB | None | 0 0

```
THM{SECRET__CODE}
```

## Outcome:

This exercise highlighted my ability to:

- Utilize SOC tools and workflows to identify and trace potential cybersecurity threats.
- Analyze network logs for suspicious patterns using ELK stack.
- Detect C2 communications and assess the attacker's methods, including legitimate binaries and popular platforms for malicious activity.

This hands-on project demonstrated critical skills in event analysis, IDS alert investigation, and real-world application of cybersecurity tools.