Act2

Q1. How many hackers are trying to get access to our servers? And how many attempts?

Approach : I just identify fail attempt (cuz mostly hacker cant be finish hack in first time so, it must have lot of fail tempting), and the number of hacker I identified by using souce_ip

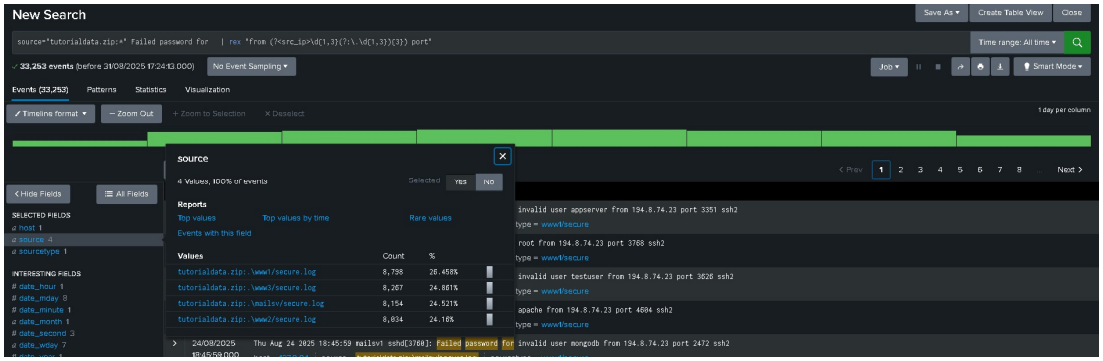
Answer: 185 unique hackers (distinct source IPs), 33,253 failed login attempts. Distinct hackers are identified by counting unique source IP addresses. Attempts are measured from failed login entries.

Q2. What time do hackers appear to try to hack our servers?

Answer: Hackers appear mainly around 18:00. Using Splunk timechart

Q3. Which server had the most attempts?

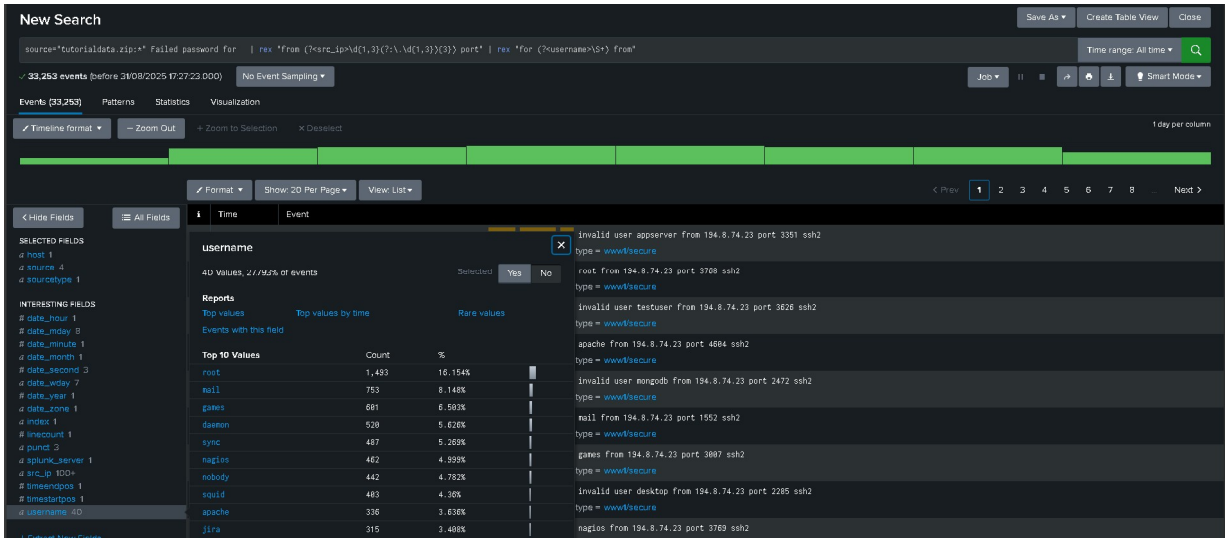
Answer: www1 server had the most failed attempts, 8,798 (~26.46%).



Q4. What is the most popular account that hackers use to try to break in?

Approach: I find that the username will appear middle of for and from so I just extract a new field and get the statics.

Answer: The 'root' account is the most targeted, with 1,493 attempts (16.15%).



Q5. Can you find attempts to get access to sensitive information from our web servers?

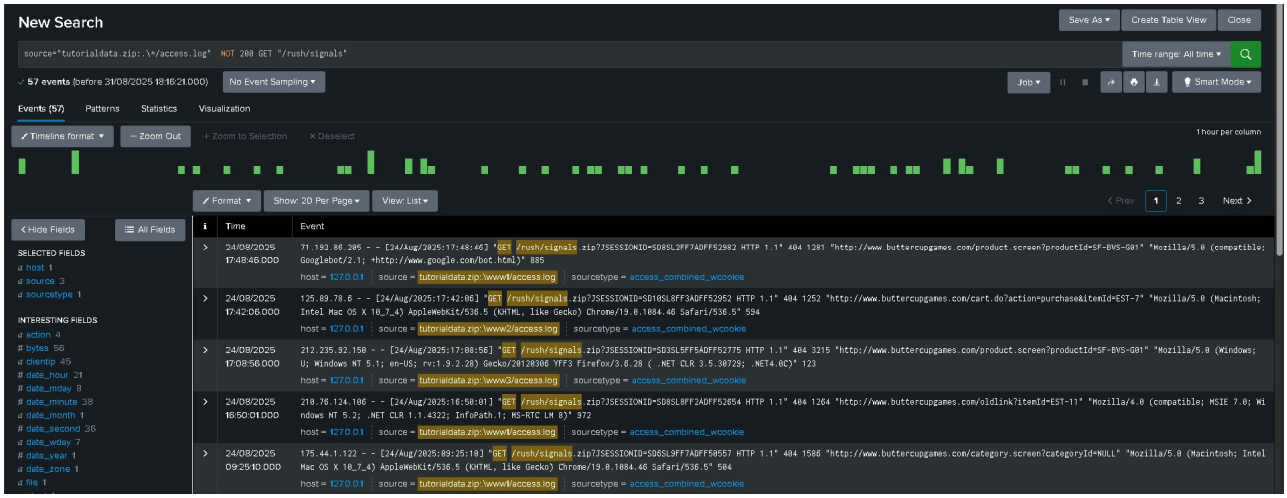
How many attempts were there?

Approach: Just identify some of sensitive file type like zip from fail get req, then I found that signals.zip was request multiple times.

Answer: Yes. 57 attempts were found.

Q6. What resource/file are hackers looking for?

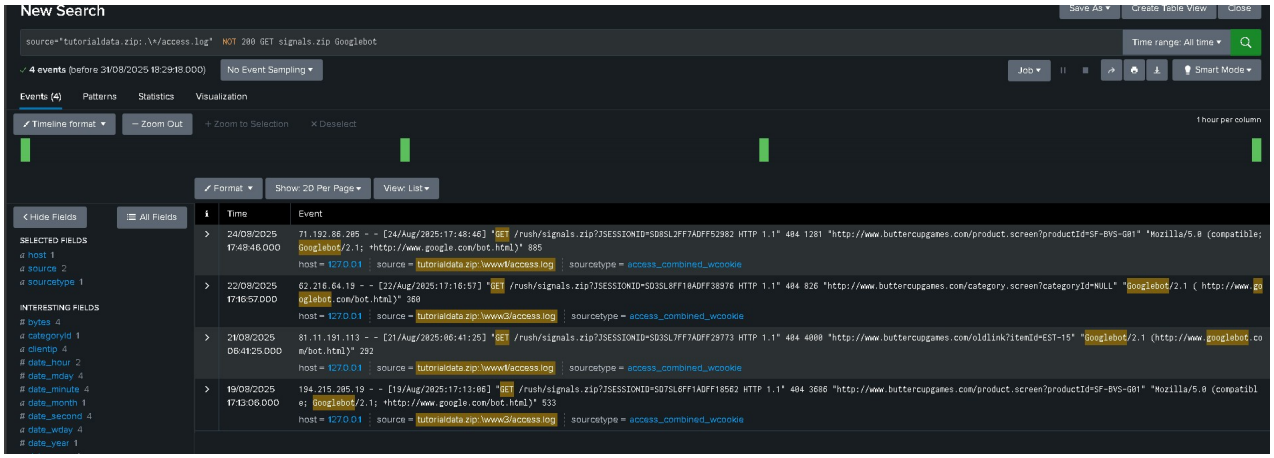
Answer: The main resource hackers are looking for is signals.zip.



Q7. Can you find any bots crawling our websites?

Answer: Yes. The User-Agent field shows Googlebot across multiple IPs, confirming it is

a web crawler.



Q8. What are they doing on the site?

Answer: The bots are crawling the site and attempting to access signals.zip.