

BGP Ranking

Security Ranking of Internet Service Providers



CIRCL
Computer Incident
Response Center
Luxembourg

SECURITY MADE IN LETZEBUERG

Alexandre Dulaunoy

February 1, 2011

Agenda

- Challenge in dataset collection and analysis
- Ranking Internet Service Provider
- Design and implementation
- Future

Data Source and Dataset

- A large variety of private/public datasets including IP, prefixes or ASN for suspicious activities.
- Level of trust is variable. (e.g. dshield dataset vs Arbor ATLAS/Active Threat Feed)
- Scope and detection techniques can vary a lot. (e.g. Black-hole monitoring vs URL extracted from malware)
- Even "whois" can be sometimes considered as a dataset when a malicious ISP controls some objects. (e.g. route-object updated by Botnet operator)

Challenges In Analysis

- Datasets are very large, formats are unstable and incompatible.
- Datasets are evolving over time. (e.g. 24 hours step is usual)
- Datasets trust might change over time.
- Dataset creation is often unclear. (e.g. not uncommon to see "similar" dataset)
- For classification, the least common denominator is often used. (e.g. CIDR block or ASN)
- → Analysis and ranking depend on all those factors.

Why Ranking ISPs?

- CSIRTs can assess the level of trust per ISPs. (e.g. know to host drive-by-download website, reactive to abuse handling, ...)
- Improve assessment between ISPs. (e.g. IP peering policies)
- Detecting common suspicious activities among ISPs/ASN.
- Can be used as an additional weight factor to abuse handling.

AS Ranking Implementation

- Implementation released as free software/open source. (e.g. run your own private ranking)
- Ranking of AS or Subnet must be fast enough
 - allowing continuous ranking processing,
 - adding or discarding data sources
 - and giving fast lookup at the same time.
- Key/value store to allow "mapreduce-like" processing.
- Implementation written in Python and latest version uses Redis as a key-value store.
- BGP Ranking supports IPv4 and IPv6.

Data Source Model

- Each data source is a tuple $s(\text{sourceid}, \text{impact})$.
- Impact is defining the weight of a datasource.

Current datasource (config file)

```
; classname = impact
DshieldDaily = 1
DshieldTopIPs = 2
;Abusix = 2
ZeustrackerDdos = 5
ZeustrackerIpBlockList = 5
SpyeyetrackerDdos = 5
SpyeyetrackerIpBlockList = 5
SshblBase = 5
;ShadowserverSinkhole = 10
;ShadowserverReport = 10
;ShadowserverReport2 = 10
;Atlas = 20
```

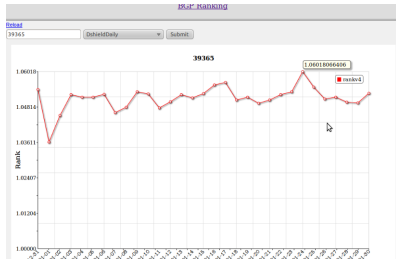
AS Ranking Calculation

Formula

$$AS_{rank} = 1 + \left(\frac{AS_{vote} \left(\sum_{s=1}^{\#s} (Occ \cdot S_{impact}) \right)}{AS_{size}} \right)$$

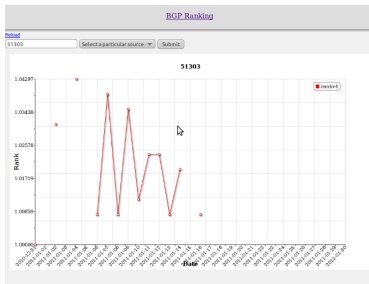
- Number of malicious occurrence per unique IP (Occ).
- Grand total of IP addresses announced by the ASN (AS_size).
- Sum of vote for the ASN (AS_vote).
- Each iteration of the Occ sum is saved. (e.g. to discard a source from ranking calculation)

BGP Ranking Interfaces 1/2



- BGP Ranking accessible via a simple HTTP interface.
- User can select a specific ASN to get its ranking.
- Ranking can be dynamically calculated from a specific datasource.
- Web interface is directly accessing the Redis back-end.

BGP Ranking Interfaces 2/2



← Recently shutdown ASN in Russia.

- Top ASN per source list or globally.
- Additional DNS interface to query BGP ranking.

Conclusion - Next Steps - Q and A

- Shared impact values per data source. (→ ranking of datasets)
- Extending BGP ranking to a collaborative ranking scheme for CSIRTs. (public/private ranking)
- Integrating BGP feed to monitor stability of ISPs in addition to security ranking.
- XMPP query interface for integration with AbuseHelper.
- Source code and git repository:
<https://github.com/CIRCL/bgp-ranking>

hack.lu 2011



Call For Paper: 1st March 2011. Just before TF-CSIRT 22-23 September in Luxembourg too.