**Read-Me File (for all key pages)**

**Tiversa Dashboard:**

Warning list: only the first “Investigate” button is clickable. Others investigation page can be developed as the first one.

Live Stream: When mouse hover, it will pause. No any clickable function, but it can be developed if needed.

**Investigation Page: (tiversa\_handle\_page.html)**

Hover over the map, file count will appear. The data is read through the map’s JS file.

The line graph provides three options, which are the three top file count states. The data is read through the JS file, which is used to generate the graph.

Both the map and graph are shown on a weekly basis.

**Search Result page: (infection\_result.html)**

Infection IP list is displayed based on the input date and other criterias through the search panel. “Detail” will show all the files that are downloaded from this IP address.

The pie chart is showing the top 6 infection type based on the search criteria.

The infection list next to the pie chart displays the file count for each infection type.

“Search All File” button is to perform the search based on any of the infection type being checked in the Infection List, it will return the list of file based on the infection type chosen.

**Preventative Page:**

The first panel shows comparison of 3 cities with the top 5 infections and their average in the line graph.

The second panel contains 2 3D-Donut graphs. First 3D Donut graph shows the top user agents and the total infected files they distribute. Second 3D-Donut graph shows the top ports and the total infected files they distribute.

**Timeline Page:**

The timeline page shows a line graph of the timeline of the selected IP Block. The x-axis denotes the date on which the infected files were uploaded/downloaded within that IP Block. The y-axis denotes the total count of infected files being uploaded/downloaded on the corresponding date.

Upon clicking any point in the graph, a table will appear below, showing the details of the file activity recorded.

**Product 1 (Infected IP List) Page:**

The Product 1 Page is the infected IP list page, which gives the list of all IPs which are uploading/downloading the malware infected files within the IP Block of the company. Upon clicking the “Detail” link, further details for that corresponding IP are shown (File-name, port, infection type, user agent).

**Client Dashboard:**

The first panel of the client dashboard depicts a geographic density map of malware. The darker the state, the more the count of infections. The second panel shows file count in the form a line graph. You can choose between states and the graph will adapt as needed. The next three panels are all different visualizations of file type, user agents, and infections. Each of these graphs are clickable and customizable. The live stream can be paused when hovered over.

**Tiversa Malware Map:**

This map depicts the global distribution of malware from our database. The darker the country, the more malware. Map is zoomable and can be made to be responsive.

**Infected File List Page:**

This page will show when search all files by one infection type from the search result page. This page will display all sha1 of some specific infection type(s) in one client’s one state IP block.

The list’s columns include SHA1, number of files of this SHA1, detail button and a checkbox for selecting for generate offending IP list. Through this page, analyst can select all SHA1 to generate the offending IP list for further investigate.

The detail button can show the details of this specific SHA1. Details include the filename, infection type, port and user agent.

**Offending IP List Page:**

This page will show after clicking the generate offending ip list button. Offending IP list includes the IP, Location, Number of Infected File, Number of SHA1, Number of Distinct FileName and detail button. When clicking the detail button, the behavior of this specific IP will be shown.

**Behavior of IP Page:**

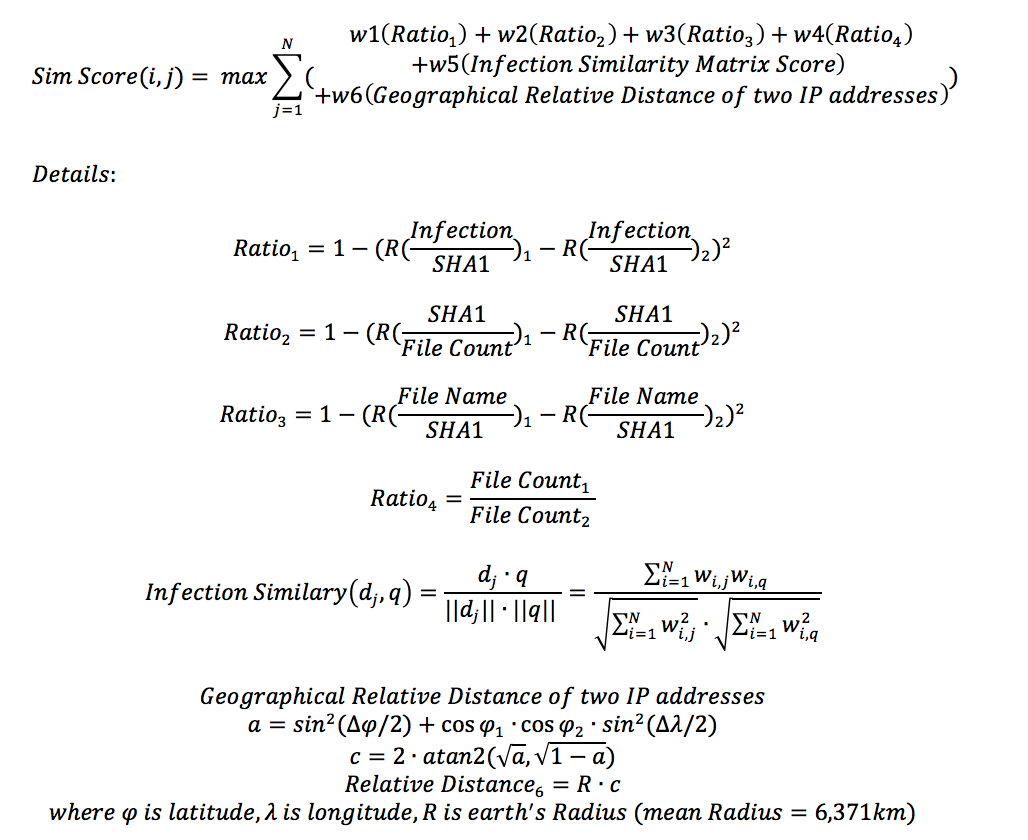
The first part of this page is a line graph and three ratio bars. The line graph show the activity of this IP during one year period and there are four lines in it. They are count, SHA1, filenames and infection types. And three ratio bars are the ratio of SHA1 and file count, the ratio of infection and SHA1, the ratio of SHA1 and filenames.

Another part is the location of this IP, including Country, State, City, Longitude and Latitude.

Through this page, analyst can find other IP with similar behaviors.

**Find Similar**

In this page, our goal is to let the analysis to find similar IPs based on our algorithm.



So by using this formula, we can clearly see that we take 6 factors into consideration:

1. Infection over SHA1: in this ratio, we are intent to measure the variation of SHA1, so in this case we will know that

**Landing Page**

Landing page shows different types of malware spread globally. This page shows 3 types of offenders. There are 15 patterns for each type of offenders which is shown in the landing page in random fashion. This page can be plugged in with the database and show real time data as necessary.

This page consists of the following files,

1. LandingPageDemo.html
2. LandingPageDemo.js
3. LandingPageDemo.css
4. LocalTime.js

Left bottom table shows the information of high volume offenders. It is synced with the animation in the map.

The table in the bottom mid section of the map shows a list of offenders of all three types.

Both the tables can be plugged in with database through a webservice or API call to show live feed.

\*Only “LandingPageDemo” files are fully functional. Other landing page files are for test purposes.

**Tiversa Malware Analysis**

This pages shows statistical information about number of files with certain File Type, infected by certain infection as well as type of user agent. The first pie chart shows Top 5 file type counts both in absolute number and in percentage. By clicking on the switch to funnel button, another type of visualization is shown. Each individual component of the graph is removable for clearer comparison. The second pie chart uses similar design but shows top 5 infection type among all data.

The bar chart on the bottom shows top 10 user agent and corresponding file count. By click on the "Sort values" check box, data will be sorted according to the file count in descending order.