



# Cybersecurity

## Project 3 Review Questions

Make a copy of this document before you begin. Place your answers below each question.

### Windows Server Log Questions

#### Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, our report shows changes in severity levels; after the attack, there is an increase in severity from around 14%.

The first screenshot displays the severity count before the attack.

The screenshot shows a 'Severity Level Report' for the source 'windows\_server\_logs.csv' on host 'Habib-PC'. It displays 4,761 events before 08/08/2023 14:01:13.000. The report is filtered by 'top severity'. The table below shows the distribution of severity levels.

| severity      | count | percent   |
|---------------|-------|-----------|
| informational | 4429  | 93.885330 |
| high          | 329   | 6.914670  |

The second screenshot displays the severity count after the attack.

The screenshot shows a 'Severity Level Report' for the source 'windows\_server\_logs.csv' on host 'Habib-PC'. It displays 5,948 events before 08/08/2023 14:07:44.000. The report is filtered by 'top severity'. The table below shows the distribution of severity levels.

| severity      | count | percent   |
|---------------|-------|-----------|
| informational | 4381  | 79.770575 |
| high          | 1111  | 20.229425 |

## Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, Windows activity after the attack showed that the number of successful logins increased from 4,616 to 5,854, which means 1,238 successfully logged in to the VSI domain during the attack. In contrast, the number of failed login got decreased from 142 to 91.

The image contains two screenshots of a Splunk search interface. The top screenshot shows a search for 'windows\_server\_logs.csv' with 4,758 events. The bottom screenshot shows a search for 'windows\_server\_attack\_logs.csv' with 5,948 events. Both screenshots display a table with columns for status, count, and percent.

| status  | count | percent   |
|---------|-------|-----------|
| success | 4616  | 97.015553 |
| failure | 142   | 2.984447  |

| status  | count | percent   |
|---------|-------|-----------|
| success | 5854  | 98.436186 |
| failure | 93    | 1.563814  |

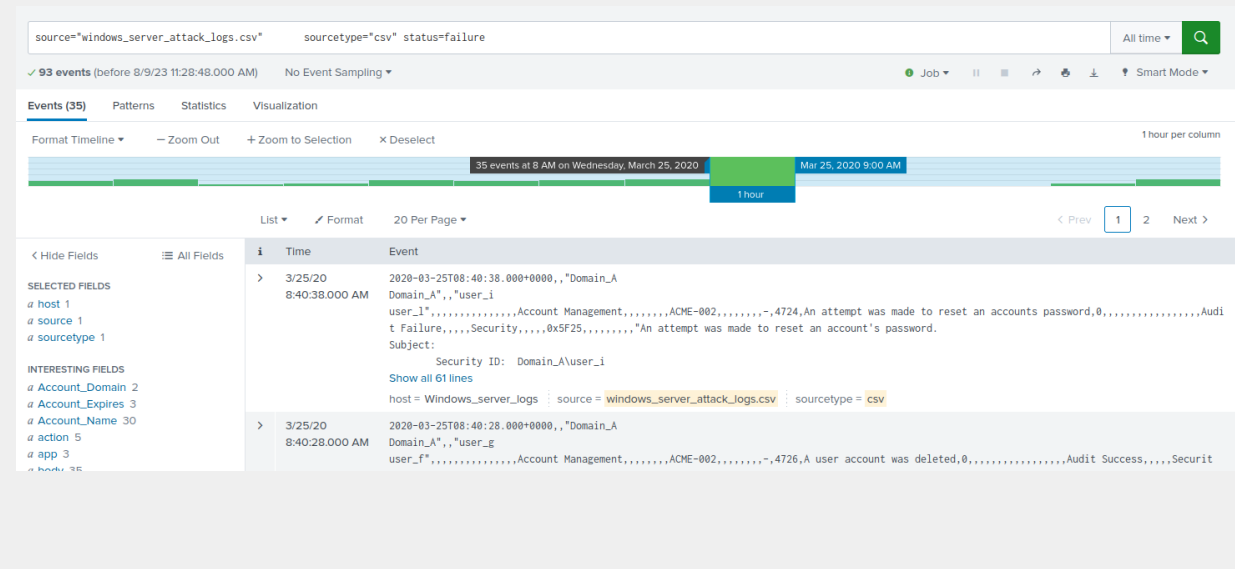
## Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes, Our alert detected a suspicious volume for failed Windows activity.

- If so, what was the count of events in the hour(s) it occurred?

The count of events was 35 failed Windows activities.



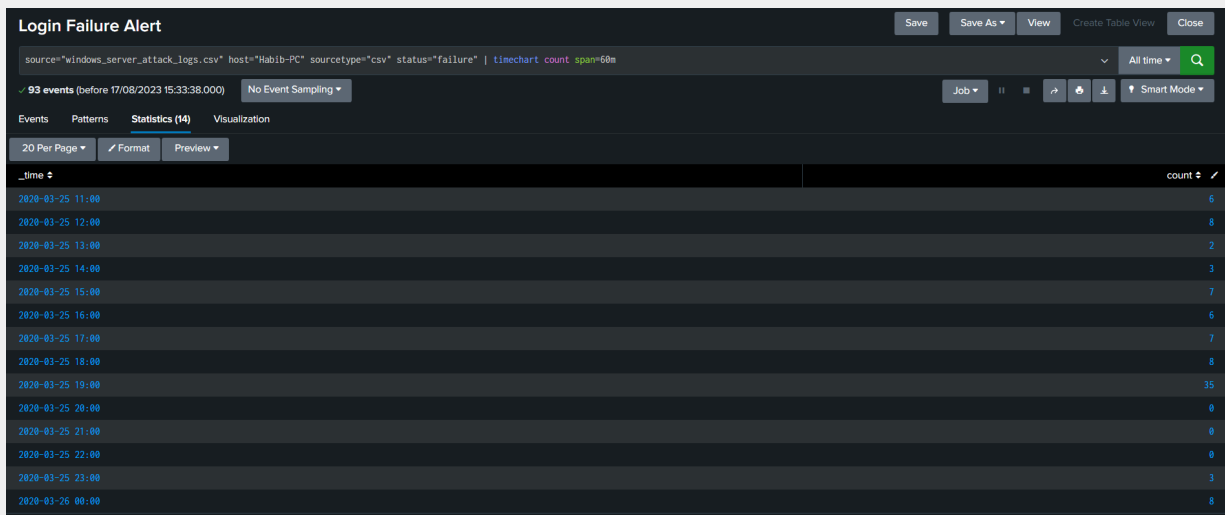
- When did it occur?

It occurred at 8:00 AM on Wednesday, March 25, 2020.

- Would your alert be triggered for this activity?

Yes, we received an alert for Windows failed login activities because I set my alert to be triggered when the number of failed logins exceeds 15.

Then the system will send the automatic email to the SOC team.



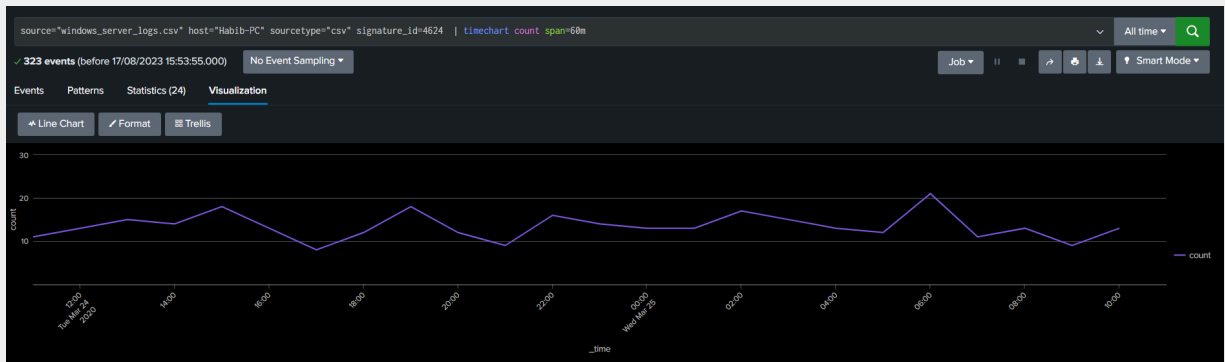
- After reviewing, would you change your threshold from what you previously selected?

I would not change our threshold as it was set low enough to be triggered by this attack and high enough that we were not getting false positives during the other hours of the attack resulting in alert fatigue.

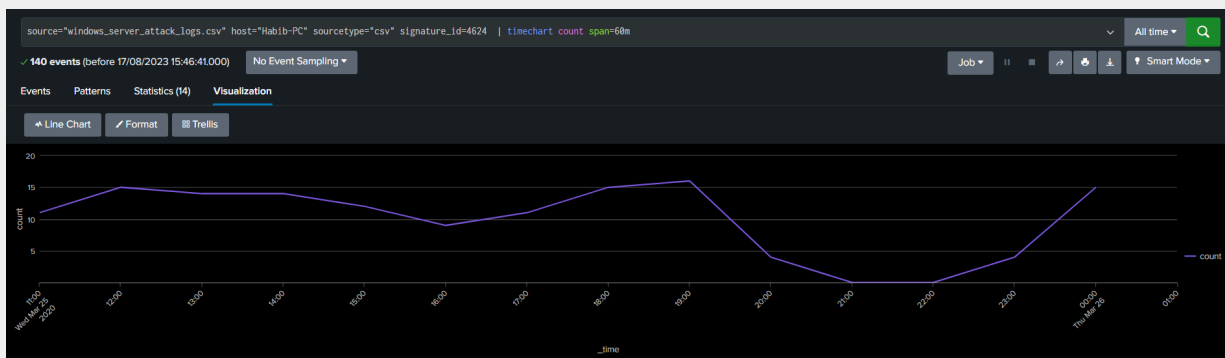
## Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Log before attack



## Attack log



The data above shows an increase in the total number an account successfully logged on. The usual data shows a top of 21, whereas on the day of the attack, we can see it exceeding our threshold of 25

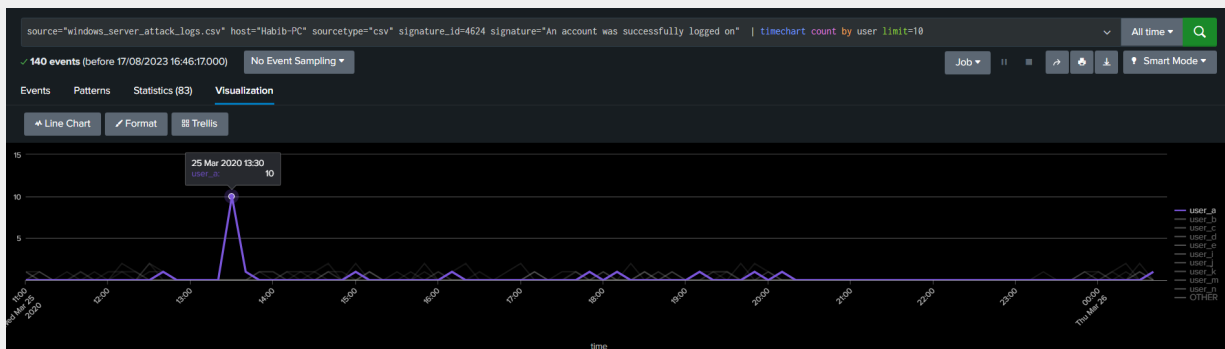
- If so, what was the count of events in the hour(s) it occurred?



The count of the event in one hour time chart period for successful login dated March 25, 2020, at 6:00 AM was 21, then the count of events dropped to 11 at 7:00 AM of the same day.

- Who is the primary user logging in?

The primary user logging in is user\_a, with a count of 10

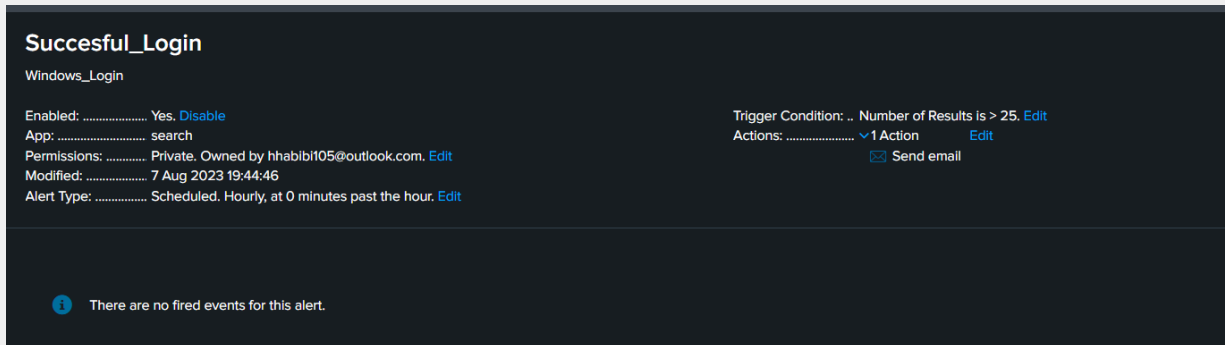


- When did it occur?

It occurred at 13:20 on March 25, 2020,

- Would your alert be triggered for this activity?

No, our alert will not be triggered as we set our threshold to alert us if there are more than 25 successful logins within an hour.



- After reviewing, would you change your threshold from what you previously selected?

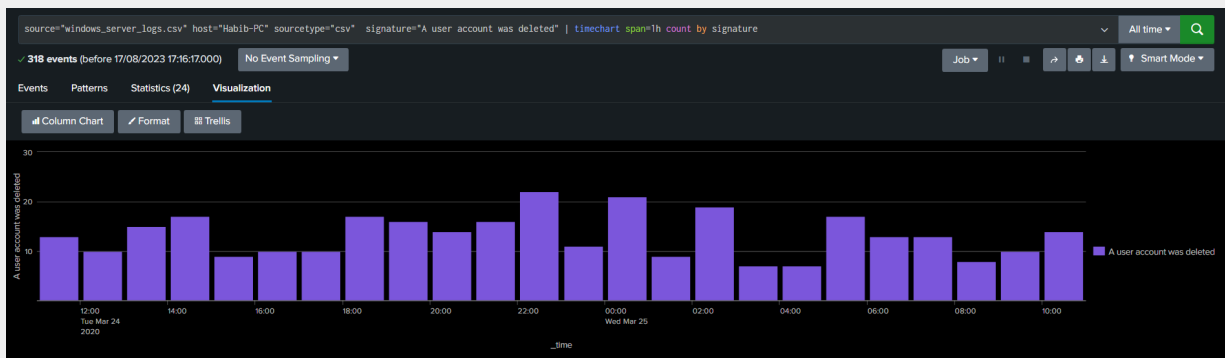
Yes, I will change our threshold slightly, but more log data analysis is to make that determination as we want to avoid alert fatigue. We will want to create an alert if logins dip below a certain number per hour, as this attack affected login capabilities. I also prefer to set additional alerts as the activity for signature events increased that we were not monitoring for.

## Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes, we did notice a suspicious volume of deleted accounts; the attack started at 11:00 AM on March 25, 2020. We can see from the below charts that there was a significant drop in the count of account deletions.

Before attack



source="windows\_server\_logs.csv" host="Habib-PC" sourcetype="csv" signature="A user account was deleted" | stats count by signature

318 events (before 17/08/2023 17:06:54.000) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

| signature                  | count |
|----------------------------|-------|
| A user account was deleted | 318   |

After attack



source="windows\_server\_attack\_logs.csv" host="Habib-PC" sourcetype="csv" signature="A user account was deleted" | stats count by signature

130 events (before 17/08/2023 17:05:53.000) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

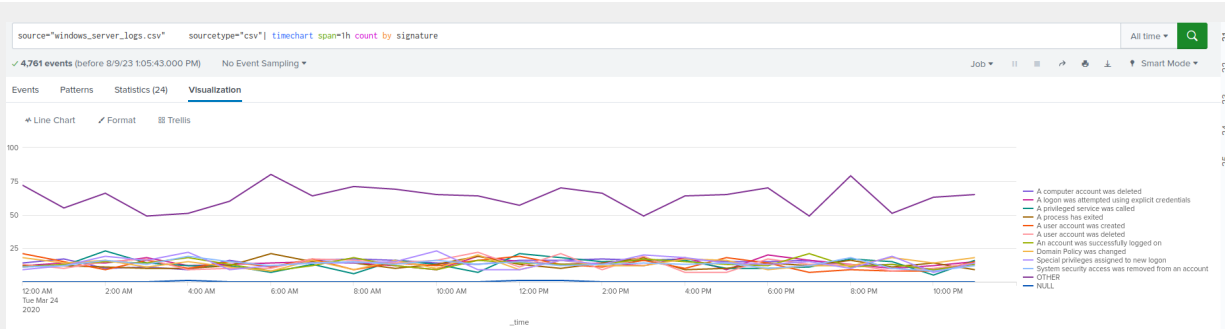
| signature                  | count |
|----------------------------|-------|
| A user account was deleted | 130   |

## Dashboard Analysis for Time Chart of Signatures

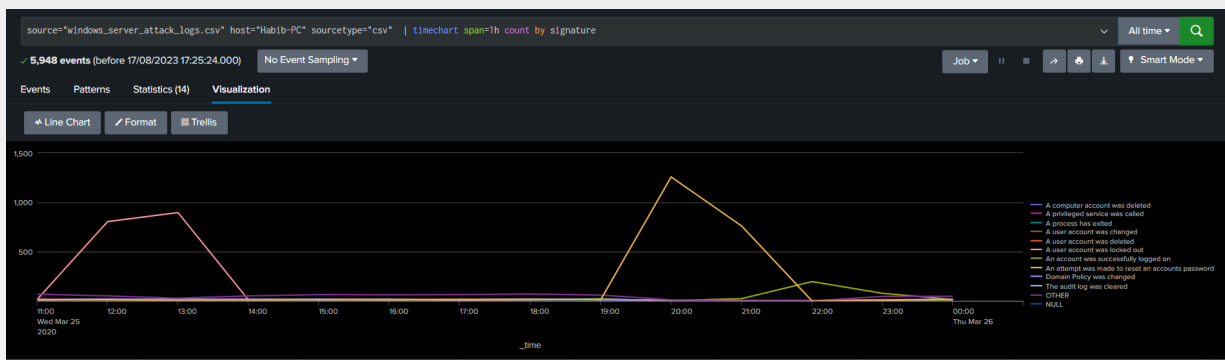
- Does anything stand out as suspicious?

Yes, in the attack logs, some events stand out from the regular Windows activity logs.





## After the attack



- What signatures stand out?

In Windows events by signature, the time chart shows a significant increase in activity:

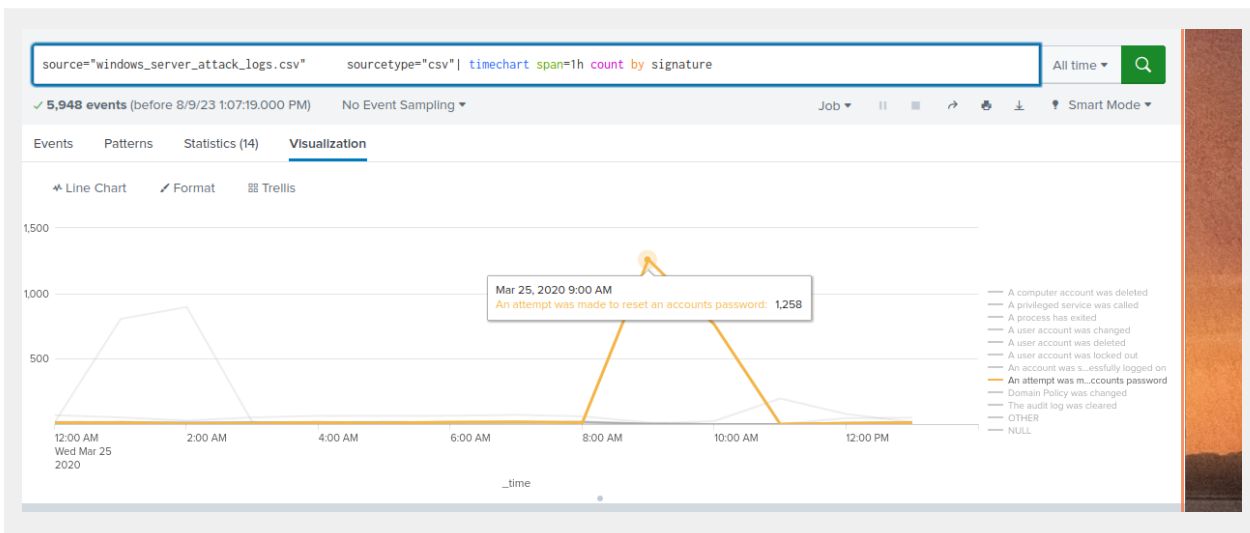
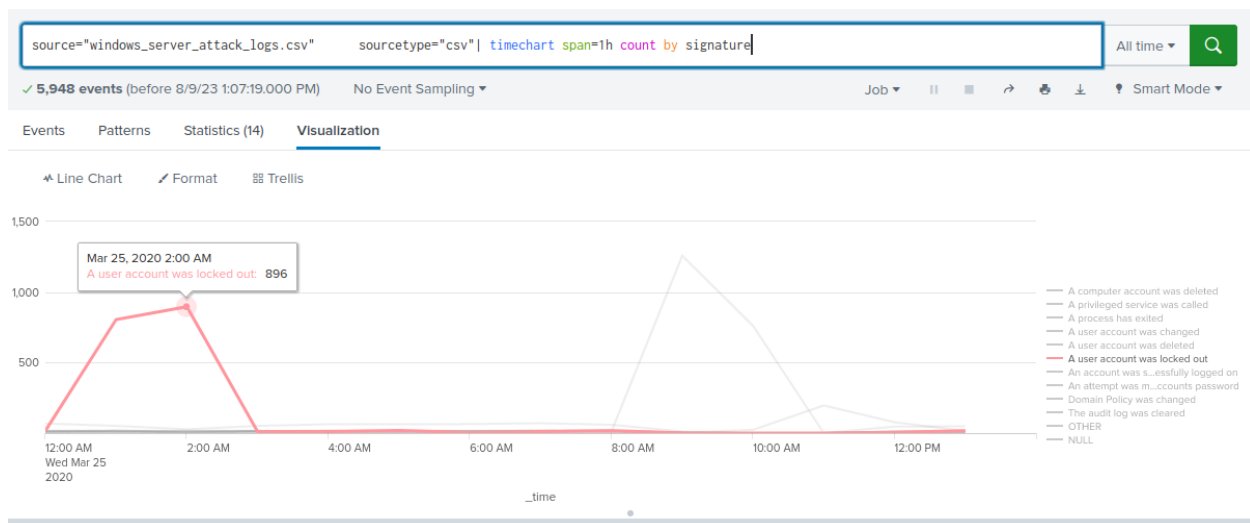
- Account password reset attempt
- A user account was locked out

- What time did it begin and stop for each signature?

The user account locked down attack began around 1:00 AM and ended at 3:00 AM on March 25, 2020. The password reset attack started at 9:00 AM and lasted until 11:00 AM on March 25, 2020.

- What is the peak count of the different signatures?

The peak for password reset attempts was 1258, followed by the user account locked-out attack the peak count is 896; for the rest of attacks related to account signature, please read the below table.



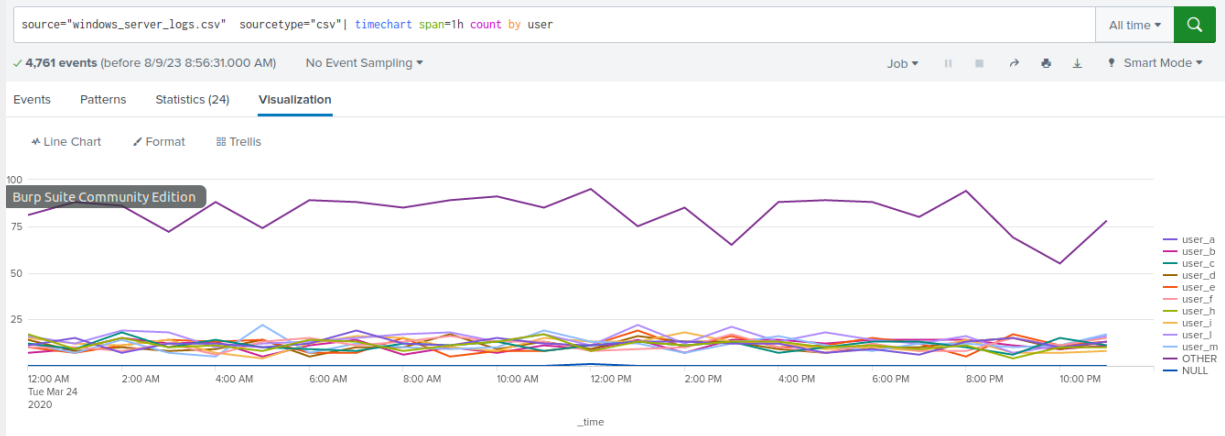
## Dashboard Analysis for Users

- Does anything stand out as suspicious?

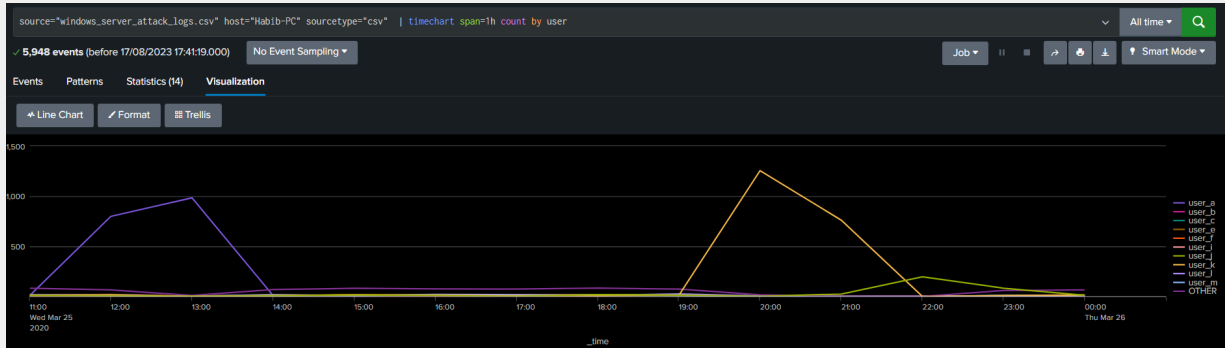
Yes, there is a suspicious spike in user activity from 2 separate accounts ( User\_a & User\_k ). Screens shots below give evidence of our findings

- Which users stand out?

Before attack:



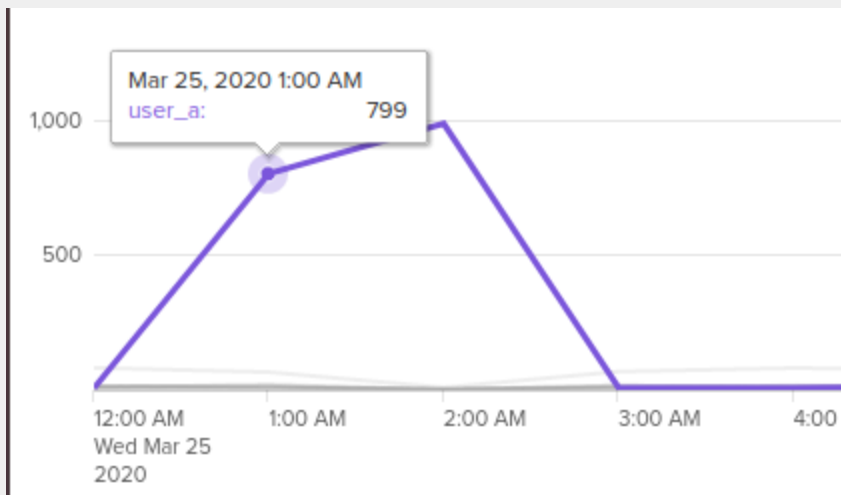
After attack:



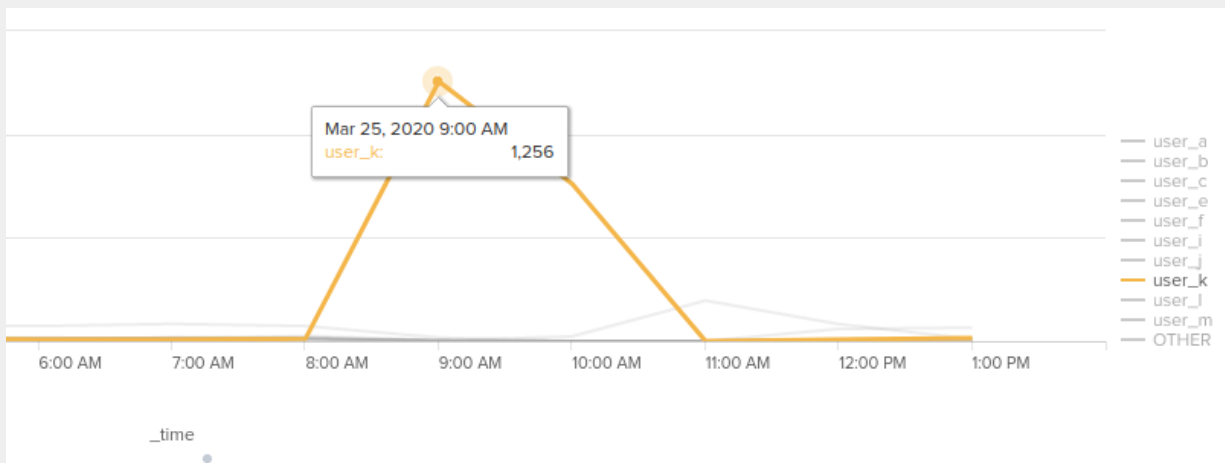
Both user\_a and user\_k have higher than usual activity within their accounts compared to normal data, as shown in the above screenshots

- What time did it begin and stop for each user?

User\_a - started at 1:00 AM and stopped at 3:00 AM, dated March,25,2020



User\_k - started at 9:00 AM and stopped at 11:00 AM, dated March,25,2020



| _time            | user_a | user_b | user_c | user_e | user_f | user_i | user_j | user_k | user_l | user_m | OTHER |
|------------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|-------|
| 2020-03-25 00:00 | 7      | 11     | 12     | 10     | 10     | 14     | 11     | 8      | 14     | 13     | 82    |
| 2020-03-25 01:00 | 799    | 18     | 12     | 20     | 9      | 15     | 6      | 9      | 9      | 10     | 66    |
| 2020-03-25 02:00 | 984    | 3      | 0      | 1      | 2      | 0      | 2      | 2      | 3      | 1      | 9     |
| 2020-03-25 03:00 | 8      | 13     | 8      | 17     | 9      | 12     | 8      | 4      | 17     | 10     | 68    |
| 2020-03-25 04:00 | 8      | 10     | 10     | 5      | 15     | 9      | 15     | 16     | 8      | 10     | 81    |
| 2020-03-25 05:00 | 13     | 6      | 9      | 14     | 9      | 10     | 9      | 13     | 19     | 15     | 75    |
| 2020-03-25 06:00 | 10     | 9      | 11     | 14     | 14     | 9      | 2      | 7      | 17     | 12     | 73    |
| 2020-03-25 07:00 | 16     | 11     | 9      | 15     | 14     | 8      | 18     | 7      | 10     | 15     | 83    |
| 2020-03-25 08:00 | 18     | 14     | 7      | 9      | 12     | 12     | 13     | 12     | 25     | 10     | 73    |
| 2020-03-25 09:00 | 3      | 1      | 5      | 0      | 1      | 2      | 2      | 1256   | 5      | 1      | 17    |
| 2020-03-25 10:00 | 0      | 0      | 0      | 0      | 0      | 0      | 23     | 761    | 0      | 0      | 0     |
| 2020-03-25 11:00 | 0      | 0      | 0      | 0      | 0      | 0      | 196    | 0      | 0      | 0      | 0     |
| 2020-03-25 12:00 | 4      | 8      | 10     | 3      | 6      | 4      | 82     | 8      | 6      | 7      | 59    |
| 2020-03-25 13:00 | 8      | 5      | 12     | 9      | 8      | 11     | 11     | 15     | 12     | 8      | 65    |

- What is the peak count of the different users?

User\_a - 984

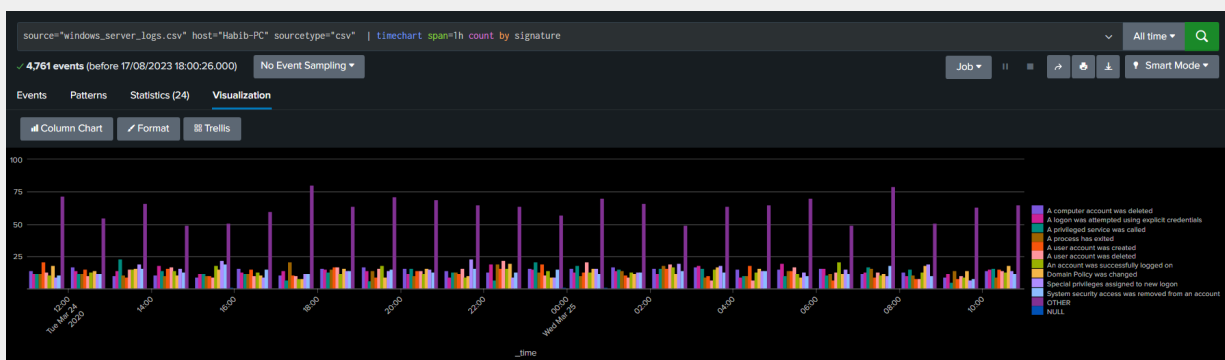
User\_k - 1256

## Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

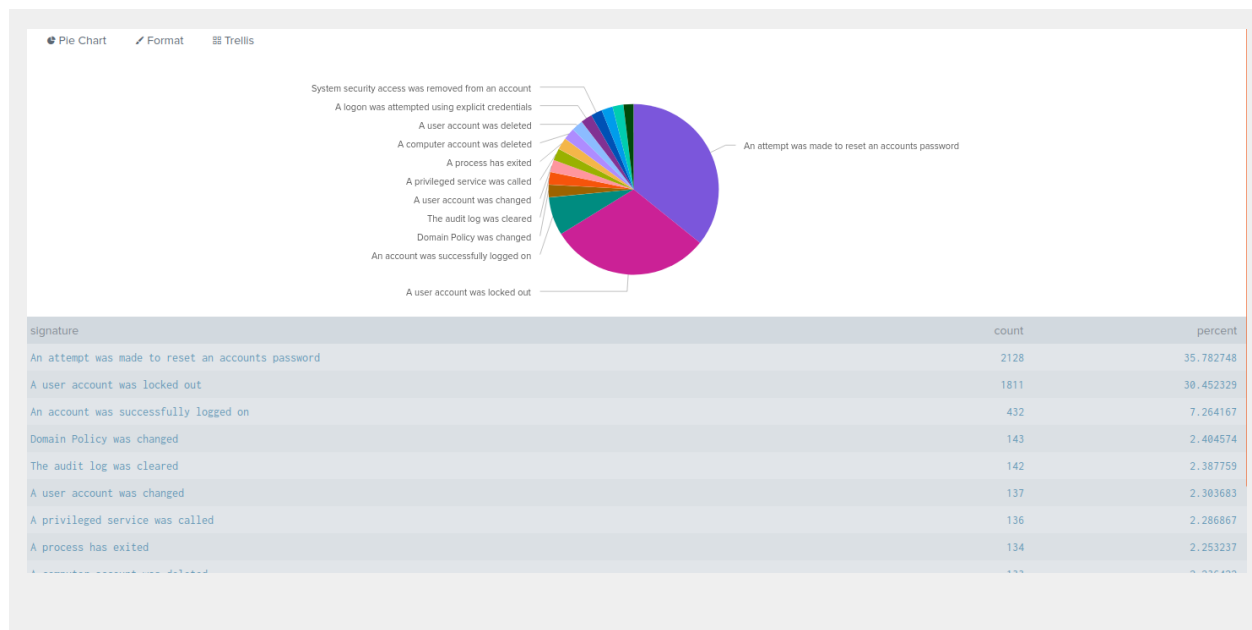
- Does anything appear suspicious?

The suspicious activity is carried out in two signature types: An attempt was made to reset an account password, and a User account was locked out.

Before attack



After attack, logs are shown below.



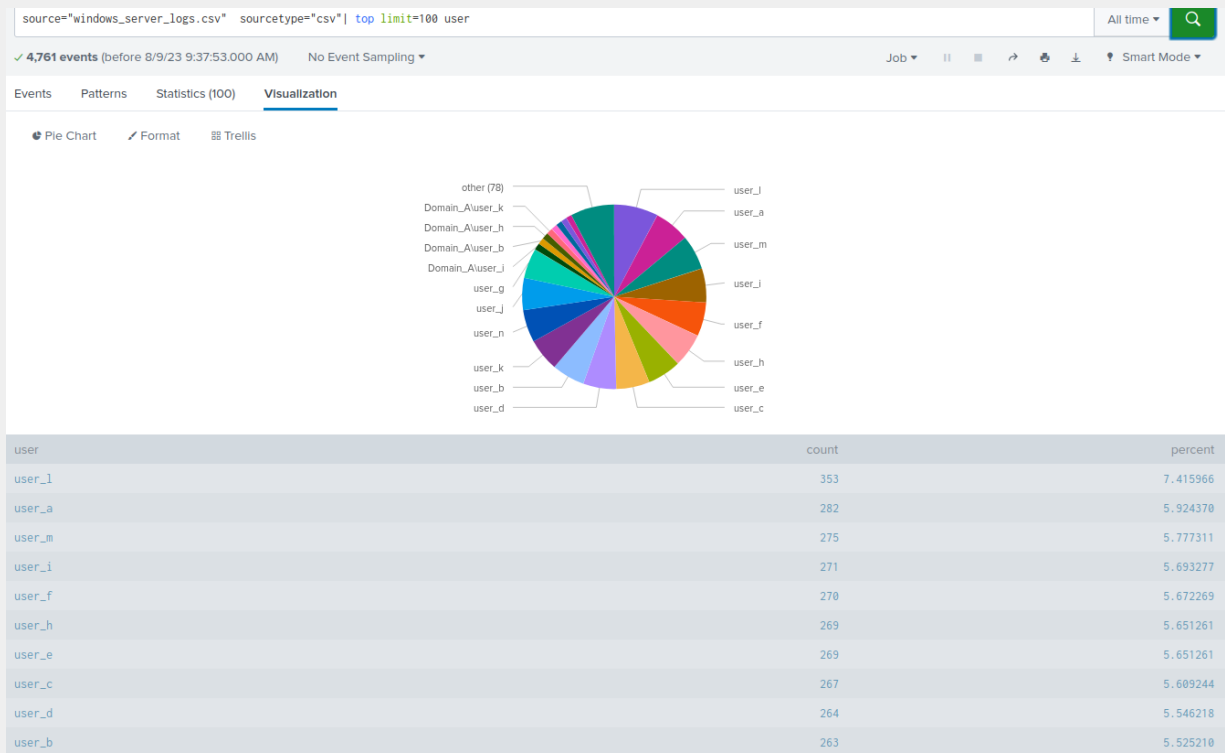
- Do the results match your findings in your time chart for signatures?

Yes, they match as the overall data shows a spike in both “ Account password reset attempt and A user account was locked out”, which is reflected on normal logs vs attack day logs graphs above

## Dashboard Analysis for Users with Bar, Graph, and Pie Charts

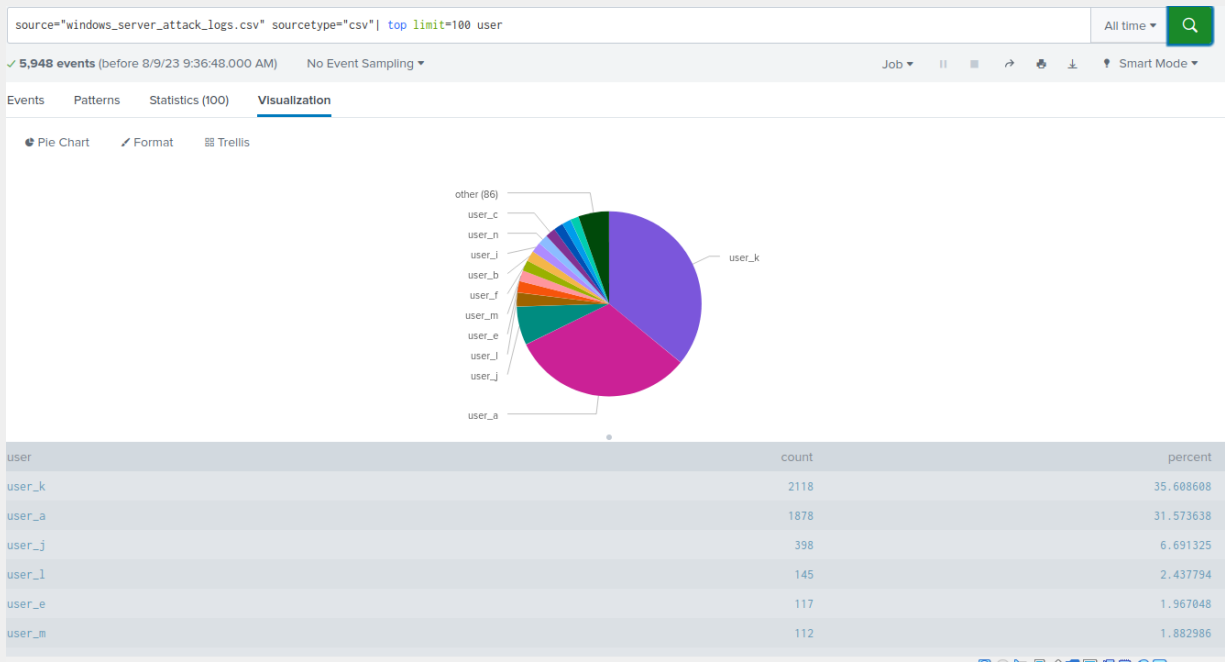
- Does anything stand out as suspicious?

Before the attack:



After the attack:

Yes, there is an increase in the number of activities by user\_a and user\_k



- Do the results match your findings in your time chart for users?

This information is reflective of our above findings of an attack on the user\_a account, which began at 1 am and the user\_k account, which began at 9 am, causing a spike in their user activity

## Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

An advantage of using the statistical time charts for signature and user is that you can quickly read the count for each event or the user per hour and find out exactly when the attack began. The disadvantage of using these over the bar chart and pie chart is that it needs to be made apparent when there was a change in activity.



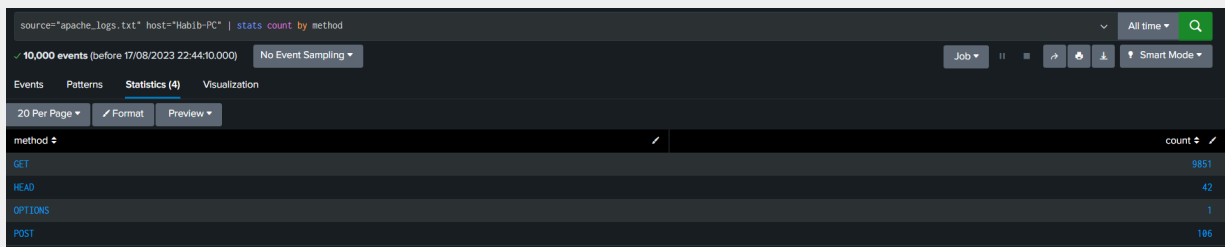
The visualisations in the line chart show you where is the spikes or declines in an event and what time the event occurs. The pie chart quickly shows you which event or user has an increase in activity.

## Apache Web Server Log Questions

### Report Analysis for Methods

- Did you detect any suspicious changes in HTTP methods? If so, which one?

Before the attack:



source="apache\_logs.txt" host="Habib-PC" | stats count by method

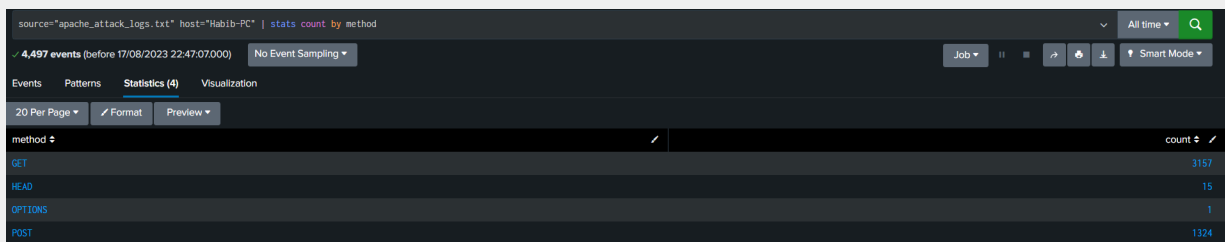
10,000 events (before 17/08/2023 22:44:10.000) No Event Sampling

Events Patterns Statistics (4) Visualization

20 Per Page Format Preview

| method  | count |
|---------|-------|
| GET     | 9851  |
| HEAD    | 42    |
| OPTIONS | 1     |
| POST    | 106   |

After the attack:



source="apache\_attack\_logs.txt" host="Habib-PC" | stats count by method

4,497 events (before 17/08/2023 22:47:07.000) No Event Sampling

Events Patterns Statistics (4) Visualization

20 Per Page Format Preview

| method  | count |
|---------|-------|
| GET     | 3157  |
| HEAD    | 15    |
| OPTIONS | 1     |
| POST    | 1324  |

Yes, we can notice a significant increase in HTTP POST requests during the attack.

- What is that method used for?

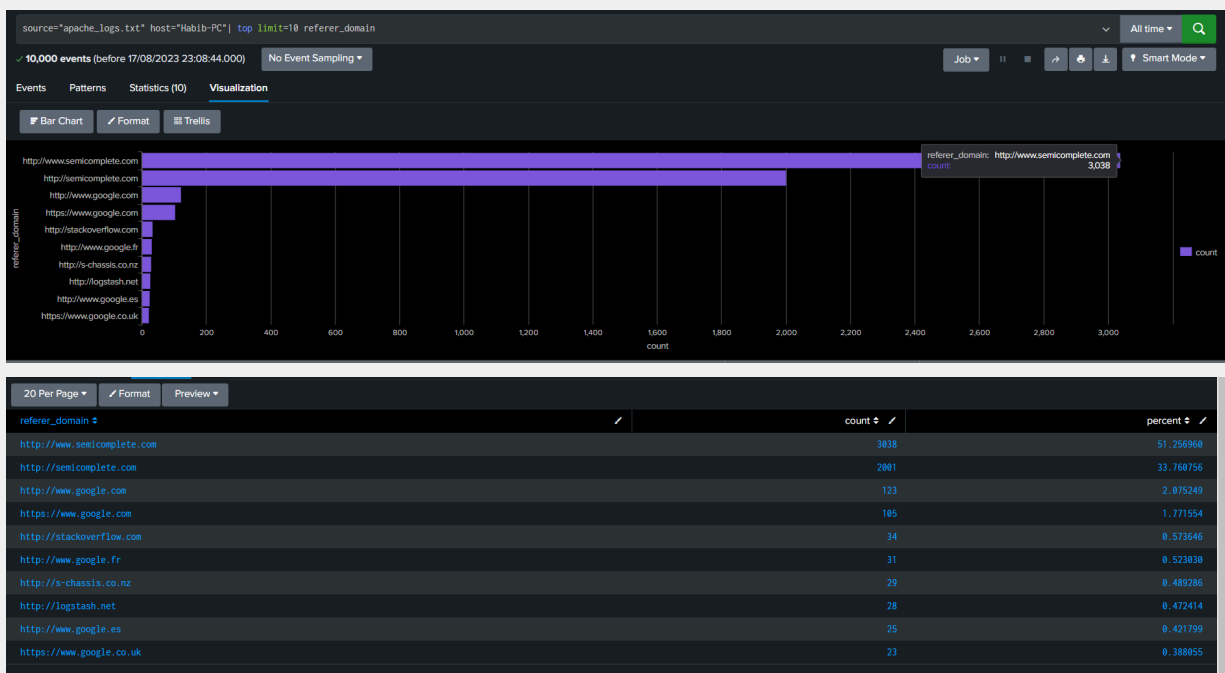
The HTTP GET method is one of the standard request methods used in the Hypertext Transfer Protocol (HTTP) to retrieve data from a web server. It is commonly used when requesting information or resources from a specific URL.

Unlike the HTTP GET method, which is used to retrieve data, the POST method is used to send data from the client to the server in the body of the request. This data can be in various formats, such as HTML form data, JSON, XML, or any other format that the server supports.

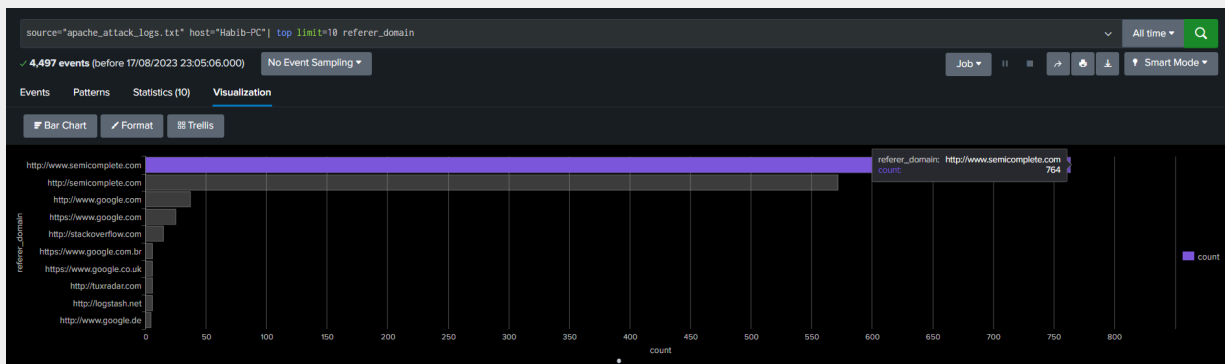
## Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Before attack:



After attack:



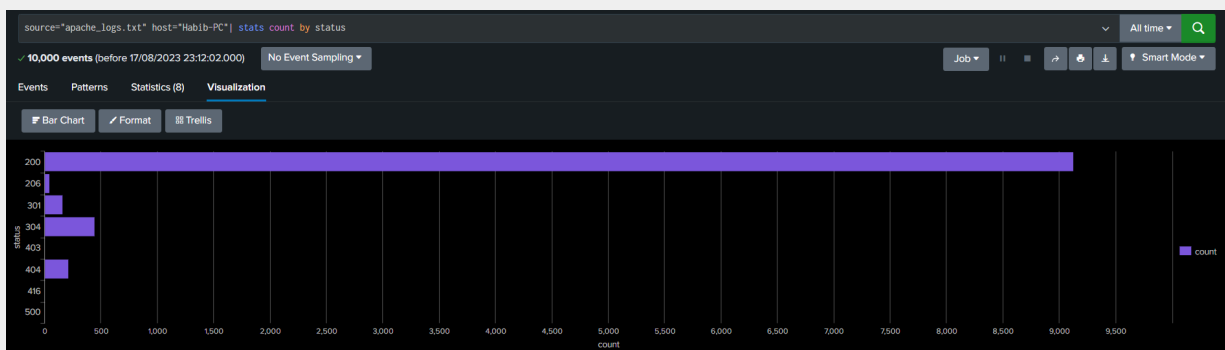
| source="apache_attack_logs.txt" host="Habib-PC"   top limit=10 referrer_domain |          |                 |               | All time          | 🔍       |
|--|----------|-----------------|---------------|-------------------|---------|
| 4,497 events (before 17/08/2023 23:05:06.000)                                  |          |                 |               | No Event Sampling |         |
| Events   | Patterns | Statistics (10) | Visualization | Job               | ⏏       |
| Bar Chart  | Format   | Trellis         |               | 📄                 | 📁       |
|  |          |                 |               | Smart Mode        |         |
| 20 Per Page  |          |                 |               | Format            | Preview |
| referrer_domain  |          | count           | percent       |                   |         |
| http://www.semicomplete.com  |          | 764             | 49.226884     |                   |         |
| http://semicomplete.com  |          | 572             | 36.855670     |                   |         |
| http://www.google.com  |          | 37              | 2.384021      |                   |         |
| https://www.google.com   |          | 25              | 1.610825      |                   |         |
| http://stackoverflow.com   |          | 15              | 0.966495      |                   |         |
| https://www.google.com.br  |          | 6               | 0.386598      |                   |         |
| https://www.google.co.uk   |          | 6               | 0.386598      |                   |         |
| http://tuxrader.com  |          | 6               | 0.386598      |                   |         |
| http://logstash.net  |          | 6               | 0.386598      |                   |         |
| http://www.google.de   |          | 5               | 0.322165      |                   |         |

We did see some changes in the results of the top 10 referrer domains, with the last 5 of the list.

## Report Analysis for HTTP Response Codes

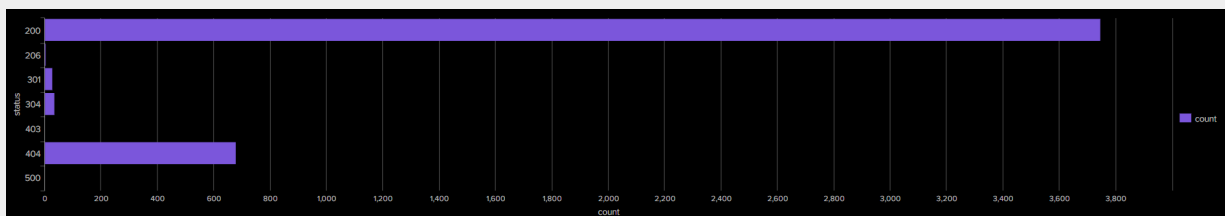
- Did you detect any suspicious changes in HTTP response codes?

Before:



| status ↕ ✎ | count ↕ ✎ |
|------------|-----------|
| 200        | 9126      |
| 206        | 45        |
| 301        | 164       |
| 304        | 445       |
| 403        | 2         |
| 404        | 213       |
| 416        | 2         |
| 500        | 3         |

After attack:



| status ↕ ✎ | count ↕ ✎ |
|------------|-----------|
| 200        | 3746      |
| 206        | 5         |
| 301        | 29        |
| 304        | 36        |
| 403        | 1         |
| 404        | 679       |
| 500        | 1         |

A 404 status code could occur for various reasons, such as if the URL is mistyped, the resource has been moved or deleted, the server is misconfigured, or the server is down.

When encountering a 404 error, users typically see a "404 Not Found" message in their web browser, indicating that the requested page or resource is unavailable.

After the attack, we noticed a significant increase in 404 status codes, meaning that the server could not load up the requested page or the server got down.

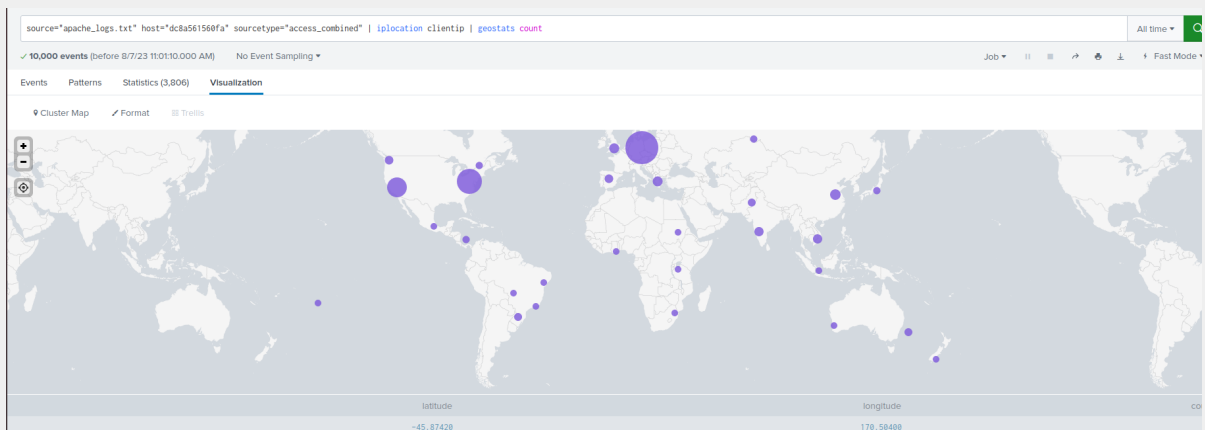
HTTP response code 200 is one of the standard status codes a web server can send to respond to an HTTP request. It indicates that the request has been successfully processed, and the server returns the requested data as the response.

Also saw a significant decrease in the status code 200 and 206 (partial loading of requested resources) at the time of the attack.

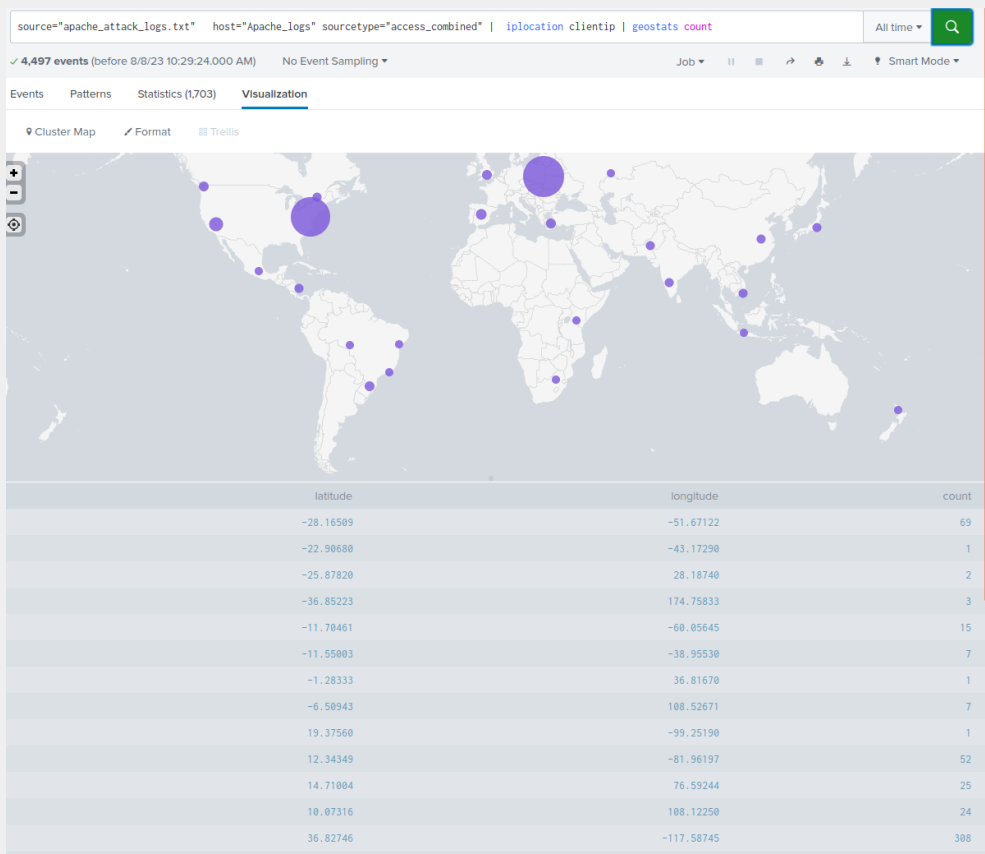
## Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Before the attack:



After the attack:



Decreased nearly half of all international activity.

During the period of the attack, a suspicious volume of activity came from Ukraine

- If so, what was the count of the hour(s) it occurred in?

2 occurrences, one at 6:00 PM (730 ) and one at 8:00 PM (1415 )

|                  |      |
|------------------|------|
| 2020-03-25 18:00 | 730  |
| 2020-03-25 20:00 | 1415 |

Alt answer:

937 events at 8:05 PM

- Would your alert be triggered for this activity?

Yes, our alert will be triggered as we set our threshold to alert us if there are more than 150 international activities in an hour.

- After reviewing, would you change the threshold that you previously selected?

No, as our threshold was set at a perfect amount where it wasn't falsely alerting normal hourly activities and only flagged for the two high-volume international activities

### **Alert Analysis for HTTP POST Activity**

- Did you detect any suspicious volume of HTTP POST activity?

Yes, during the attack, there was a significant spike in HTTP post activity

- If so, what was the count of the hour(s) it occurred in?

The count was 1296

- When did it occur?

8:05 PM March 25, 2020,

- After reviewing, would you change the threshold that you previously selected?

I would not initially change my threshold value, which is currently set to 15. I would prefer to further analyse my daily Apache logs to determine if the number could be safely increased.

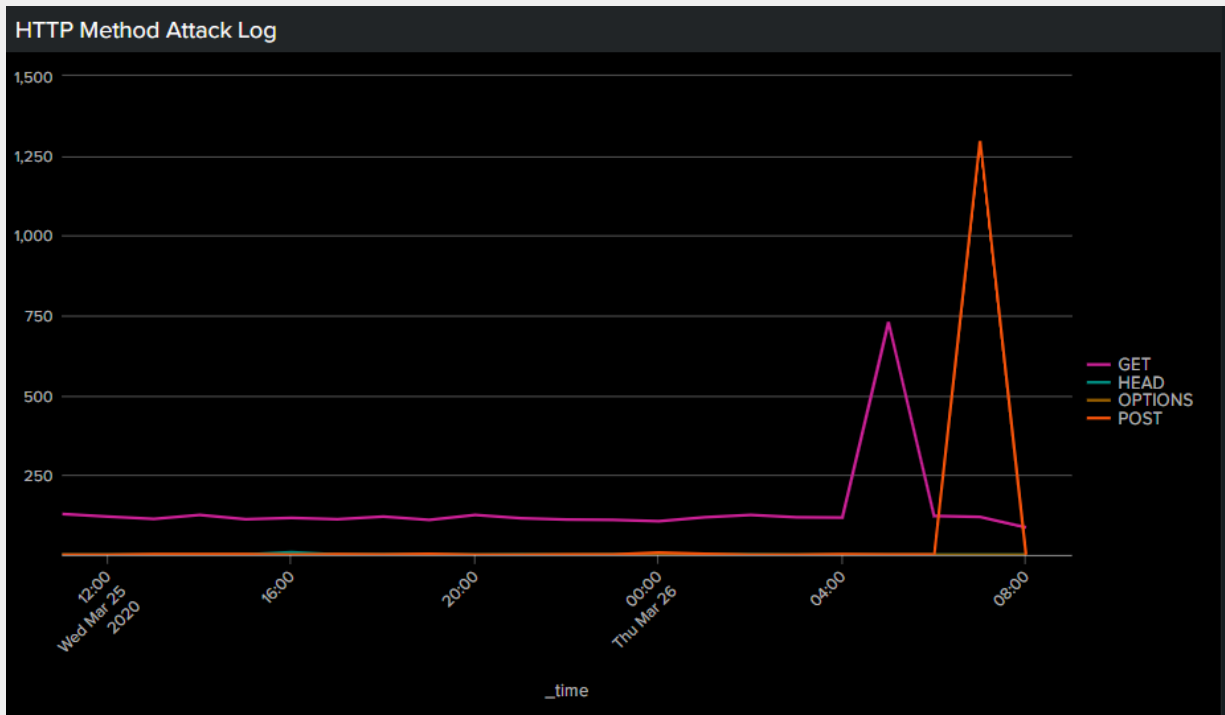
### **Dashboard Analysis for Time Chart of HTTP Methods**

- Does anything stand out as suspicious?



After the attack:





The dramatic increase in the HTTP Post method vs the amount on a regular business day

- Which method seems to be used in the attack?

By the time chart, it would appear that the HTTP method used in the attack is POST

- At what times did the attack start and stop?

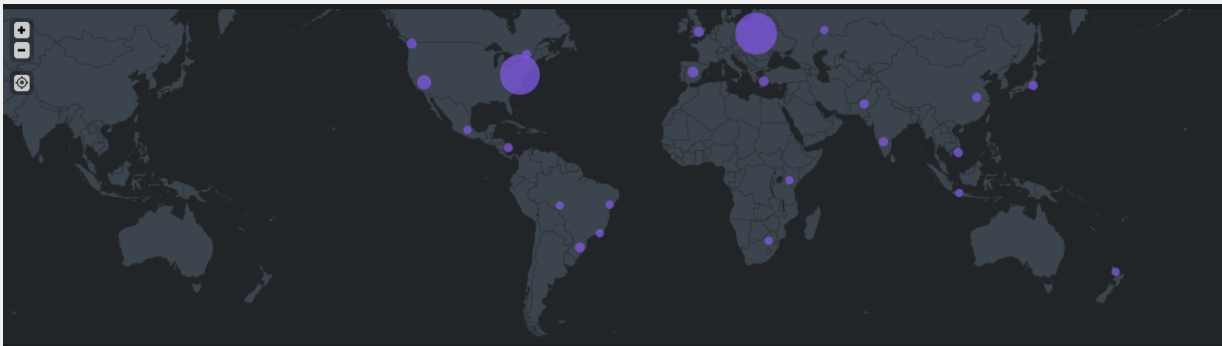
The attack started at 6:00 PM and ended at 8:00 PM

- What is the peak count of the top method during the attack?

The peak count of the attack was 1,296

## Dashboard Analysis for Cluster Map

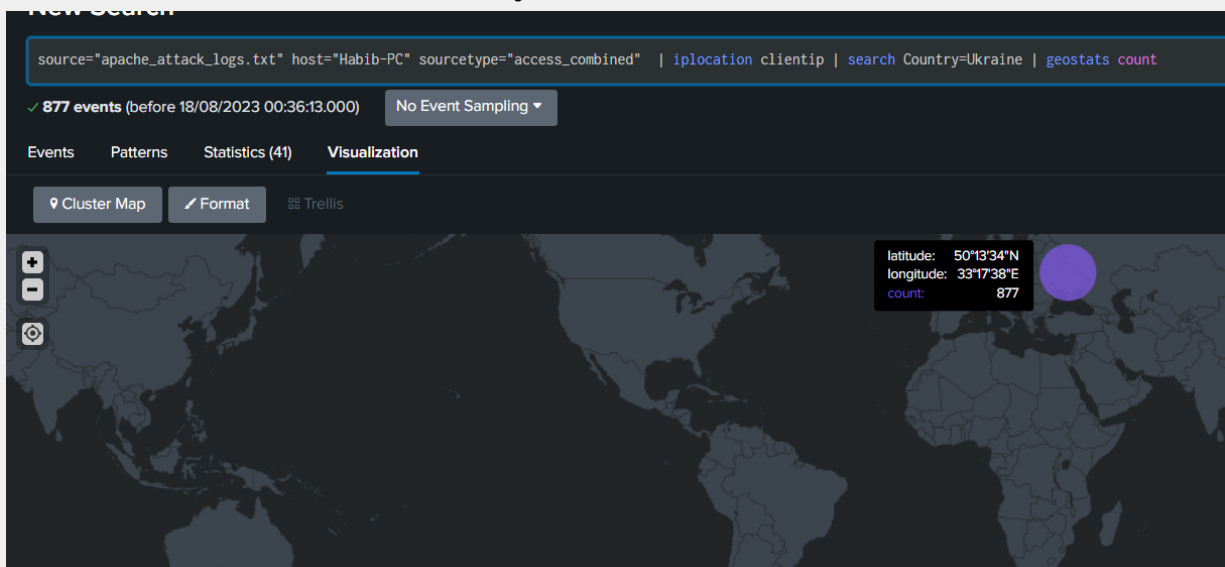
- Does anything stand out as suspicious?



A lot of activity came from Ukraine during the reported time of the attack.

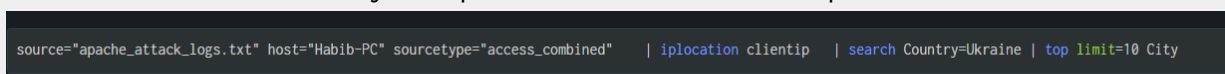
- Which new location (city, country) on the map has a high volume of activity?  
(Hint: Zoom in on the map.)

My select statement resulted from me that a total of 877 activities were carried out from the cities of Kyiv and Kharkiv of Ukraine.



- What is the count of that city?

The table below shows Kyiv equals 438 and Kharkiv equals 432.



| City                                | count | percent   |
|-------------------------------------|-------|-----------|
| Kyiv (Solom'yans'kyi district)      | 438   | 49.942987 |
| Kharkiv (Shevchenkivs'kyi District) | 432   | 49.258837 |
| Lviv                                | 3     | 0.342075  |
| Vinnitsia                           | 1     | 0.114025  |
| Solonka                             | 1     | 0.114025  |
| Kyiv (Shevchenkivs'kyi district)    | 1     | 0.114025  |
| Onipro                              | 1     | 0.114025  |

## Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, from the URI log, suspicious activities like an increase in the VSI\_Account\_logon page from 101 to 1323 during the attack, as shown below.

URI Count before the attack:

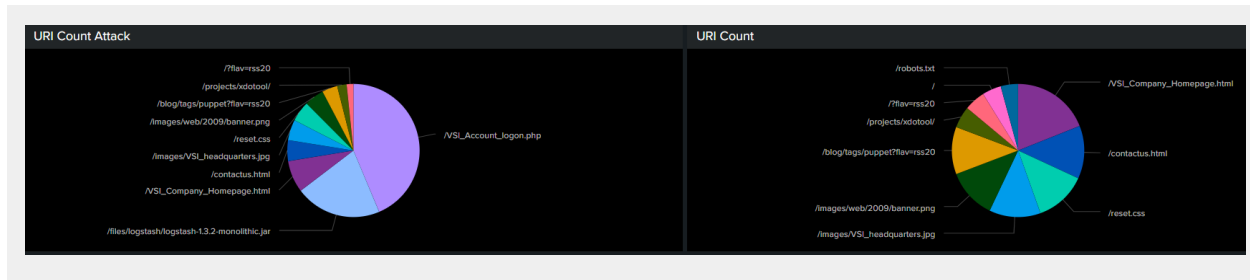
|   |     |          |
|---|-----|----------|
| /?flav=atom   | 137 | 1.370000 |
| /articles/dynamic-dns-with-dhcp/  | 135 | 1.350000 |
| /presentations/logstash-scale11x/images/ahhh____rage_face_by_samusmmx-d5g5zap.png | 128 | 1.280000 |
| /VSI_Account_logon.php  | 101 | 1.010000 |
| /blog/geekery/ssl-latency.html  | 77  | 0.770000 |
| /files/logstash/logstash-1.3.2-monolithic.jar                                     | 61  | 0.610000 |

URI Count after the attack:

| source="apache_attack_logs.txt" host="Habib-PC" sourcetype="access_combined" top limit=10 uri |       |           |
|---|-------|-----------|
| 4,497 events (before 18/08/2023 01:03:36.000) No Event Sampling                               |       |           |
| Events Patterns Statistics (10) Visualization   |       |           |
| 20 Per Page Format Preview  |       |           |
| uri   | count | percent   |
| /VSI_Account_logon.php  | 1323  | 29.419613 |
| /files/logstash/logstash-1.3.2-monolithic.jar   | 638   | 14.187236 |
| /VSI_Company_Homepage.html  | 235   | 5.225706  |
| /contactus.html   | 153   | 3.402268  |
| /images/VSI_headquarters.jpg  | 152   | 3.380831  |
| /reset.css  | 151   | 3.357794  |
| /images/web/2009/banner.png   | 145   | 3.224372  |
| /blog/tags/puppet?flav=rss20  | 114   | 2.535023  |
| /projects/xdotool/  | 70    | 1.556593  |
| /?flav=rss20  | 50    | 1.111852  |

- What URI is hit the most?

We can see that during the attack VSI\_Account\_logon.php page was hit the most.



- Based on the URI being accessed, what could the attacker potentially be doing?

From the log data, it is evident that the attacker made a deliberate effort to execute a brute-force attack or SQL injection against the VSI web server.