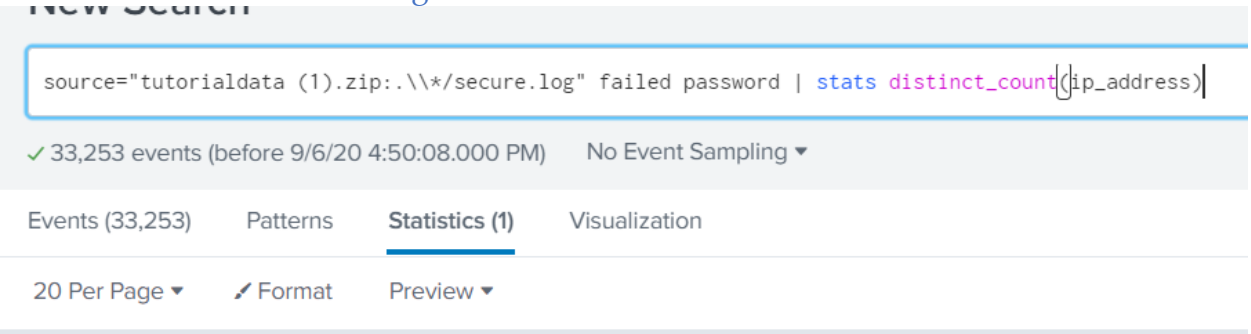
Part I. Can you find people trying to break into the servers?

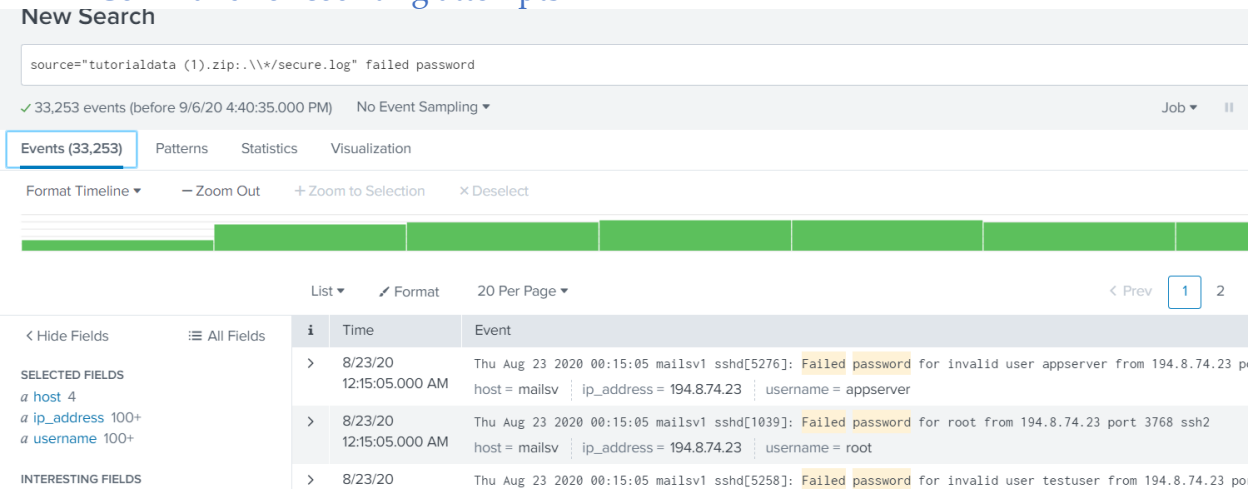
Q1. How many hackers are trying to get access to our servers? And how many attempts are there?

Hackers: 185, Attempts: 33253

Command for counting hacker

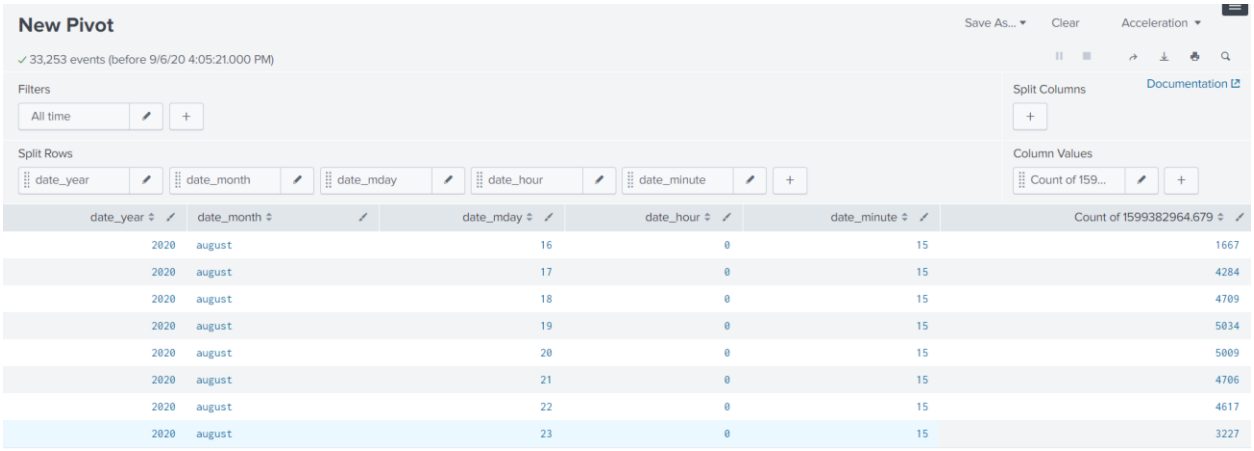


Command for counting attempts



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

16-23 Aug 2020 00:15:01

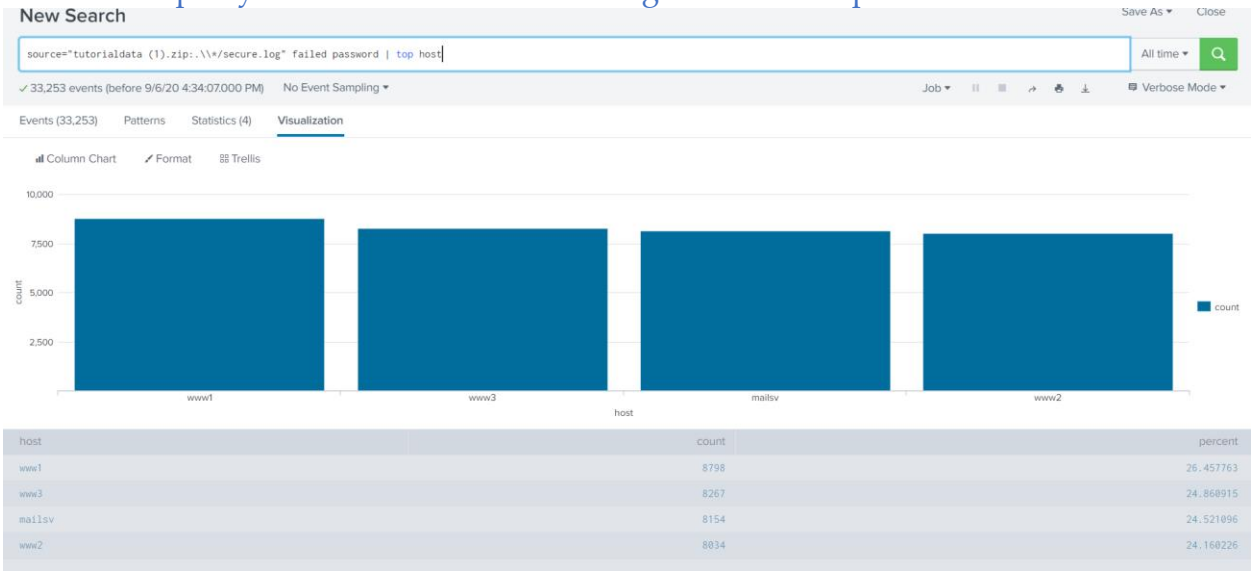


date_year	date_month	date_mday	date_hour	date_minute	Count of 1599382964.679
2020	august	16	0	15	1667
2020	august	17	0	15	4284
2020	august	18	0	15	4709
2020	august	19	0	15	5034
2020	august	20	0	15	5009
2020	august	21	0	15	4706
2020	august	22	0	15	4617
2020	august	23	0	15	3227

This result is visualized from search keyword “failed password”

Q3. Which server (mailsv, www1, www2, www3) seem to see the most attempts?

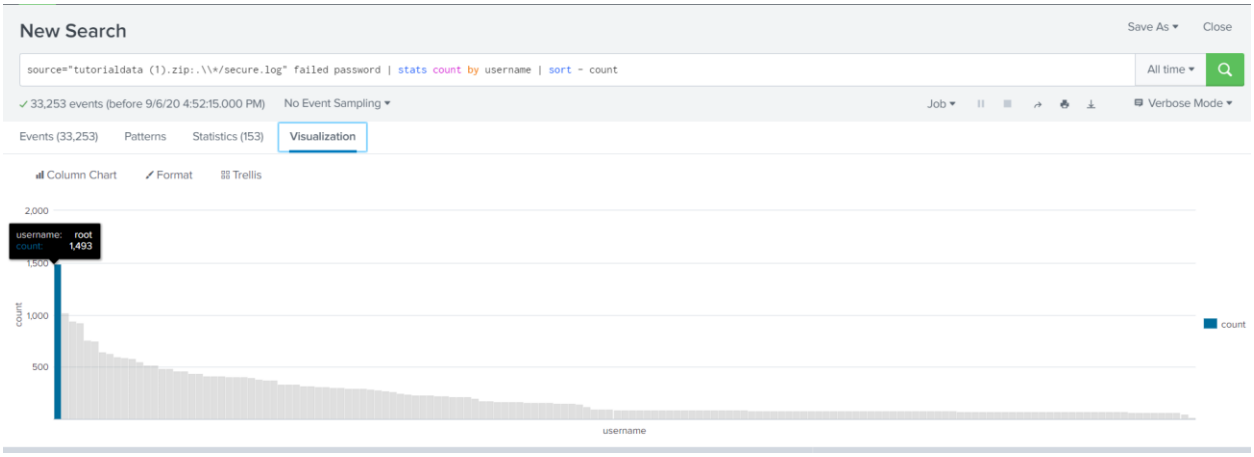
It’s equally distribute but www1 hold get most attempts



host	count	percent
www1	8798	26.457763
www3	8267	24.860915
mailsv	8154	24.521096
www2	8034	24.160226

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

root

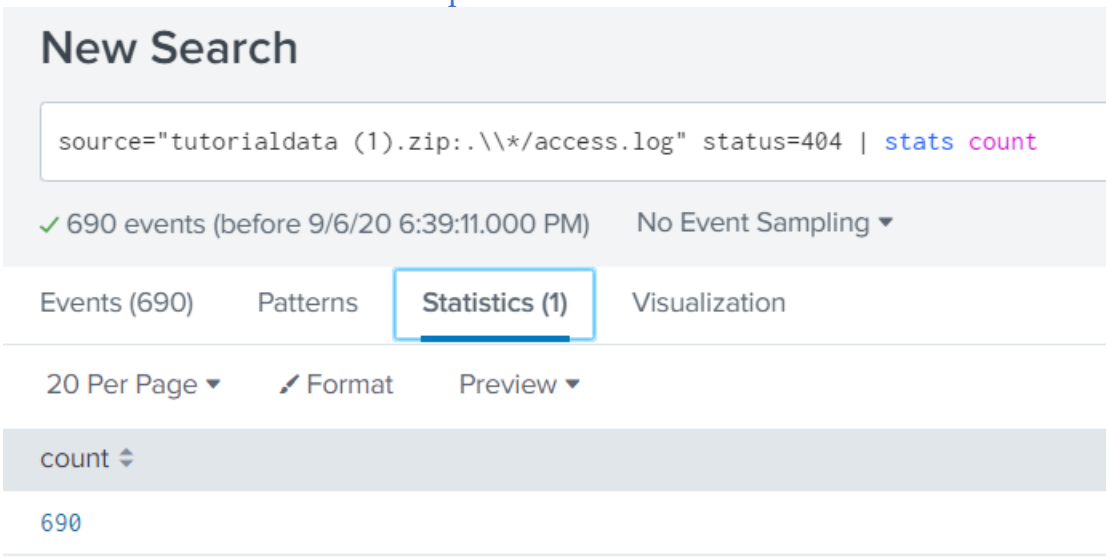


Part II. Sensitive Files on Web Servers

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

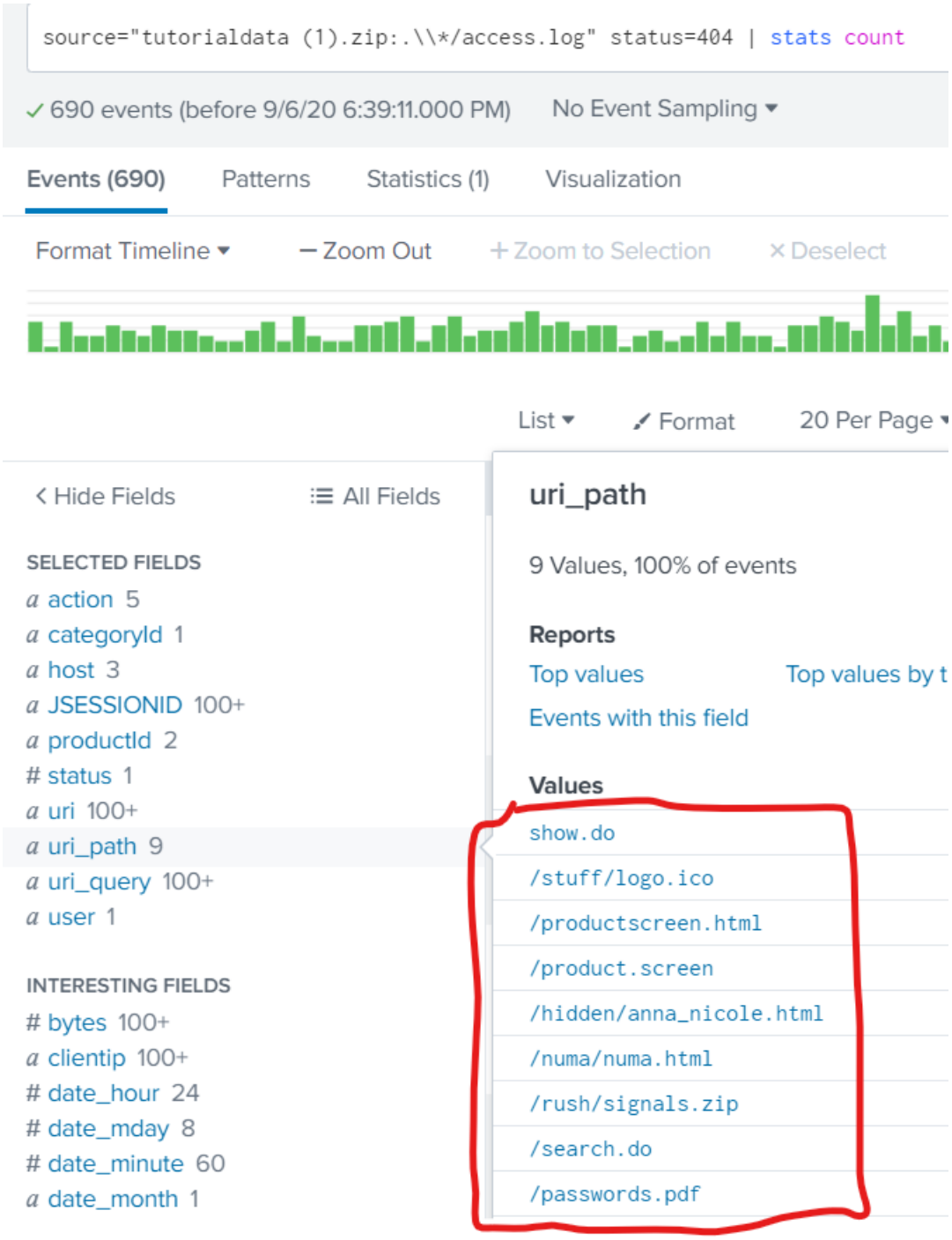
I guess that request not found (404) can infer hacker try to access to sensitive information without knowing endpoint.

Then there are 690 attempts.



Q6. What resource/file are hackers looking for?

List below are resources that they are looking for.


source="tutorialdata (1).zip:.*/access.log" status=404 | stats count
690 events (before 9/6/20 6:39:11.000 PM)
No Event Sampling
Events (690)
Patterns
Statistics (1)
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a action 5
a categoryId 1
a host 3
a JSESSIONID 100+
a productId 2
status 1
a uri 100+
a uri_path 9
a uri_query 100+
a user 1
INTERESTING FIELDS
bytes 100+
a clientip 100+
date_hour 24
date_mday 8
date_minute 60
a date_month 1
uri_path
9 Values, 100% of events
Reports
Top values
Top values by t
Events with this field
Values
show.do
/stuff/logo.ico
/productscreen.html
/product.screen
/hidden/anna_nicole.html
/numa/numa.html
/rush/signals.zip
/search.do
/passwords.pdf