Fast and Scalable Ranking Scheme for Internet Resources - Current Usage and What’s the Future?

How to Track Suspicious Resources on Internet without Losing your Mind

Alexandre Dulaunoy

September 22, 2011
Agenda

• BGP Ranking - what’s new after TF-CSIRT Symposium in Barcelona?
• New API(s) in BGP Ranking
• The use of ranking in incident response and analysis
• Passive DNS and BGP Ranking integration
• Conclusion
Internet Resources and Security?

an IP address has the DNS properties MX, A, CNAME, and NS announced by an ASN peering with stability has been tracked by Zeus Tracker, dshield.org, AMADa Blocklist, and has been reported to Abuse Helper, CSIRT RTIR, Abuse Helper, and CSIRT RTIR. 

has the DNS properties MX, A, CNAME, and NS announced by an ASN peering with stability has been reported to Abuse Helper, CSIRT RTIR, Abuse Helper, and CSIRT RTIR. 

fast-flux: double-flux

fast-flux: single-flux

3 of 15
BGP Ranking - Security Ranking of ASN

an IP address has the DNS properties MX A CNAME NS announced by an ASN peering with stability has been tracked by Zeus Tracker AMaDa Blocklist dshield.org has been reported to Abuse Helper CSIRT RTIR

BGP Ranking

stability

announced by an ASN

peering with

has the DNS properties
BGP Ranking Implementation and Current Users

- Main public version available at http://bgpranking.circl.lu/
- Stable version source code available at https://github.com/CIRCL/bgp-ranking
- Two private installations known (beside CIRCL)
- Peak of 200 queries per second on the BGP Ranking public whois interface
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) → private interface
- Each iteration of the Occ sum is saved (e.g. to discard a blacklist from the ranking calculation)
API - whois Interface

Query the whois interface

```
whois -h pdns.circl.lu 42741
# ASN, Rank, Matched BL, Highest Malicious Ranking, ...
42741,1.01953125,4/17,1.2625,2/60541
```

- ASN
- Ranking (float)
- # of blacklist matched versus the total blacklist
- Best malicious ranking (float)
- Current malicious position (top is most malicious)
- (current vote) only for the private CSIRT API
API - JSON Interface

GET http://bgpranking.circl.lu/json?date=;source=;asn=42741;ip_details=2011-03-28T05:47:09.530829

API - XMPP Interface

Add bgpranking@p.smile.public.lu in your friend list...

help
(10:40:09 PM) bgpranking@p.smile.public.lu: BGP Ranking is the XMPP interface of the CIRCL BGP Ranking http://bgpranking.circl.lu/

query is: asn followed by ASN number to get the ranking
ip followed by an IP address to return ASN ranking

ip 8.8.8.8
(10:42:05 PM) bgpranking@p.smile.public.lu: # ASN, Rank, Matched BL, Highest Malicious Ranking, Current Position 15169,1.00287958483351,5/17,1.140625,775/63443

Integrated and used in AbuseHelper by CERT.be.
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 (e.g. detect outliers in large set of IP addresses)
A daily use: ease your log analysis

• 300 million lines of proxy logs? You have 30 minutes to find out what’s happened?
• Prefix the ranking AS15169,1.00273578519859,74.125.... to the log file
• logs-ranking → sort -r -g -t”,” -k2 proxy.log-ranked
• https://github.com/adulau/logs-ranking
A daily use: ease your memory dump analysis

- During a large incident, we got many memory dumps in a single day
- Dumping all the memory per process and we extracted all URLs and IPs from each memory dump
- Ranking URLs and IPs, and analyzing the processes with the higher malicious rank
- Ranking can be used for a lot of reverse analysis techniques
PDNS - Monitoring and Ranking DNS records

an IP address has the DNS properties
MX
A
CNAME
NS
announced by an ASN peering with
stability has been tracked by
Zeus Tracker
AMaDa Blocklist
dshield.org has been reported to
Abuse Helper
CSIRT RTIR
BGP Ranking
PDNS
has the DNS properties
announced by an ASN
peer with
stability

Abuse Helper
CSIRT RTIR

has been reported to

dshield.org has been reported to

AMaDa Blocklist
Zeus Tracker

has been tracked by

BGP Ranking

45 of 15

13 of 15
Passive DNS implementation from scratch

- Project started end of February 2011 (work-in-progress) with another Redis key-value datastore
- Only 2K lines of Perl code for the website, dnscap parser and Redis stream insert/update
- Running with 6 DNS sensors on recursive nameserver located in LU
- ~ 25 million keys in less than 6 months
- Fast lookup time but ranking of all resource elements takes 2 days
- Everything in ~ 4GB of memory (→ space for the future...)
- [http://pdns.circl.lu/](http://pdns.circl.lu/)
Conclusion

- The security ranking of Internet resources helps us (and others) to work everyday with the amount of data collected
- Domain and DNS records "real-time" ranking is the next step
- BGP Ranking and Passive DNS datasets available for researchers
- Passive DNS and ranking common query interface (with CERT.at) → Internet-Draft