ItsyBitsy

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 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.

Answer the questions below

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

Adjust the date to the march 2022

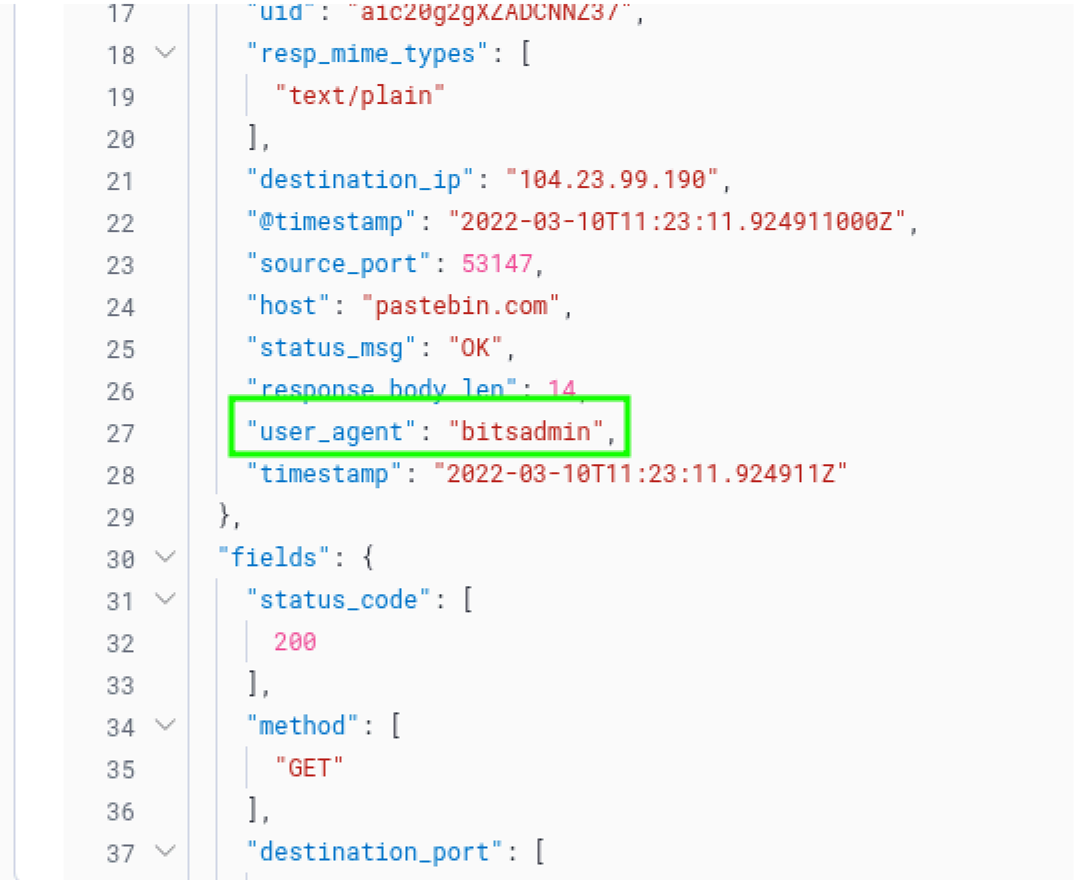
1482

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

192.166.65.54

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

Filter the logs with the ip of the attacker , and look for the useragent

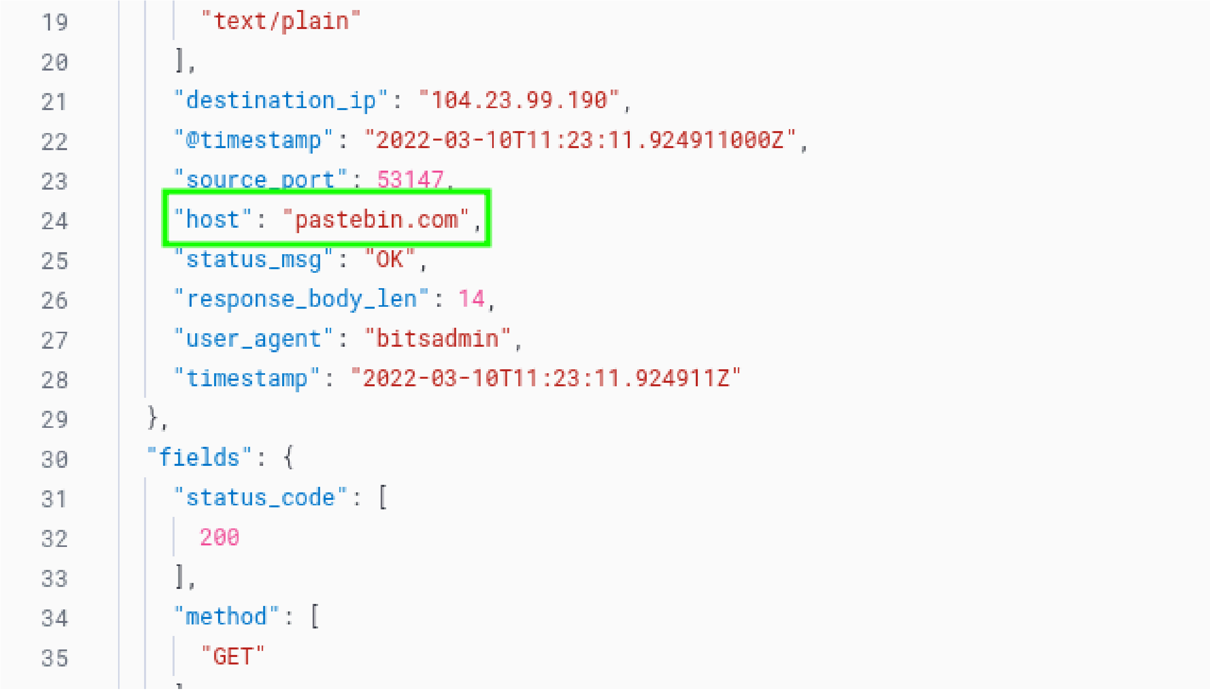


```
    "uid": "a1c20g2gXZADCNNZ37",
    "resp_mime_types": [
      "text/plain"
    ],
    "destination_ip": "104.23.99.190",
    "@timestamp": "2022-03-10T11:23:11.924911000Z",
    "source_port": 53147,
    "host": "pastebin.com",
    "status_msg": "OK",
    "response_body_len": 14,
    "user_agent": "bitsadmin",
    "timestamp": "2022-03-10T11:23:11.924911Z"
  },
  "fields": {
    "status_code": [
      200
    ],
    "method": [
      "GET"
    ],
    "destination_port": [
```

btsadmin

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?

Look for the hostname in the same log



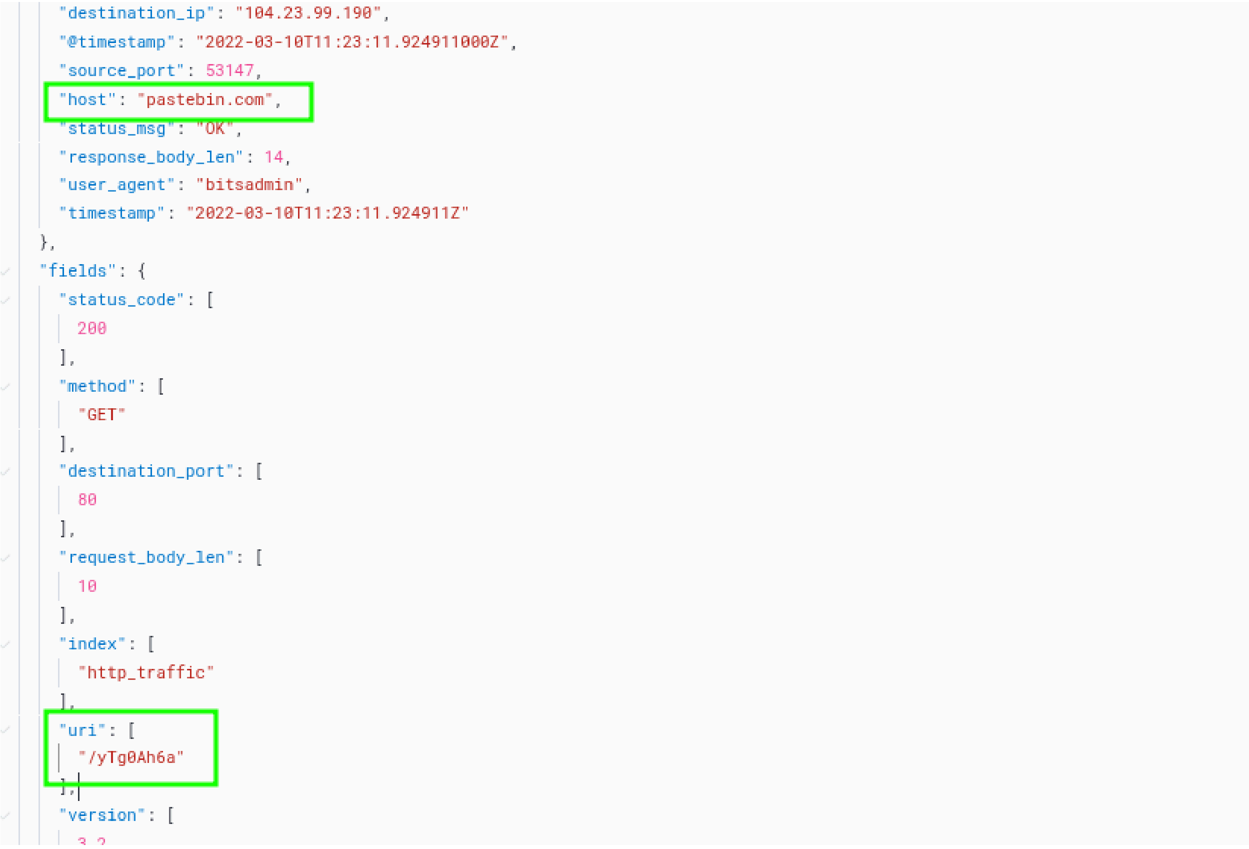
```
      "text/plain"
    ],
    "destination_ip": "104.23.99.190",
    "@timestamp": "2022-03-10T11:23:11.924911000Z",
    "source_port": 53147,
    "host": "pastebin.com",
    "status_msg": "OK",
    "response_body_len": 14,
    "user_agent": "bitsadmin",
    "timestamp": "2022-03-10T11:23:11.924911Z"
  },
  "fields": {
    "status_code": [
      200
    ],
    "method": [
      "GET"
```

pastebin.com

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

URL which is the combination of the domain / ip and the path of the page

Find the URL path in the same log



```
    "destination_ip": "104.23.99.190",
    "@timestamp": "2022-03-10T11:23:11.924911000Z",
    "source_port": 53147,
    "host": "pastebin.com",
    "status_msg": "OK",
    "response_body_len": 14,
    "user_agent": "bitsadmin",
    "timestamp": "2022-03-10T11:23:11.924911Z"
  },
  "fields": {
    "status_code": [
      200
    ],
    "method": [
      "GET"
    ],
    "destination_port": [
      80
    ],
    "request_body_len": [
      10
    ],
    "index": [
      "http_traffic"
    ],
    "uri": [
      "/yTg0Ah6a"
    ],
    "version": [
      3.2
```

pastebin.com/yTg0Ah6a

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

Navigate to the site *pastebin.com/yTg0Ah6a* and get the both file and the flag

secret.txt

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

THM{SECRET__CODE}