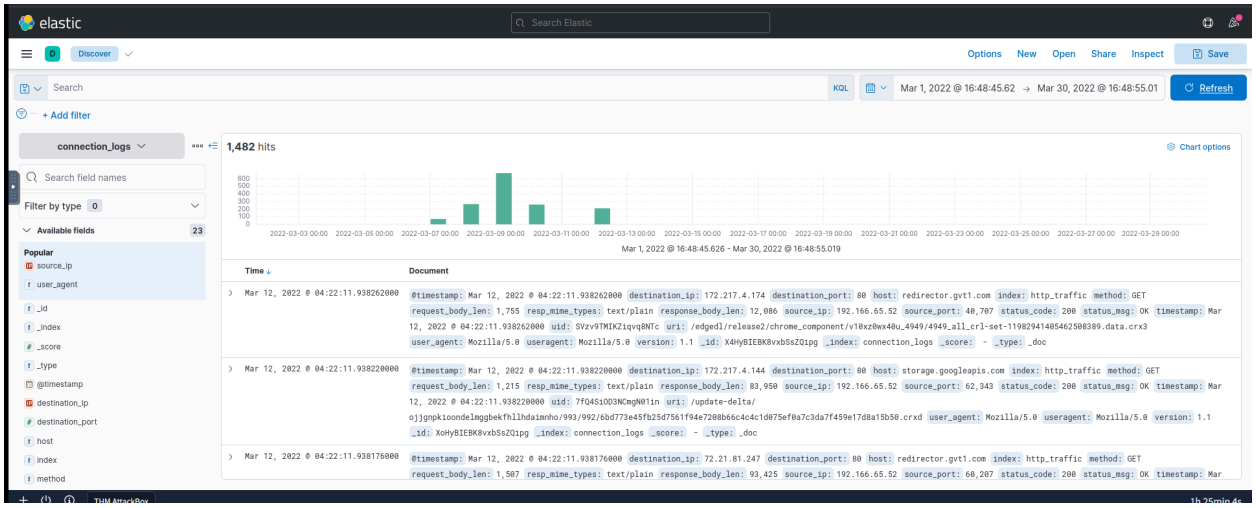
Intro

During normal SOC monitoring, an IDS alert flagged potential command-and-control (C2) communication associated with a user named **Browne** from the HR department. The alert referenced a suspicious file containing the pattern **THM:{_____}**.

A week's worth of HTTP connection logs was exported and ingested into the **connection_logs** index in Kibana. No host logs were available, so the investigation relied entirely on network telemetry.

Q1- How many events were returned for the month of March 2022?

- I performed a quick date filter on the connection logs for March 2022.
  The total number of events returned was: **1482 events**



Q2- What is the IP associated with the suspected user in the logs?

- Since we are looking for IPs I went to the source IP field to just to take a peek and seen that there were only two connections
- Since the first IP had the most traffic I looked at the second connection first to just browse at the network traffic

- After checking the field you can see that it stood out because it was making outbound HTTP requests to a Pastebin URL, which is unusual in enterprise environments.
- This matched the alert description about a suspicious file with the THM format.

Q3- The user's machine used a legit windows binary to download a file from the C2 server. What is the name of the binary?

- The **user-agent** field in the suspicious HTTP request showed that the download was made using: **bitsadmin**
- Rather than a web browser. Bitsadmin is a legitimate but deprecated Windows tool frequently abused by malware to

perform silent or background file downloads, making this behavior especially suspicious.

Q4- The infected machine connected with a famous filesharing site in this period, which also acts as a C2 server used by the malware authors to communicate. What is the name of the filesharing site?

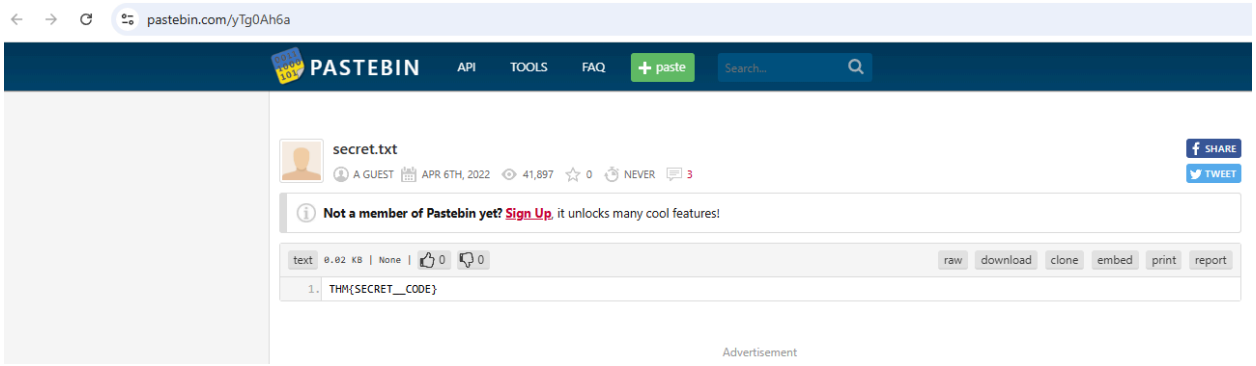
Q5- What is the full URL of the C2 to which the infected host is connected?

- Using the image above we can see that a connection was made to “pastebin[.]com”
- After putting this website into VirusTotal to learn more about it we discover that “pastebin[.]com” is safe to navigate itself but is often used alot by malware. This confirmed our alert from the IDS we got earlier.
- After confirming the website was safe to click we navigated to the link using the domain and the uri we were provided “ pastebin[.]com/yTg0Ah6a”

Q6-A file was accessed on the filesharing site. What is the name of the file accessed?

Q7- The file contains a secret code with the format THM{_____}.

- We get these last two answers from the website here.



By pivoting through the logs — IP → domain → tool → URL → file — I confirmed:

- The internal IP associated with the suspected user
- The use of bitsadmin for the download
- The C2 server domain (pastebin.com)
- The full URL the infected host contacted
- The file retrieved (secret.txt)
- The malicious THM formatted content inside the file

This established a full picture of the suspicious activity.

What I Learned

- Network logs often do not include usernames, so IP-based correlation is essential.
- Services like Pastebin are commonly abused for C2 communication and file hosting.
- Bitsadmin usage for downloads is a strong indicator of malicious activity.
- VirusTotal is a safe preliminary check before interacting with suspicious domains.
- Log pivoting (pattern → event → IP → behavior) is a core skill for SOC analysts.
- Even with limited data sources, you can still reconstruct a full attack path.