Requirements to use:

* People who are familiar with producing json files similar to ours. Of paramount importance.
* The above is satisfied mostly by system administrators of various labs around the world.

Helping System Administrators:

* Spot Anomalies using anomaly sliders
* Observe worldwide trends using linechart and table
* Give users control through anomaly sliders – User oriented, dynamic as a consequence
* Limit down things seen on the screen via non-anomaly sliders
* Textboxes work in conjunction with sliders and sliders are there visually, for the most part. Visual learning.
* Drilling down principle – Schneiderman’s mantra
* A tool that can be used as a means to an end, the end being defined by the user. For us, the end is to visually capture ssh attacks over a period of 9 weeks(temporal structure can be changed, for instance, 9 minutes). Not a solid reason at to why this should be 9 weeks but that can be given up to the user too. As of right now, 9 weeks is a good balance as far as, there is space on the browser to show it, alongside other stuff.

Things we have learned:

* Percentage changes allow us to see countries that may fly under the radar. It can be argued that once a threshold is hit(whatever this threshold is), a country/area/ASN might have malicious intent, in that, they might have botnets, bad actors etc. Sri Lanka, Saudi Arabia, Nicaragua etc.
* Absolute changes allow us to see countries that have had massive changes, not necessarily percentage wise. US, China, Russia etc.
* Percentage change ensures that this is not a population contest. Without percentage change, we would never be able to see countries like Sri Lanka and Saudi Arabia.
* In a way, these 2 methods are complimentary, in that, it allows us to see both unfamiliar and familiar countries. Familiar being defined as countries we expect to see, like China and the US, by virtue of population, politics, technological advancements, a mixture of some, a mixture of all and so on.
* Drilling down helps us see attackers. If 8 attackers had 20 attacks in time period 1 and 5 attackers had 950K attacks in time period 2, there is cause for concern. How did this happen and How to deal with it are the questions that can be asked.

Todo:

* Final Visualization that breaks down attacker info, sheds lights on dictionary groups, spot anomalies again
* Make fonts bigger where it needs to be
* Tooltip for bar graph rectangles?
* Can 2nd viz be improved from what it is currently?
* Formulating reasonable defaults.
* Write an abstract
* Colors for below 0 and at 0.