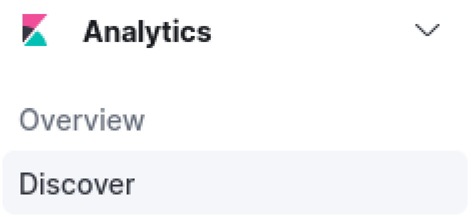
TryHackMe: ItsyBitsy

Recently, I completed a TryHackMe room called ItsyBitsy. It is an intermediate level room that involves investigating HTTP logs and answering a set of questions. I really enjoyed the room and I hope you enjoy this room as much as I did.

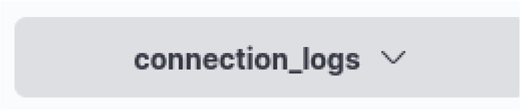
Scenario: During normal SOC monitoring, Analyst John observed an alert on an IDS solution indicating a potential C2 communication from a user Browne from the HR department. A suspicious file was accessed containing a malicious pattern THM:{________}. A week-long HTTP connect log have been pulled to investigate. Due to limited resources, only the connection logs could be pulled out and are ingested into the connection_logs index in Kibana. Our task in this room will be to examine the network connection logs of this user, find the link and the content of the file, and answer the questions.

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

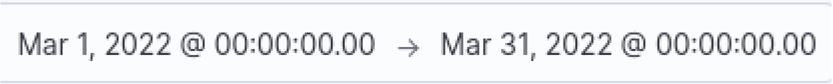
Once you have accessed the machine IP in the browser, you will be presented with the Elastic landing page. Make sure to navigate to the Discover section like as follows:



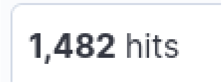
Here we will be able to investigate the logs/documents, also make sure that you are using the connection_logs index:


connection_logs

To determine how many events were returned for the month of March 2022, we can use the time filter:


Mar 1, 2022 @ 00:00:00.00 → Mar 31, 2022 @ 00:00:00.00

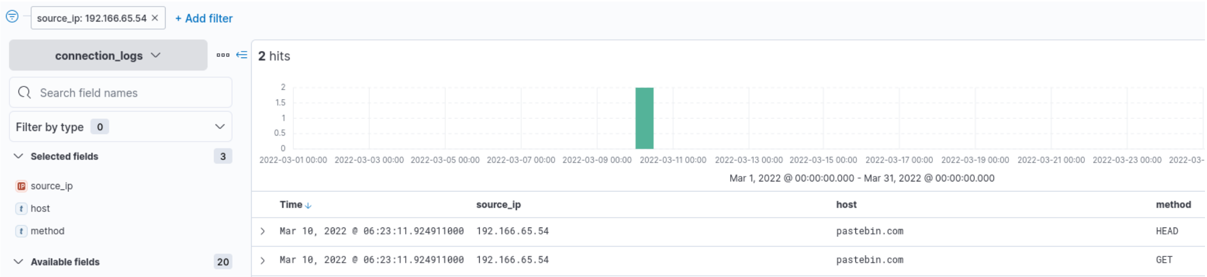
Once you have configured this properly, you can see the amount of hits just above the timeline:


1,482 hits

These hits refer to the number of events, which is the answer.

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

If you look at the available fields, there is unfortunately no field for usernames which is understandable as this is a HTTP log. Therefore, I checked out the source_field and noticed that the log file only contains 2 unique source IP addresses, after exploring the second IP address with the least amount of traffic, I noticed that it made a get request to Pastebin which is extremely suspicious:

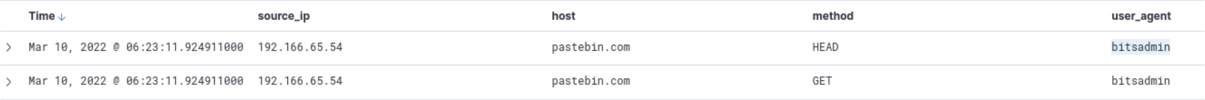


Time ↓	source_ip	host	method
Mar 10, 2022 @ 06:23:11.924911000	192.166.65.54	pastebin.com	HEAD
Mar 10, 2022 @ 06:23:11.924911000	192.166.65.54	pastebin.com	GET

The other IP address seems to have somewhat normal HTTP traffic, and for these reasons, I determined that the IP address ‘192.166.65.54’ is the answer.

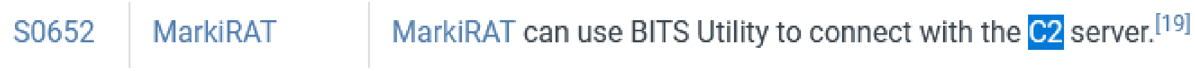
The user’s machine used a legit Windows binary to download a file from the C2 server. What is the name of the binary?

If you add the user_agent field to the logs column and filter for the IP address we identified previously, you will notice the user agent ‘bitsadmin’:



Time ↓	source_ip	host	method	user_agent
Mar 10, 2022 @ 06:23:11.924911000	192.166.65.54	pastebin.com	HEAD	bitsadmin
Mar 10, 2022 @ 06:23:11.924911000	192.166.65.54	pastebin.com	GET	bitsadmin

This is anomalous traffic as if it was normal HTTP traffic, the user agent would be from something like Firefox or Google Chrome. On further investigation you can determine that BITSAdmin is a CLI tool used to create and manage BITS Jobs. As stated by MITRE, Adversaries can abuse BITS jobs to persistently execute code. There have also been instances where threat actors have used BITSAdmin to connect with a C2 server:



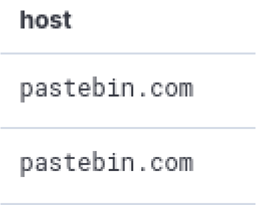
S0652	MarkiRAT	MarkiRAT can use BITS Utility to connect with the C2 server.[19]

https://attack.mitre.org/techniques/T1197/

https://attack.mitre.org/software/S0190/

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 this filesharing site?

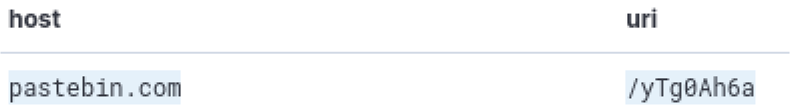
As we have discovered early on, Pastebin was connected to by the infected user.



host
pastebin.com
pastebin.com

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

If we add the URI field to our search, we can find the full URL of the C2 server:

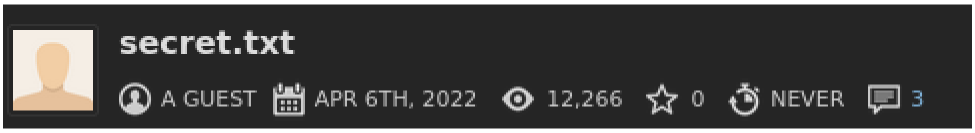


host	uri
pastebin.com	/yTg0Ah6a

It is just the host combined with the URI.

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

If we navigate to the full URI found previously, we can see the name of the file accessed which is secret.txt:

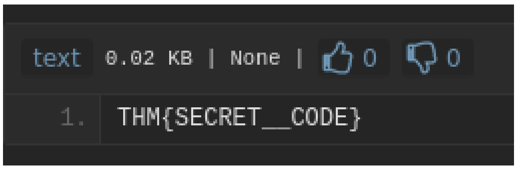


secret.txt

A GUEST APR 6TH, 2022 12,266 0 NEVER 3

The file contains a secret code with the format THM{______}.

The final flag can be seen on the same page as visited in the previous question:



text 0.02 KB | None | 0 0

```
THM{SECRET__CODE}
```

Completing the TryHackMe ItsyBitsy room provided valuable hands-on experience in SOC monitoring, log analysis, and identifying IOCs. By leveraging the ELK stack and understanding common attack vectors, I was able to identify malicious/suspicious behaviour and complete this room.