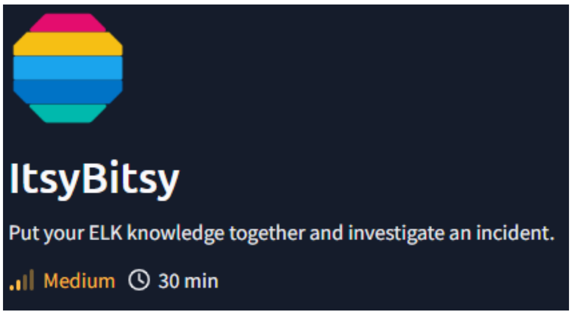


ItsyBitsy

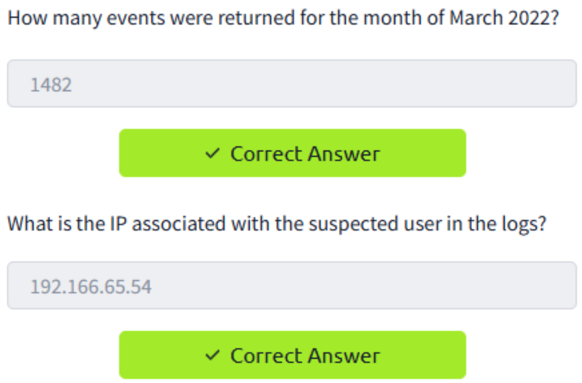
Put your ELK knowledge together and investigate an incident.

Medium 30 min

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 connection logs 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.

For the first two questions I used filters:



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

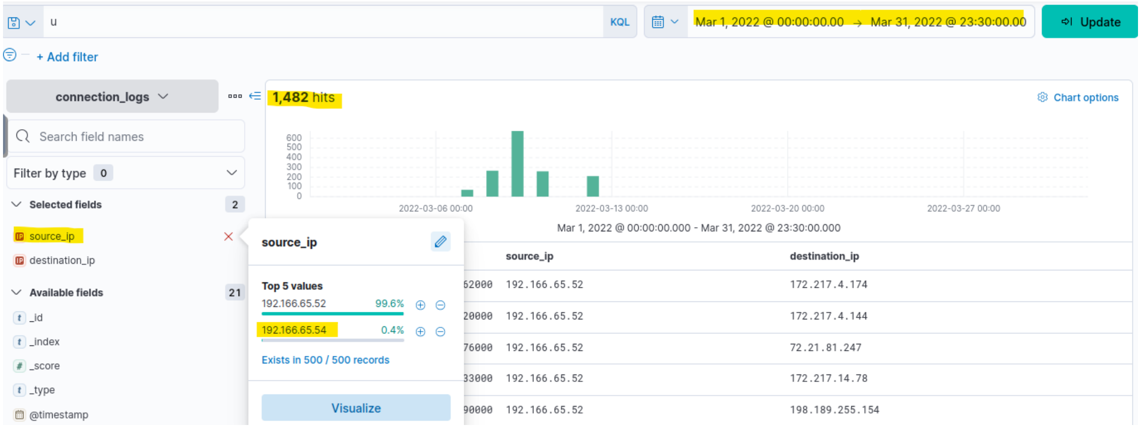
1482

✓ Correct Answer

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

192.166.65.54

✓ Correct Answer



u

KQL

Mar 1, 2022 @ 00:00:00.00 → Mar 31, 2022 @ 23:30:00.00

Update

+ Add filter

connection_logs

1,482 hits

Search field names

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%

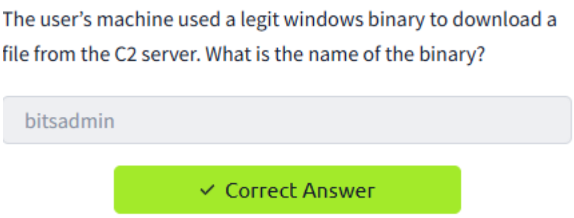
Exists in 500 / 500 records

Visualize

Mar 1, 2022 @ 00:00:00.000 - Mar 31, 2022 @ 23:30:00.000

```
        source_ip          destination_ip
62000   192.166.65.52      172.217.4.174
20000   192.166.65.52      172.217.4.144
76000   192.166.65.52      72.21.81.247
33000   192.166.65.52      172.217.14.78
90000   192.166.65.52      198.189.255.154
```

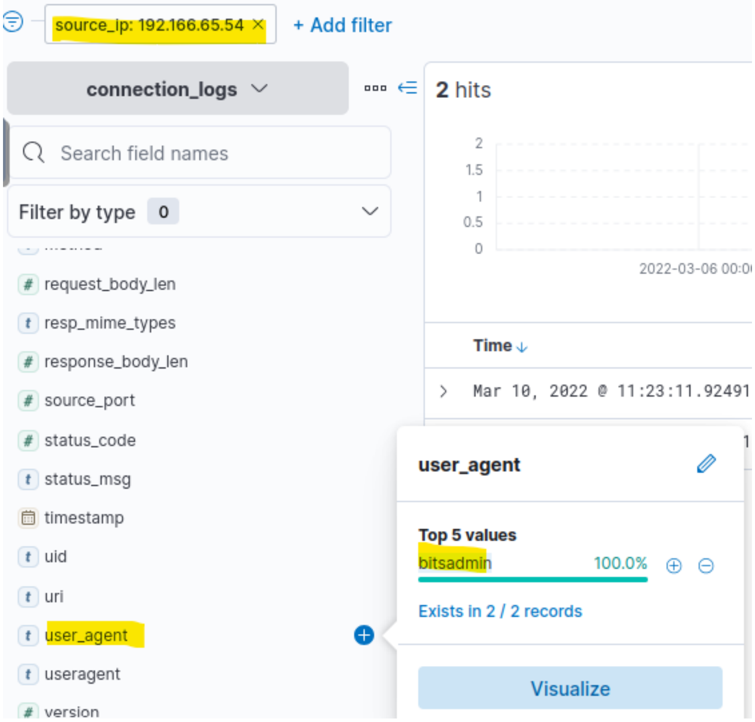
Again we used a filter for the source ip that we where looking before.



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

bitsadmin

✓ Correct Answer



source_ip: 192.166.65.54 ✕

+ Add filter

connection_logs

Search field names

Filter by type 0

request_body_len

resp_mime_types

response_body_len

source_port

status_code

status_msg

timestamp

uid

uri

user_agent

useragent

version

2 hits

Time ↓

Mar 10, 2022 @ 11:23:11.92491

user_agent

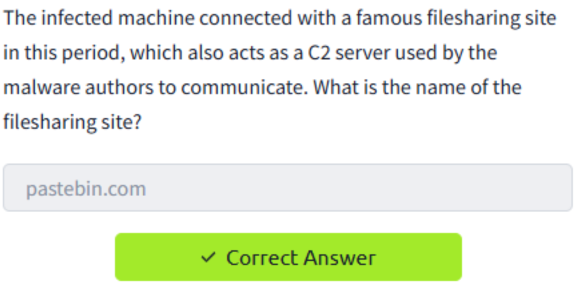
Top 5 values

bitsadmin 100.0%

Exists in 2 / 2 records

Visualize

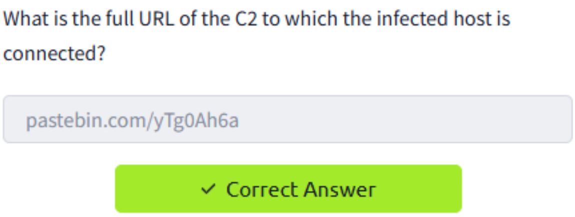
After I search for the ip also I could search for the next two questions:



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?

pastebin.com

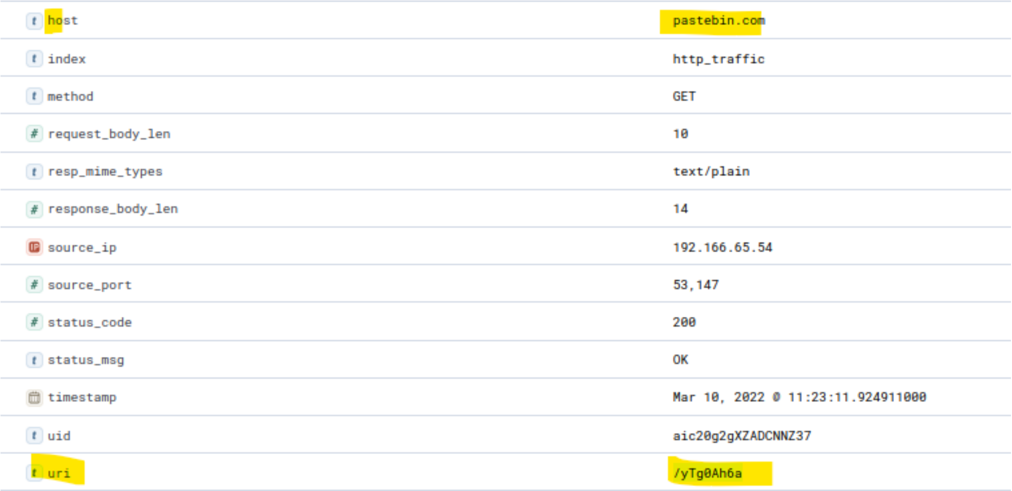
✓ Correct Answer



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

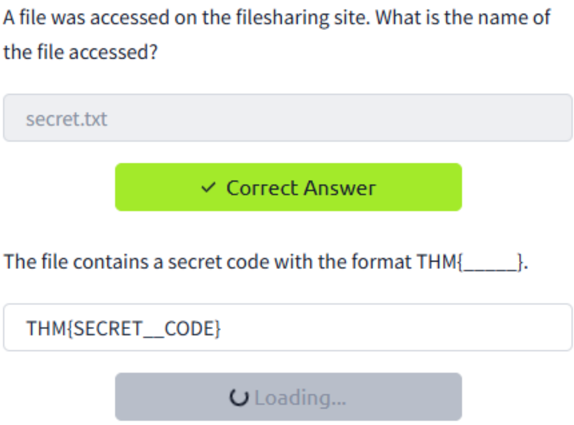
pastebin.com/yTg0Ah6a

✓ Correct Answer



host	pastebin.com
index	http_traffic
method	GET
request_body_len	10
resp_mime_types	text/plain
response_body_len	14
source_ip	192.166.65.54
source_port	53,147
status_code	200
status_msg	OK
timestamp	Mar 10, 2022 @ 11:23:11.924911000
uid	aic20g2gXZADCNNZ37
uri	/yTg0Ah6a

When I went to the website I could find the next two questions:

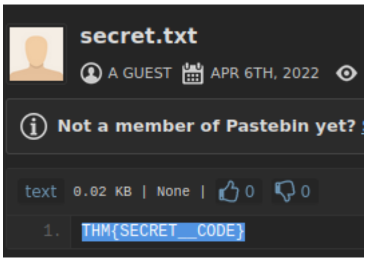


A file was accessed on the filesharing site. What is the name of the file accessed?

secret.txt

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

THM{SECRET__CODE}



secret.txt

A GUEST APR 6TH, 2022

Not a member of Pastebin yet?

```
THM{SECRET__CODE}
```