D4 Project

IPASN History and BGPRanking

Team CIRCL
https://www.d4-project.org/

20190328

Raphaël Vinot

IPASN History - Problem statement

- Rapidely figuring out the owner of a specific IP address is a common problem
- Resolving that relationship for a massive amount of IP addresses at scale is a medium hard problem
- Doing so for a specific day in the past is somewhat more difficult
- Comparing the resolution across sources is pretty painful
- Doing all that together is pretty much a pain

IPASN History - Objective

- Fast, scalable, flexible framework to load multiple data sources of BGP announcements
- Flexible configuration of the size of the history to keep in memory
- Fire and forget model
- Simple REST API
- Even simpler Python client and API

IPASN History - (short) History

- D4 Project (co-funded under INEA CEF EU program) started - 1st November 2018
- A PoC of IPASN History was initially developped in 2012-2013 and only supported IPv4
- Was used in production for BGP Ranking over many years
- The current version was released initially in November 2018 after a complete rewrite
- The support of multiple data source was added in March 2019

IPASN History - Current status

- Supports Caida and RIPE as data sources
- Supports requests for IPv4 and IPv6
- Python3 module
- Simple REST API
- Used in production in the new version of BGP Ranking

BGP Ranking - Problem statement

- There are 10th of thousands of actors on the internet owning IP Addresses
- Many of them own a very small amount of IP addresses (/24)
- They change nem, purposes and owner relatively often
- Their security practicies are poor, if they ever exist
- They are plain malicious and have no legitimate purpose
- One way to find these malicious providers is to map them to lists of known malicious IPs

BGP Ranking - Objective

- Daily ranking of internet profiders by maliciousness
- History of said rankings over a long period of time
- Fire and forget model
- Simple REST API
- Even simpler Python client and API

BGP Ranking - (short) History

- D4 Project (co-funded under INEA CEF EU program) started - 1st November 2018
- A PoC of BGP Ranking was initially developped in the early 2010s and only supported IPv4
- The current version was released initially in November 2018 after a complete rewrite
- The integration with IPASN HIstory was finalized in February 2019

IPASN History - Current status

- The public instance automatically loads a couple dozen of publicly available lists of known malicious IPs
- Supports the ShadowServer data (requires an account from Shadow Server)
- Supports IPv4 and IPv6 lists
- Python3 module
- Simple REST API

IPASN History & BGP Ranking

- IPASN History source code:
  `https://github.com/D4-project/IPASN-History`
- IPASN History Query interface over BGP Ranking:
  `https://bgpranking-ng.circl.lu/ipasn`
- BGP Ranking source code:
  `https://github.com/D4-project/BGP-Ranking`
- BGP Ranking interface:
  `https://bgpranking-ng.circl.lu/`

Get in touch if you want to join the project, host a sensor or contribute

- Collaboration can include research partnership, sharing of collected streams or improving the software.
- Contact: info@circl.lu
- `https://github.com/D4-Project` - `https://twitter.com/d4_project`