**UR-VIRT-RICH-CYBER-PT-062021-U-C**

**ELK Stack Project**

Josh Black

Laura Pratt

Courtney Templeton

**Kibana Exploration Activity**

To start, I added a sample data set. See below.

Graphical user interface, text, application

Description automatically generated

Next, I selected to view the data on my dashboard.

Graphical user interface, application, Word

Description automatically generated

The next step is to answer the following questions:

Answer the following questions:

* In the last 7 days, how many unique visitors were located in India?

Graphical user interface, chart, application

Description automatically generated

There were 246 unique visitors from India.

* In the last 24 hours, of the visitors from China, how many were using Mac OSX?

Graphical user interface, application

Description automatically generated

* In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

A picture containing graphical user interface

Description automatically generated

404 code= 6.098%

503 code= 1.22%

* In the last 7 days, what country produced the majority of the traffic on the website?

Graphical user interface, text

Description automatically generated

I was able to hide the other layers and just isolate the total requests per country and then based on the heat map, determined that China had the highest total number of requests producing the most traffic.

* Of the traffic that's coming from that country, what time of day had the highest amount of activity?

Chart, scatter chart

Description automatically generated

According to this heat map, the time of day was 1300 that had the highest amount of activity.

* List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).

Table

Description automatically generated

File types:

gz-compressed files created using the gzip compression utility

css-these files help define got, size, color, spacing, border and location of HTML information on a webpage. They are downloaded with their .html counterparts and rendered by the browser

deb-a file with the .deb file extension is a Debian (Linux) Software Package file. These files are installed when using the apt package manager.

Zip-a lossless compression format. A .zip file may contain one or more files or directories that have been compressed.

1. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.
   * Locate the time frame in the last 7 days with the most amount of bytes (activity).

Chart, scatter chart

Description automatically generated

* + In your own words, is there anything that seems potentially strange about this activity?

It appears that one particular user is using almost double the amount of bytes as multiple users at one time.

1. Filter the data by this event. Graphical user interface, application

   Description automatically generated
2. What is the timestamp for this event?Graphical user interface

   Description automatically generated with medium confidenceGraphical user interface

   Description automatically generated with medium confidence
3. What kind of file was downloaded?Graphical user interface, text, application, website

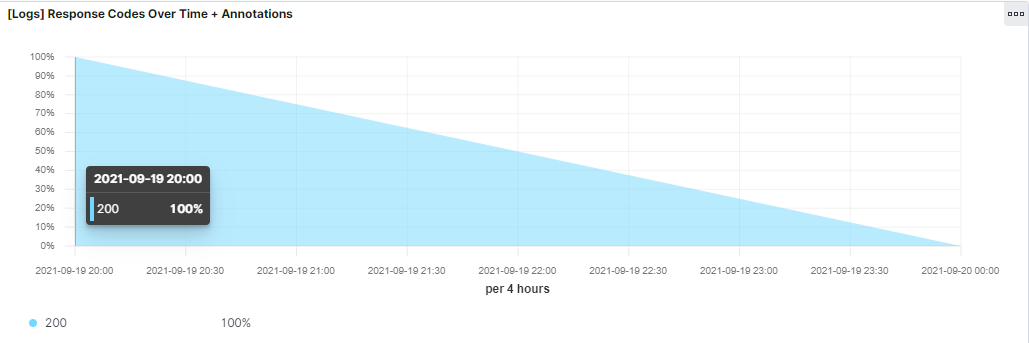
   Description automatically generated
   * From what country did this activity originate?

Graphical user interface, application

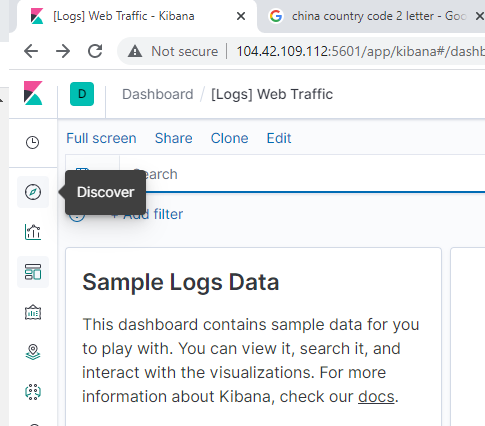
Description automatically generated

* + What HTTP response codes were encountered by this visitor?

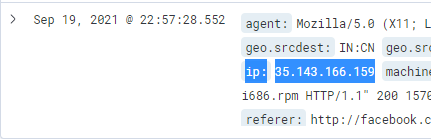
The response code was 200.



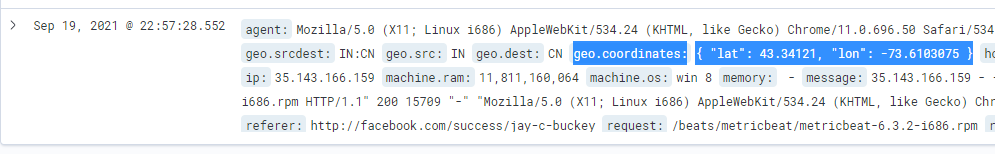
1. Switch to the Kibana Discover page to see more details about this activity.



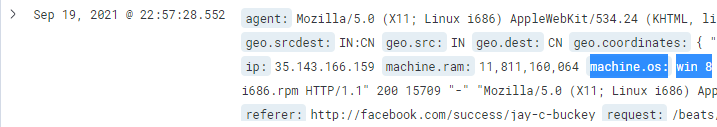
* + What is the source IP address of this activity?



* + What are the geo coordinates of this activity?



* + What OS was the source machine running?



* + What is the full URL that was accessed?



* + From what website did the visitor's traffic originate?



1. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing?

It looks like the user is trying to get the metricbeat package via Facebook.

* + Was the file they downloaded malicious? If not, what is the file used for?

It does not appear malicious based on the data provided. It just appears that they were trying to get the program for data collection through Facebook.

* + Is there anything that seems suspicious about this activity?

It is somewhat suspicious just because of the user trying to navigate data collection via Facebook.

* + Is any of the traffic you inspected potentially outside of compliance guidelines?

Not with the packet information that I saw.