Activity File: Exploring Kibana

From My "Sample Logs Data"

Answer the following questions:

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

225

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

12

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

404 Errors: 28

503 Errors: 20

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

China

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

10:00 AM

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).

css – Cascading Style Sheet. Files that contain the .css file extension are used to format the contents of an associated Web page.

deb – Files that contain the .deb file extension are Unix archive files. These files are most commonly used for installation packages that contain software developed for computers that run on the Linux OS using the Debian package management application.

gz – Files that contain the .gz file extension are called GNU zipped archive files. These are GZipped data files that are compressed by the GNU zip (gzip) compression algorithm.

rpm – RedHat Package Manager. Files that contain the .rpm file extension and are files used for the installation of software developed for computers that run on a RedHat-based Linux OS.

zip – Files that contain the .zip file extension are called Zip files. These are files that use lossless data compression to archive one or more files or directories with a number of compression algorithms, with DEFLATE being the most common.

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).

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

The majority of the avg. bytes used (15,709) was done by one unique visitor at one specific time (21:57:25) with a Windows 8 OS in order to download a .rpm file.

Filter the data by this event.

What is the timestamp for this event?

21:57:25

What kind of file was downloaded?

.rpm

From what country did this activity originate?

India

What HTTP response codes were encountered by this visitor?

HTTP status code 200 “OK”

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

What is the source IP address of this activity?

35.143.166.159

What are the geo coordinates of this activity?

{ "lat": 43.34121, "lon": -73.6103075 }

What OS was the source machine running?

win 8 (Windows 8)

What is the full URL that was accessed?

https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm

From what website did the visitor's traffic originate?

http://facebook.com/success/jay-c-buckey

Finish your investigation with a short overview of your insights.

What do you think the user was doing?

The user originally was using Facebook and clicked on a link used to download Metricbeat for a RedHat-based Linux machine.

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

The downloaded file (/beats/metricbeat/metricbeat-6.3.2-i686.rpm) is not malicious and is used to download and install the Metricbeat software.

Is there anything that seems suspicious about this activity?

Personally, I feel that Facebook probably isn't the best source to download software; however, there really isn't anything suspicious other than the poor decision making.

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

No, of the traffic that I inspected, everything was within the compliance guidelines.