Anomaly Detection on DNS Auths

Root DNS, ccTLDs and DNS providers

Team ~~Schabeltier~~Anomalizers

RIPE DNS Hackaton 2017
Amsterdam, The Netherlands
2017-04-21

Team Members (alphabetically)

- Christian Doerr (TU Delft)
- Ella Titova (VivaCell)
- Giovane Moura (SIDN Labs)
- Jan Harm Kuipers (University of Twente/SIDN Labs)
- Moritz Müller (SIDN Labs/University of Twente)
- Ricardo Schmidt (University of Twente)
- Wouter de Vries (University of Twente)

Resources

- GitHub: https://github.com/orgs/ripe-dns-anomaly/
- Demo: https://ripe-dns-anomaly.github.io

Main Problem

Auth DNS Anomaly Detection

- *How can we use Ripe Atlas data to detect automatically failures on Auth DNS (Roots, ccTLDs, etc...)?*

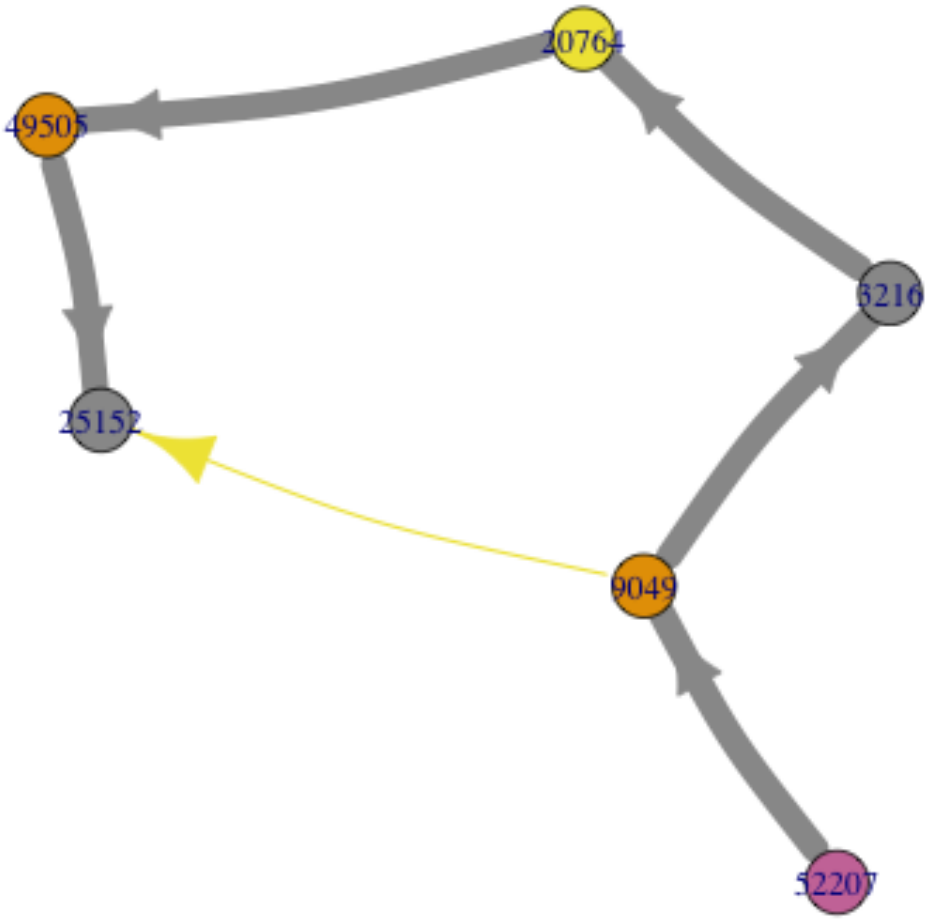
Step-by-step - CHAOS/RTT

1. Download Ripe datasets and parse them
   - https://github.com/ripe-dns-anomaly/chaos
   - `parse-json.sh $startTime $endTime bins $mid`
   - start and end = timestamps
   - bins= 600 (10minutes)
   - mid = Ripe measurement ID
2. Then, run anomaly detection per letter and site:
   - https://github.com/ripe-dns-anomaly/anomalyDetector
   - `python letter-level-detector.py data/k-root-ddos-20151130.csv output/k-root-ddos-20151130-ad-hoc.csv`
3. Then, it outputs anomalies per class type:
   - https://github.com/ripe-dns-anomaly/anomalyDetector/blob/master/README.md

Step-by-step - Path

1. Download Ripe datasets and parse them
   - https://github.com/ripe-dns-anomaly/traceroute
   - `python traceget.py --start $startTime --end $endTime --msmid $msmid`
   - start and end = timestamps
   - msmid = atlas measurement id (5001 for K-root)
2. Then, convert the format:
   - https://github.com/ripe-dns-anomaly/traceroute
   - `java -jar`
3. Last step: convert to webformat

AS Graph - Path change during Nov 30 2015 Root DNS Attack



Algorithms for Anomaly Detection

- See discussion on https://github.com/ripe-dns-anomaly/anomalyDetector/blob/master/README.md
- Twitter's robust TS analysis, ARIMA, ad-hoc
- We choose ad-hoc (ours)
- Data is not periodical
- We need more time to evaluate the best one
- Less false positives

Demo

https://ripe-dns-anomaly.github.io

Ready to be used by others

- Use by ccTLDs, Roots, etc.
- Requirement: Ripe Atlas measurements with **chaos.id** support and traceroute measurements
- Next: automate it to continuously probe it, detect and notify