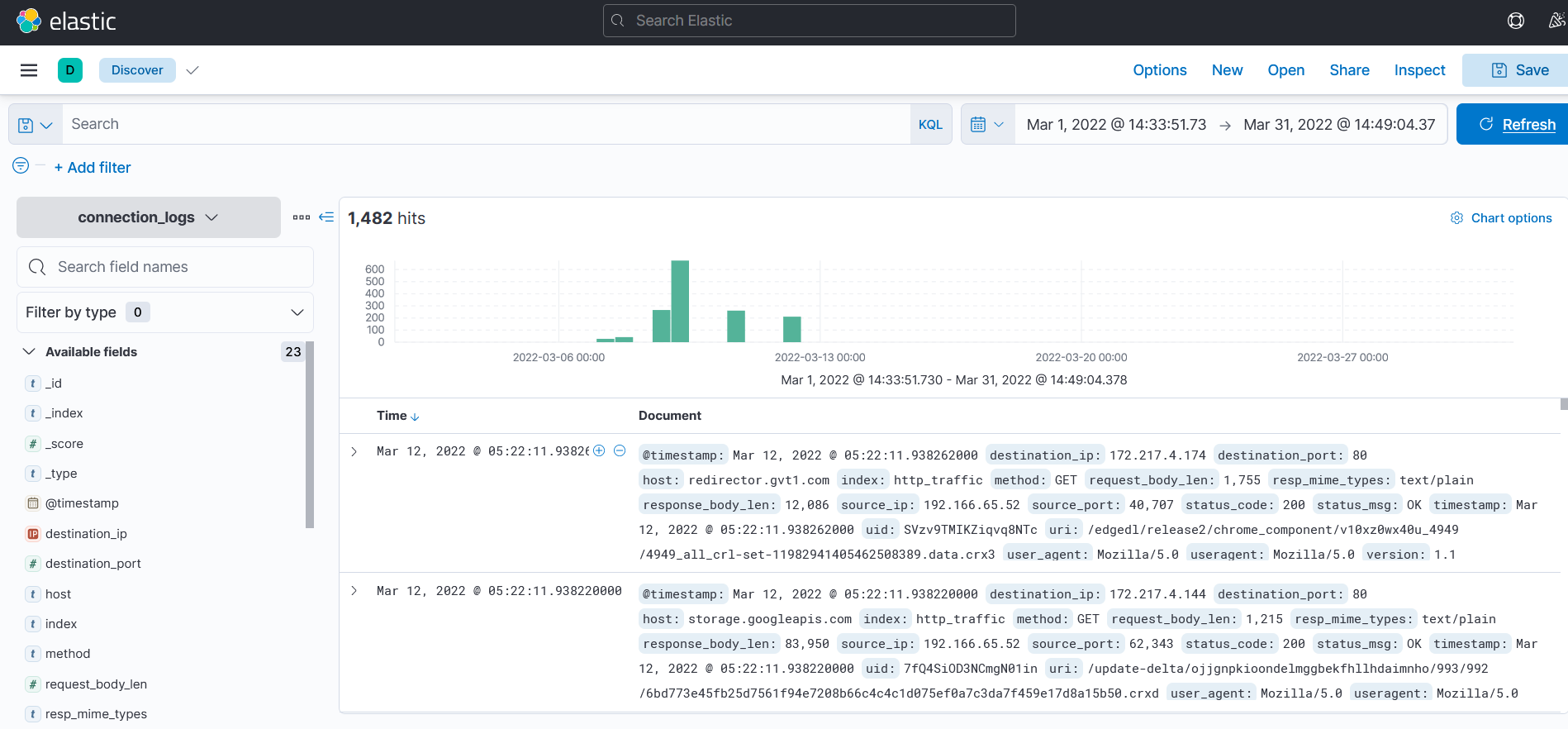
ItsyBitsy 15 minuten

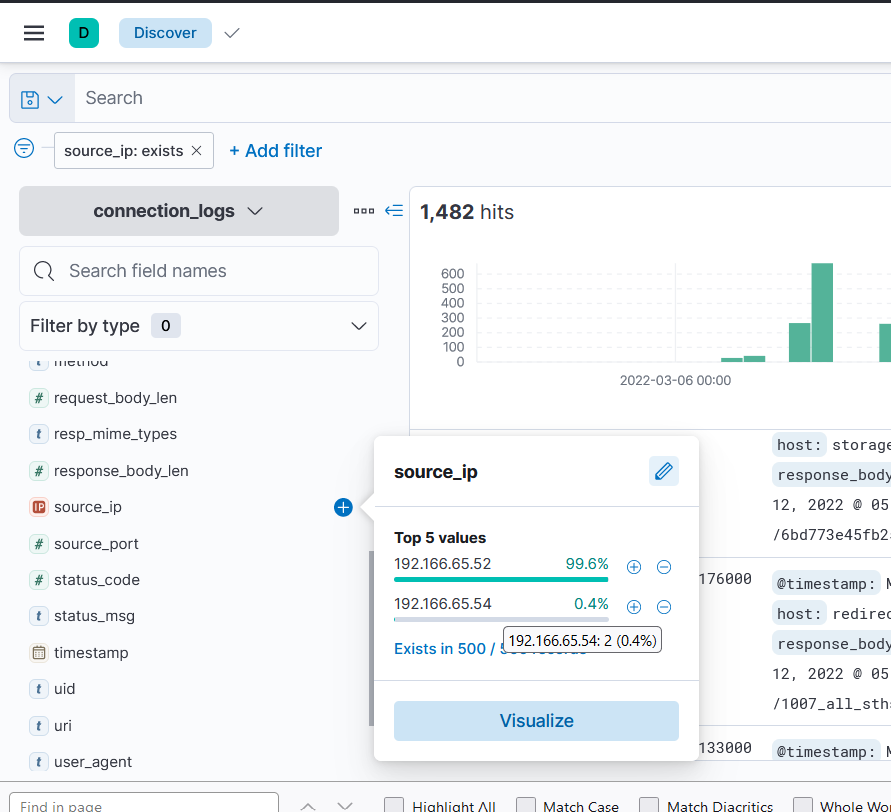
1. *How many events were returned for the month of March 2022?*

Discover 🡪 Datum instellen van 1 Maart 2022 tot 31 Maart 2022  
Oplossing: 1482

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

Filter by type 🡪 Source IP 🡪 0.4% van traffic

Oplossingen 192.166.65.54



1. 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  
  
Gekeken naar de user-agent van de logs, gefilterd op ip-adres. Bitsadmin is customer header commando waarmee je custom headers kan toevoegen aan http request



1. 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?  
     
   Te zien in de logs als host: Pastebin.com
2. What is the full URL of the C2 to which the infected host is connected?

pastebin.com/yTg0Ah6a

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

secret.txt  
Graphical user interface, text, application, email

Description automatically generated

1. The file contains a secret code with the format THM{\_\_\_\_\_}.

THM{SECRET\_\_CODE}