BGP Ranking & IP-ASN History
Making Something Useful Out of Old Massive Datasets

CIRCL
Computer Incident Response Center Luxembourg

Raphaël Vinot
raphael.vinot@circl.lu
info@circl.lu
FIRST 20190617
about CIRCL

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.
Objectives of the presentation
Our objectives of the presentation

- Why do we need tools like BGP Ranking and IPASN History
- How to effectively aggregate big datasets of malicious IPs
- Show the integration of IP ASN History and BGP Ranking
- Explain how to use the respective APIs
- Discuss the future developments
IP ASN history

- Owners of IP prefixes evolve in time
- Investigations can happen late
- BGP views may vary depending on source
- RIPE has a very comprehensive interface, but doesn’t scale for thousand IPs
BGP Ranking

- Many vendors propose lists of malicious IP addresses
- Malicious IP addresses evolve in time
- Many small providers are owned by malicious actors
- No simple way to track them over months/years
IP ASN History
Data Sources and format

- BGP Routing tables: IP Prefix $\rightarrow$ AS number
- Currently supported sources: CAIDA and Ripe (RRC01)
- Future: CIRCL
Implementation

• Load one BGP routing table per day per source
• Lookup services using patricia trees loaded in memory
• Automatic update daily
• Automatic cleanup of old dataset (default: > 180 days)
• Accessible as a web service
Features

• Fast Lookup
• Find daily ownership for an IP
• Multiple IPs lookup at once
• Import your own BGP routing table
• Run the tool in-house
Data sources

- Public lists containing IP addresses (Abuse.ch, Dshield, Bambenek Consulting, blocklist.de, ...)
- Shadowserver (fetches the list from the web interface, requires an account)
- Future: MISP instances, DNS lookup, other private sources(?)
Implementation

- Hourly fetch of data sources, aggregation by day
- Prefix and ASN lookup against IP ASN History
- Computation every 8 hours (ASN and prefix in AS)

\[
\frac{\sum (IP \text{ Address} \times source \text{ weight})}{\sum IP \text{ announced by AS}} \tag{1}
\]

\[
\frac{\sum (IP \text{ Address} \times source \text{ weight})}{\sum IP \text{ in prefix}} \tag{2}
\]
Features

- Follow the evolution of an AS over time
- Discover suspicious IPs in the neighbourhood
- Ranking by country
- Run the tool in-house, on your own feeds
Current use-case: D4 Project
Problem statement

- CSIRTs (or private organisations) build their **own honeypot, honeynet or blackhole monitoring network**
- Designing, managing and operating such infrastructure is a tedious and resource intensive task
- **Automatic sharing** between monitoring networks from different organisations is missing
- Sensors and processing are often seen as blackbox or difficult to audit
Objective

• Based on our experience with MISP\(^1\) where sharing played an important role, we transpose the model in D4 project
• Keeping the protocol and code base \textit{simple and minimal}
• Allowing every organisation to \textit{control and audit their own sensor network}
• Extending D4 or \textit{encapsulating legacy monitoring protocols} must be as simple as possible
• Ensuring that the sensor server has \textit{no control on the sensor} (unidirectional streaming)
• Don’t force users to use dedicated sensors and allow \textit{flexibility of sensor support} (software, hardware, virtual)

\(^1\)https://github.com/MISP/MISP
Integration

- Use data from D4 as a source
- Lookup DDoS data against BGP-Ranking
- Correlate DDoS datasets with other type of malicious activities
APIs
IP ASN History

- curl https://bgpranking-ng.circl.lu/ipasn_history/?ip=8.8.8.8
- With Python client: ipasn.py -ip 8.8.8.8
BGP Ranking

- With Python client: `bgpranking --asn 5577`
References

- https://bgpranking-ng.circl.lu/
- https://www.d4-project.org/
- https://github.com/D4-project/IPASN-History
- https://github.com/D4-project/BGP-Ranking/