Lucas McMahon
9/12/24

Investigating Command and Control (C2) Communication Using the ELK Stack: A Network Log Analysis Lab

Table of Contents

Introduction

In this lab, we will investigate a potential Command and Control (C2) communication detected by the Security Operations Center (SOC) during routine monitoring. Analyst John identified an alert from the Intrusion Detection System (IDS) signaling a suspicious communication originating from a user named Browne, a member of the Human Resources department. The alert indicated that a file containing a potentially malicious pattern was accessed, raising concerns about a possible security breach. Given the limited resources available, only a week's worth of HTTP connection logs were extracted and ingested into the "connection_logs" index within Kibana for further analysis.

Objectives

The objective of this lab is to leverage the Elastic Stack (ELK Stack) to analyze the ingested network connection logs, identify any C2 communications, and pinpoint the source of the malicious activity. The investigation will focus on tracing the HTTP connections made by the user, identifying any suspicious links or files accessed, and answering critical questions to determine the scope and impact of the potential threat. Through this exercise, I will enhance my understanding of log analysis and network traffic monitoring techniques using the ELK Stack to detect and mitigate security incidents.

Lab Environment.

This lab is run using TryHackMe's ItsyBitsy Challenge, using the Elastic Stack (ELK Stack) tools to analyze network traffic. The environment includes a pre-configured Kibana instance with HTTP connection logs already ingested into the "connection_logs" index. Participants will use Kibana to query and visualize these logs, focusing on identifying potential C2 communication and malicious activity in a simulated, real-world scenario.

Lucas McMahon
9/12/24

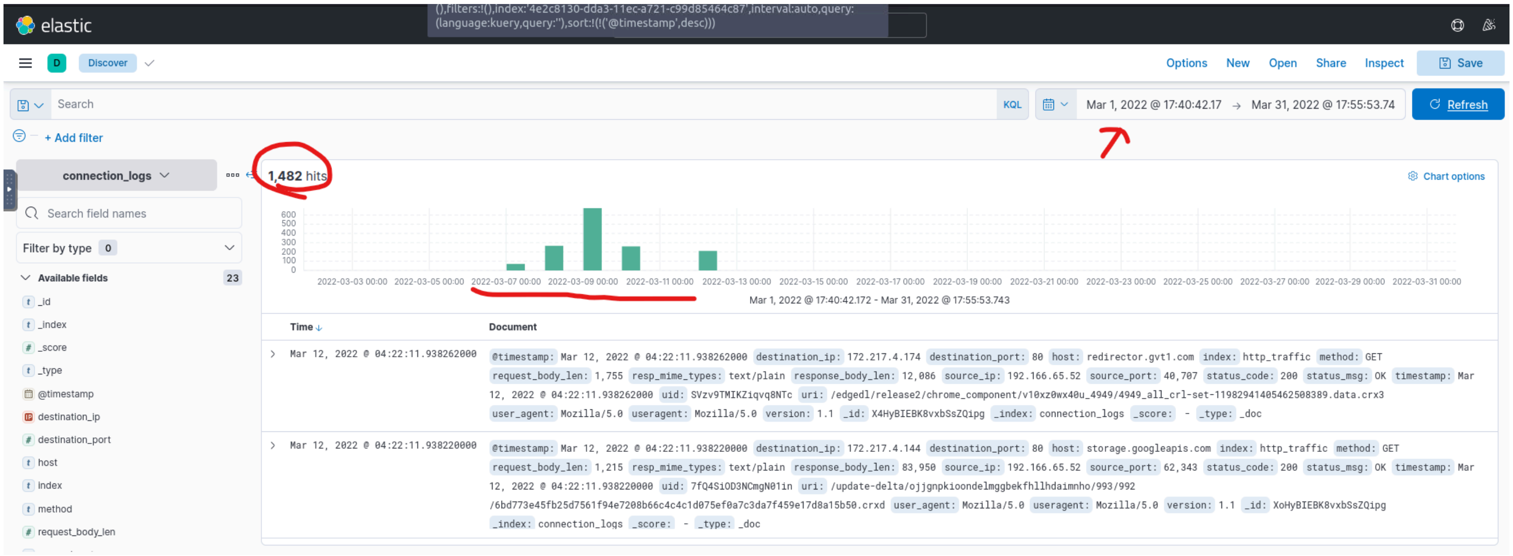
Tools and Technologies Used

- ELK Stack (Elastic Stack):
  - Elasticsearch: For storing and indexing the ingested HTTP connection logs.
  - Logstash: Used for processing and transforming the log data before ingestion.
  - Kibana: Employed for visualizing and analyzing the network traffic logs to identify patterns of suspicious activity.
- AbuseIPDB:
  - A public database for researching and validating the reputation of IP addresses involved in malicious activities.
- TryHackMe Platform (ItsyBitsy Challenge):
  - Provides a simulated environment to perform the analysis and investigation tasks.

Step-by-Step Process

Step One: Establishing the Timeline

Log in to the provided account and set the date range for March 2022. This provides a list of logs within that timeframe and displays a bar chart highlighting periods of significant activity. Notably, 1,482 logs are recorded, with a substantial concentration on March 9th - 11th.

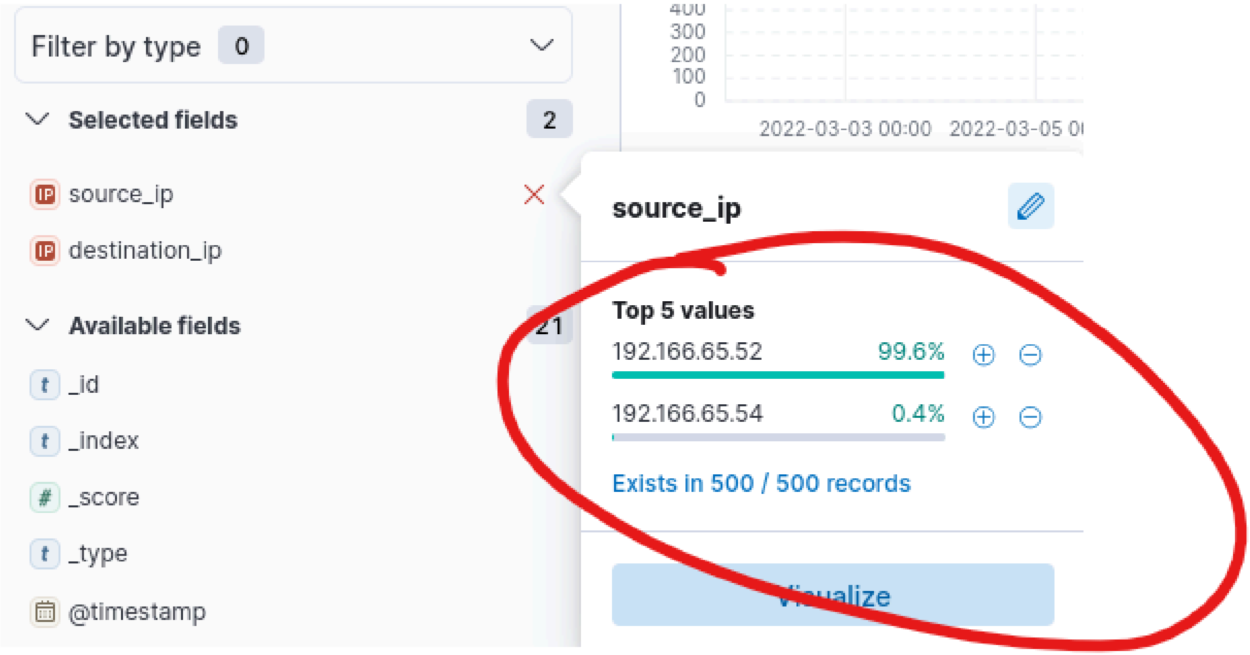


```
Time ↓                             Document
> Mar 12, 2022 @ 04:22:11.938262000  @timestamp: Mar 12, 2022 @ 04:22:11.938262000 destination_ip: 172.217.4.174 destination_port: 80 host: redirector.gvt1.com index: http_traffic method: GET
request_body_len: 1,755 resp_mime_types: text/plain response_body_len: 12,086 source_ip: 192.166.65.52 source_port: 40,707 status_code: 200 status_msg: OK timestamp: Mar
12, 2022 @ 04:22:11.938262000 uid: SVzv9TMIKZiqvq8NTc uri: /edgedl/release2/chrome_component/v10xz0wx40u_4949/4949_all_crl-set-11982941405462508389.data.crx3
user_agent: Mozilla/5.0 useragent: Mozilla/5.0 version: 1.1 _id: X4HyBIEBK8vxbSsZQipg _index: connection_logs _score: - _type: _doc

> Mar 12, 2022 @ 04:22:11.938220000  @timestamp: Mar 12, 2022 @ 04:22:11.938220000 destination_ip: 172.217.4.144 destination_port: 80 host: storage.googleapis.com index: http_traffic method: GET
request_body_len: 1,215 resp_mime_types: text/plain response_body_len: 83,950 source_ip: 192.166.65.52 source_port: 62,343 status_code: 200 status_msg: OK timestamp: Mar
12, 2022 @ 04:22:11.938220000 uid: 7fQ4SiOD3NCmgN01in uri: /update-delta/ojjgnpkioondelmggbekfhllhdaimnho/993/992
/6bd773e45fb25d7561f94e7208b66c4c4c1d075ef0a7c3da7f459e17d8a15b50.crxd user_agent: Mozilla/5.0 useragent: Mozilla/5.0 version: 1.1 _id: XoHyBIEBK8vxbSsZQipg
_index: connection_logs _score: - _type: _doc
```

Step Two: Identifying the Suspect's IP Address

Next we are asked to find the IP address associated with the suspect user. To identify the IP address associated with the suspect user, ELK Stack allows us to analyze log activity percentages for all known IP addresses.



Filter by type 0

Selected fields 2

- source_ip
- destination_ip

Available fields 21

- _id
- _index
- _score
- _type
- @timestamp

source_ip

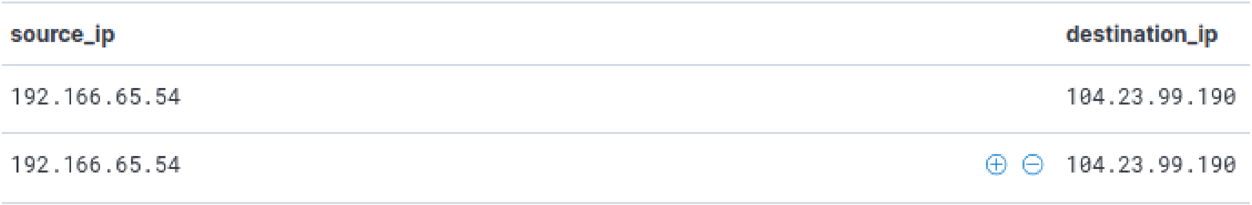
Top 5 values

192.166.65.52	99.6%
192.166.65.54	0.4%

Exists in 500 / 500 records

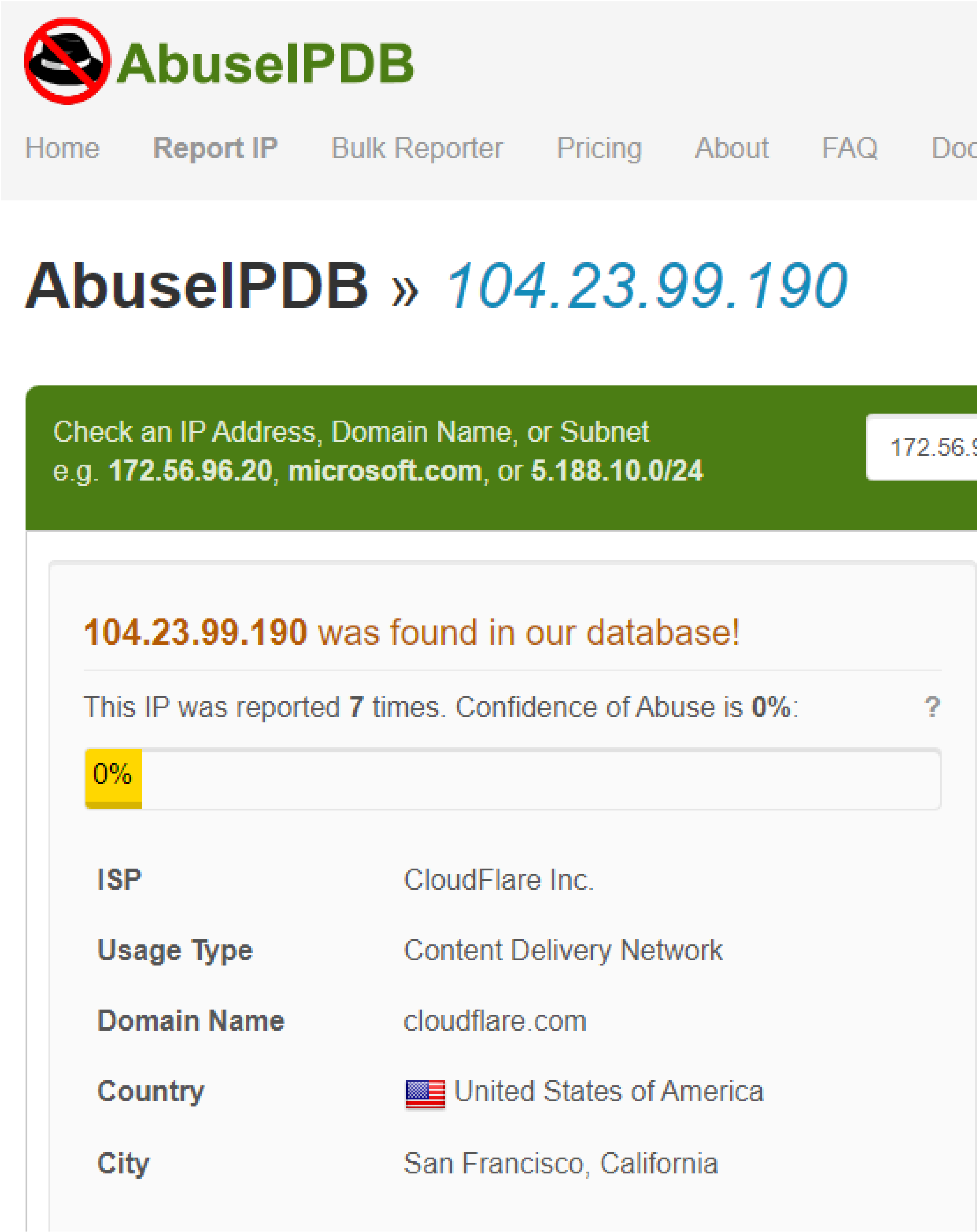
We find that two source IP addresses account for all activity: one with a significant majority and another with only two log entries, both directed to the same destination IP.

Initially, it seems logical to investigate the IP with the most activity, assuming it could indicate infection. However, after researching these IP addresses, I found no useful public information. Realizing that typical Windows machines often show high activity levels, I shifted focus to the second IP address.



source_ip	destination_ip
192.166.65.54	104.23.99.190
192.166.65.54	104.23.99.190

This source IP is private, so online research was unhelpful. However, a quick check of the destination IP on AbuseIPDB confirmed that the associated activity warranted further investigation.



AbuseIPDB » *104.23.99.190*

Check an IP Address, Domain Name, or Subnet
e.g. **172.56.96.20**, **microsoft.com**, or **5.188.10.0/24**

104.23.99.190 was found in our database!

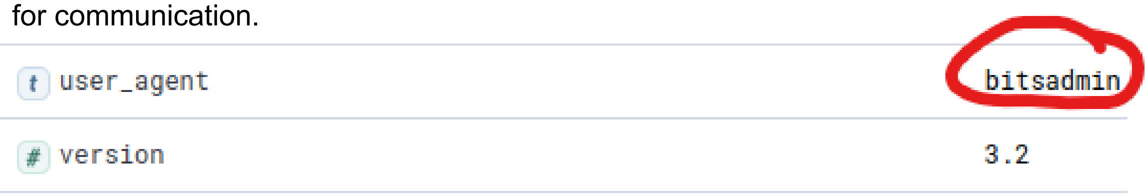
This IP was reported **7** times. Confidence of Abuse is **0%**: ?

0%

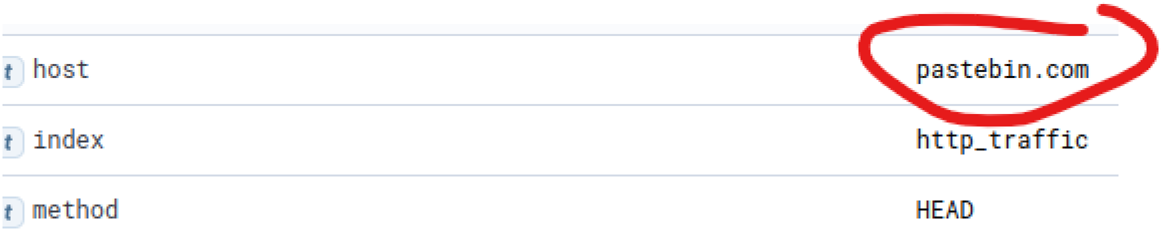
ISP	CloudFlare Inc.
Usage Type	Content Delivery Network
Domain Name	cloudflare.com
Country	🇺🇸 United States of America
City	San Francisco, California

Step Three: Analyzing the Malicious Activity

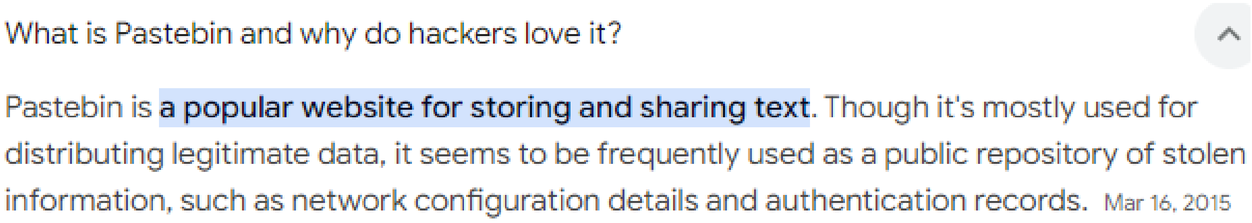
The next step is to determine which legitimate Windows binary was used to download a file from the C2 server. The logs reveal that the binary in question is `bitsadmin`, and the C2 server involved is `pastebin[.]com`, a common file-sharing site also used by malware authors for communication.



t	user_agent	bitsadmin
#	version	3.2



host	pastebin.com
index	http_traffic
method	HEAD

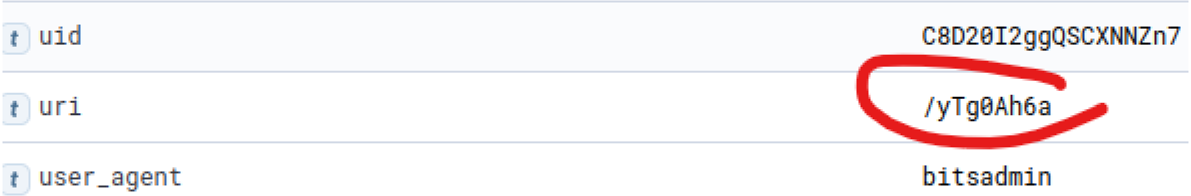


What is Pastebin and why do hackers love it?

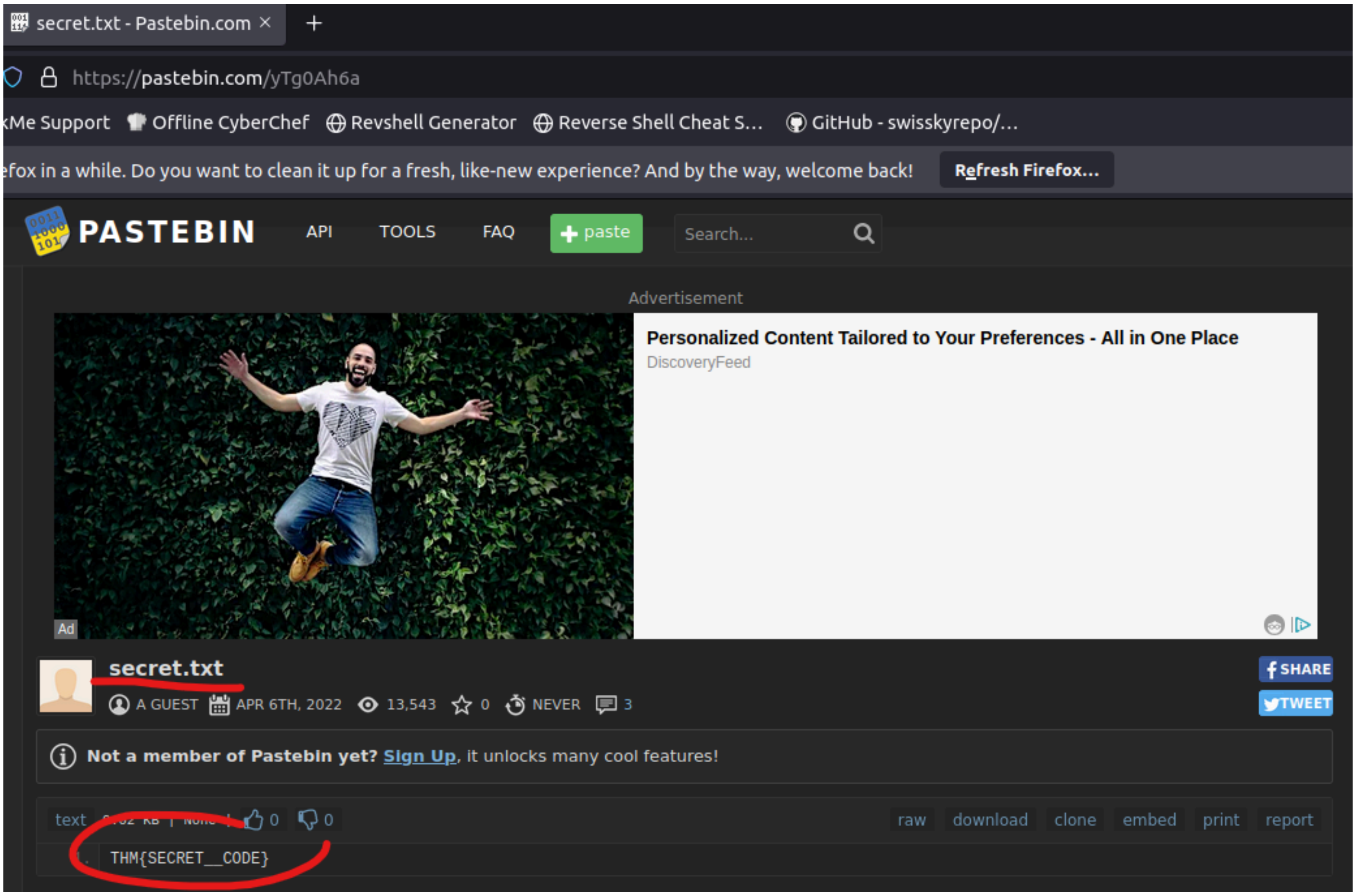
Pastebin is a popular website for storing and sharing text. Though it's mostly used for distributing legitimate data, it seems to be frequently used as a public repository of stolen information, such as network configuration details and authentication records. Mar 16, 2015

Step Four: Identifying the Accessed File

The final step is to identify the file accessed during this breach and locate the flag it contains. The log details provide the host (`pastebin.com`) and the URI (`/yTg0Ah6a`), forming the complete URL: `http://pastebin[.]com/yTg0Ah6a`. Visiting this link reveals the content accessed by the attacker.



uid	C8D20I2ggQSCXNNZn7
uri	/yTg0Ah6a
user_agent	bitsadmin



secret.txt - Pastebin.com
https://pastebin.com/yTg0Ah6a
xMe Support · Offline CyberChef · Revshell Generator · Reverse Shell Cheat S… · GitHub - swisskyrepo/…
efox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox…
PASTEBIN
API
TOOLS
FAQ
paste
Search...

secret.txt

A GUEST · APR 6TH, 2022 · 13,543 · 0 · NEVER · 3

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

text 0.02 KB | None | 0 0
raw download clone embed print report

```
THM{SECRET__CODE}
```

Results and Analysis

The investigation revealed that the suspect user, Browne, was likely involved in Command and Control (C2) communication. Analysis of the network logs indicated two source IP addresses, one of which exhibited minimal activity, drawing initial suspicion. Further investigation using AbuseIPDB confirmed that the destination IP associated with the second source IP was flagged for malicious activity.

A deeper examination of the logs revealed that the Windows binary `bitsadmin` was used to download a file from the C2 server, identified as `pastebin[.]com`. The URL path on Pastebin was retrieved, confirming the presence of a malicious file and the associated flag required for this challenge.

Challenges Faced

Limited Data Availability:

- Only HTTP connection logs were available, restricting the scope of the investigation and requiring a more focused analysis of network traffic.

Initial Misinterpretation of Log Data:

- The initial focus on the IP address with the most activity delayed the identification of the actual C2 communication. This required a shift in strategy to consider less obvious patterns.

Reliance on External Information:

- The need to consult external databases (such as AbuseIPDB) for IP reputation added an additional layer of complexity to the investigation process.

Conclusion

The investigation successfully identified a Command and Control (C2) communication using the ELK Stack to analyze HTTP connection logs. The suspect, Browne, was found to be using `bitsadmin` to communicate with a malicious server hosted on Pastebin, confirming the presence of a security breach. The lab exercise highlighted the importance of analyzing both common and uncommon network activity patterns to detect potential threats. It also demonstrated the effective use of log analysis tools to uncover evidence of malicious behavior, even with limited data.

References

Elastic Stack Documentation:
Elasticsearch, Logstash, Kibana

AbuseIPDB:
AbuseIPDB - IP Address Lookup

TryHackMe - ItsyBitsy Challenge:
TryHackMe