The Routing Table Tool Suite (RT-Tools)

MAPPING THE INTERNET ONE ROUTE AT A TIME OR ALL ROUTES AT ONE TIME

Base Capabilities
The RT-Tools suite displays Autonomous Systems (AS) Network traffic based upon the path analysis of aggregate routing tables. The routing tables are built from data acquired from open source resources located at Oregon University and RIPE. The analysis tools provide a method to make a group of complex relationships more manageable.

- Geopolitical Affiliation and Stability
- Business Relationships
- Asset Valuation
- Resource Dependence
- Proxy or Filtering Chokepoints

Differentiators
- Analysis comes from tracking data points over time
- Can be configured to view data comparisons
- Allows for pivoting against different data sources to enrich understanding
- Analyzes several routing tables sources concurrently
- Work product shows enriched aggregate consensus

Geo RTViz Map

RT-Tools can provide insights into organization characteristics such as method to make a group of complex relationships more manageable.

• Resource Dependence

RT-Tools Visualization

North Korean Internet Outages in March 2013
Recently North Korea (Democratic People’s Republic of Korea) has been in the news for a variety of reasons. There was a recent spread rumor that North Korea had launched an offer to host the BitTorrent site “The Pirate Bay”. There are also numerous legitimate news outlets publishing stories that include North Korea in attributing issues with Internet connectivity to acts of aggression from other the United States or South Korea (Alliance of Korea).

Contrary to these reports, public routing data is standing up an entirely different story. AS322 is routing all North Korean IP addresses through two routes, AS4837 (across terrestrial routing via China, and AS12389) provide an alternative path through Iran. AS322 hosts only 1254 IP addresses and all are connected to AS4837, which are also connected to an Internet backbone. On March 3, 2012, AS322 started advertising AS4837. “The Pirate Bay”, AS322, and its address space through AS12389. “The Pirate Bay”. There is very little traffic into and out of the traffic is stable.

These facts indicate an alternate explanation to the North Korean accusations. The sudden uptick of traffic to the Pirate Bay and the North Korean infrastructure is not a sign of interest in the site. Additionally, a large number of well-connected Internet users happen to route it in both the United States and South Korea. However, this traffic increase should not be attributed to the United States or South Korean governments. It is more likely a well-intentioned effort of routing the Pirate Bay.

Iran Internet Routing Changes January 2012
An investigation of the global BGP routing tables presents a country of interest, in this case Iran, as being a very complex nexus of events. By removing the ASNs that are not directly interconnecting the Internet or providing alternate access the table we get an interesting view of information.

This investigation from January 7, 2012, of the external peers showing that two major routing chaslepoints exist in Iran. AS12880 provides high-speed Internet access for over four million IP addresses, while AS9241 hosts many other country’s need to connect out to connect through AS12880 and AS9241. Many networks connect through both AS’s. The Open Net Initiative reports that direct content management in external traffic, and then indirectly show the Internet that running traffic a packet through AS12880, but content management through AS9241 is unknown. The Islamic Republic of Iran Broadcasting (IRIB) has a routing decision to provide content which depends both of those chaslepoints. By looking at the routing table snapshot for a single time period and charting which ASN are dependent on ASNs for Internet access and which organizations leverage this visibility to ensure resilient network access. Some resources are important and require alternate paths for access in case one of the service disruptions.

Iran Internet Routing Changes February 2012
The visualization from February 1, 2012, is missing AS42586; it did not disappear from Iran’s communication infrastructure, but it did enter its directly connected route to the outside world. Problems occurred in the absence of the country of interest from external service providers AS42586 and AS8672.

A significant change in Iran January 7, 2012, shows the February 1, 2012 visualization AS42586, becomes visible and directly connected to the Internet, without visibly using external service providers. Other observed ASNs that highlight interesting behavior are those that appear to be Tier 2 service providers, like AS9121, or are highly connected to previously mentioned AS42586 or AS4259. Some of these ASNs are now more directly connected to the AS12880. The newly visible ASNs are not connecting through a new external service provider; they were previously routed through the route to the Internet through AS4257. What is changed is that they now have route that bypasses Internet transit hosts and become visible in the visualization.

Iran Internet Routing Changes March 2012
The routing visualization from March 1, 2012, shows considerably more activity with regards to the directly connected route to the outside world. AS12880 in connected in its natural state of how we now see AS42586. AS42586 is providing necessary ASNs to connect to the Internet. However, AS12389, AS1239, AS4257, AS4577, AS4837, and AS42586. The association that AS12880 provides Internet routing towards a group any connection that routes around the chokepoint is potentially significant.

Data Fusion
RT-Tools integrate data from various sources so that the final product is greater than the sum of its parts. The tools combine information from routing tables with resources that provide entity identification and attribution. This approach establishes a framework that makes patterns more available to analysts.

Future Plans
We are designing RT-Tools to allow external data sources to add greater context. The resulting RTViz map can provide dynamic access to additional data sources to promote real-time analysis that can track historical changes in a single unified interface.

http://www.cert.org/flocon

CERT/CC-2013-72
©2013 Carnegie Mellon University