BGP AS / ISP Security Ranking

Raphaël Vinot
raphael.vinot@gmail.com

Conostix

Workshop
Hack.lu 2010

Table of contents

Content

Basics terms

- What is the Border Gateway Protocol (BGP) ?
- What is an Autonomous System (AS) ?

Border Gateway Protocol (BGP)

- Routing protocol of the Internet
- Associate Autonomous Systems and Networks
- Use policies (QoS and security)

Autonomous System (AS)

- Identify operators without using IPs
- One or more subnet for each ASN
- Assignation: IANA, RIR and LIR

Content

RIS Whois

- Routing Information Service (RIS)
- Updated every 8 hours

193.0.19.19

```
route: 193.0.18.0/23
origin: AS3333
descr: RIPE-NCC-AS RIPE Network Coordination Centre
lastupd-frst: 2010-06-21 15:10Z 198.32.176.24@rrc14
lastupd-last: 2010-08-31 22:48Z 198.32.160.187@rrc11
seen-at: rrc00,rrc01,rrc03,rrc04,rrc05,rrc06,rrc07,[...]
num-rispeers: 102
source: RISWHOIS
```

Whois

- More information (owner)
- Many, incompatible, databases
- Find the right server

- Deactivated by default

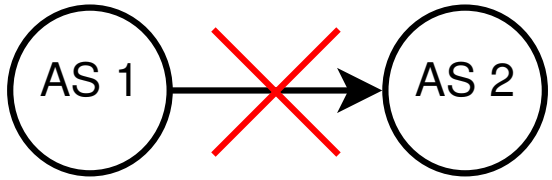
Datasets

- Used is the system now:
  - abuse.ch ZeuS Tracker
  - Dshield (Top IPs and Daily)
- Other modules available:
  - Arbor ATLAS/Active Threat Feed
  - Shadowserver (three lists)
  - Abusix

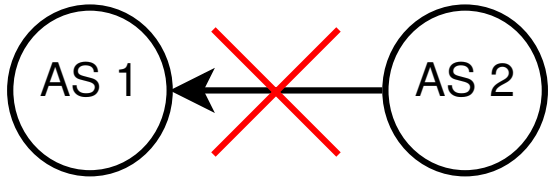
Content

Mitigation

- Blackholing
  - From the AS (Command & Control Server)



  - To the AS (Phishing, keylogger)



Information

- Alert the user
- Contact the provider
- Contact the authorities
- History

Content

High-level view

- Aggregation
  1. datasets
  2. RIS Whois and Whois entries
- Ranking by Autonomous System Number

$$R = 1 + \frac{(SUM(IPs * s\_impact) * SUM(vote))}{AS\_size}$$

IPs all the IPs from the ASN, by sources.

s_impact value assigned to the source

vote vote against this AS (actually not implemented)

AS_size total of IPs

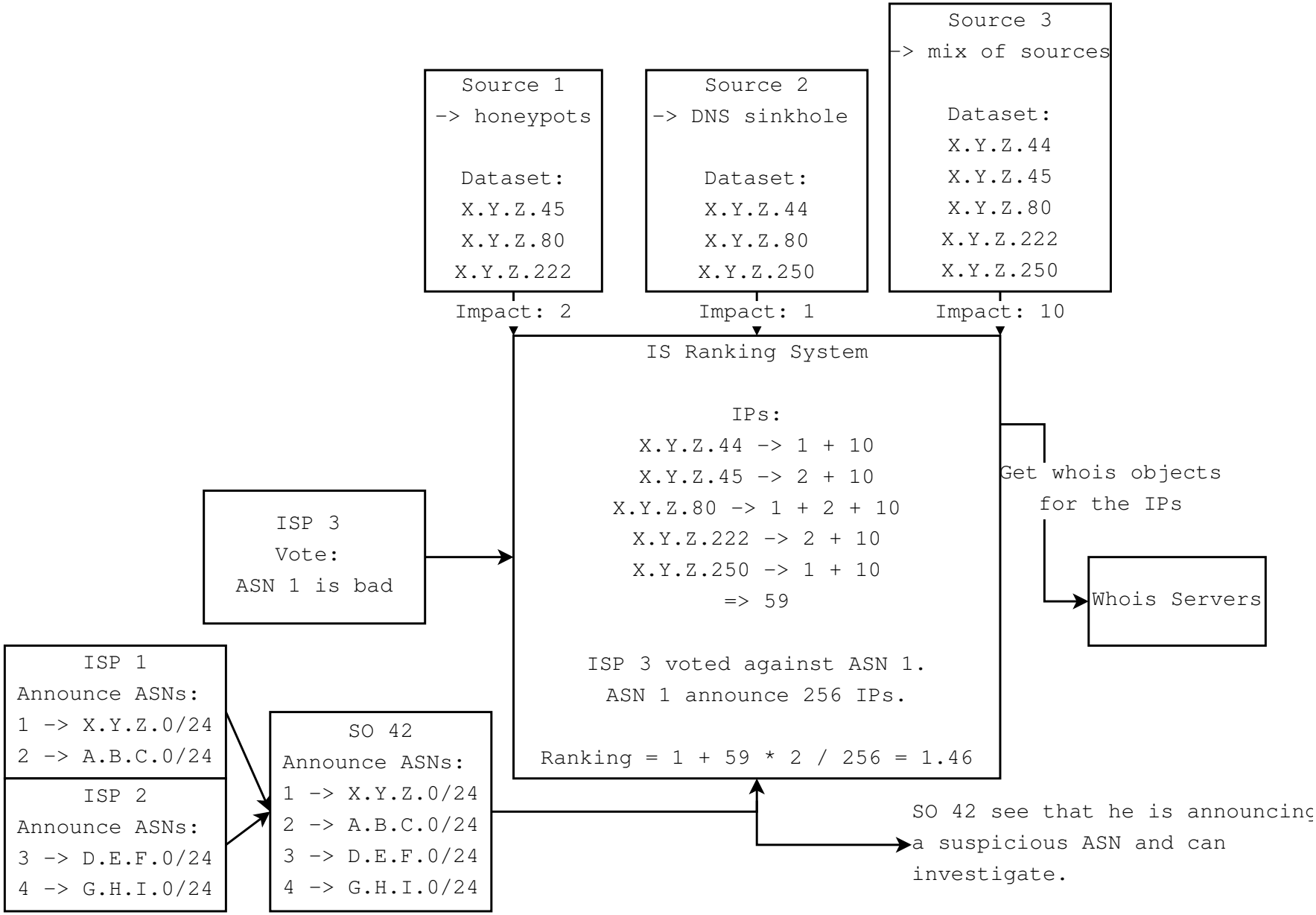


Figure: High level

Content

Input

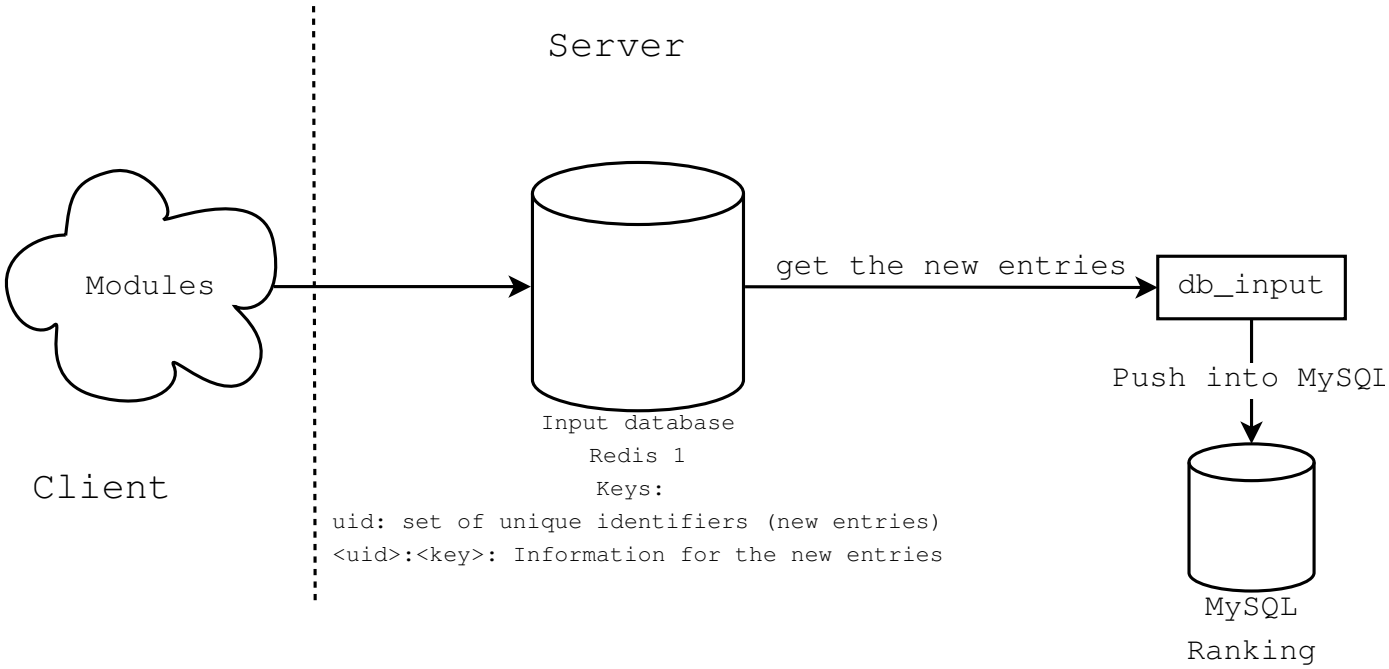


Figure: Input of new information

- Modules push the information into redis
- A "reader" push them into MySQL

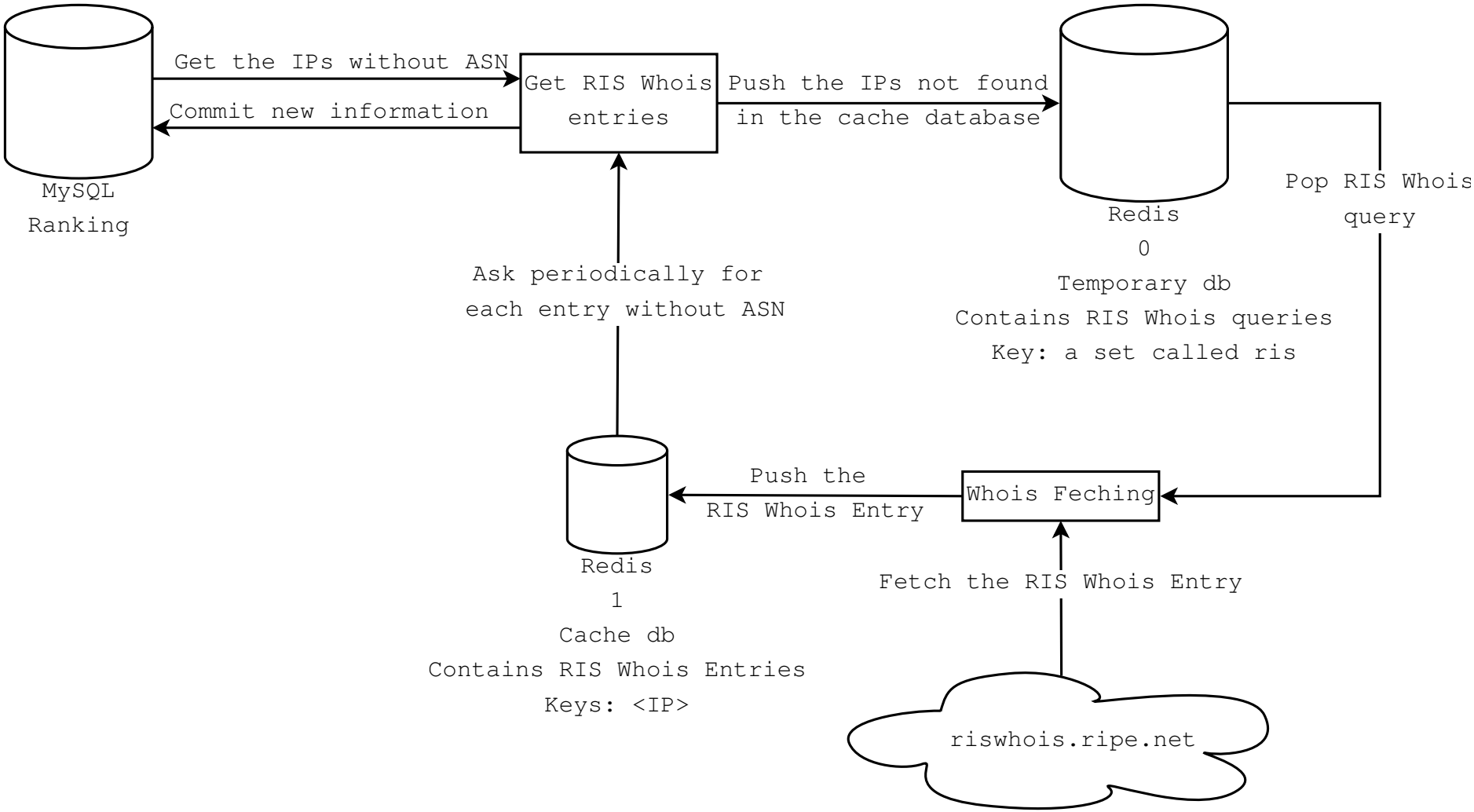


Figure: RIS Whois fetching

Ranking

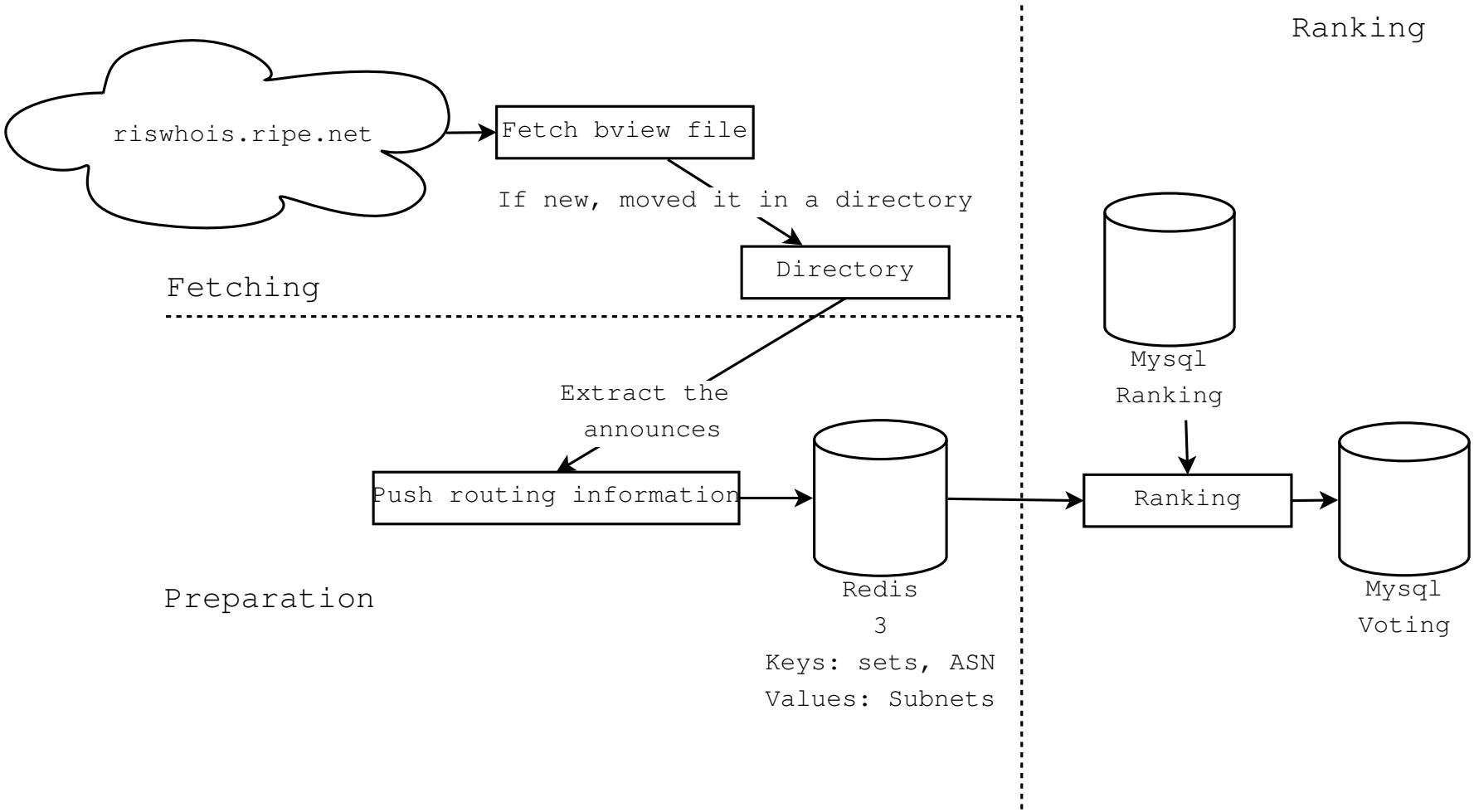


Figure: Ranking

Modules - Input API

- Supported information:
  - Always: IP and Source
  - If possible: Timestamp
  - Sometimes: Infections type, raw field
- Multiprocessing
- Format:
  - $< UID >:< FIELD >$
  - List of UID
- Interest: No limitations on the type of the sources

Content

Global Ranking

ASN	AS Description	Comments
65024 Origin: 8551	-Private Use AS- BEZEQ-INTERNATIONAL	Private AS Configuration problem ? Odd.
50693	*No description,* *not a good sign.*	178.20.200.0/21 Dusan Bajic, Serbia
29436	ASN-IMPERIAL Imperial ISP	193.238.36.0/22 Buryanov K. Volodimirovich, Ukraine
21342	AKAMAI-ASN2 Akamai Technologies AS	193.108.88.0/24 - 193.108.91.0/24 Noam Freedman, Cambridge - False positive?
131089	Same as 50693	61.19.64.0/22 Kitti Srikate Srikate, Thailand
40427	IRONPORT-SYSTEMS-CI365	False positive, I hope so... :)

- All the sources are merged
- Some false positives / odd entries (Dshield Daily)
- Small subnets

Ranking: Dshield Top IPs

ASN	AS Description	Comments
45847	NSTRU-AS-AP, university network Nakornsitammarat	202.29.33.0/24 Watcharapong Sanguankum, Thailand
48061	RUTUBE-AS CJSC RuTube	194.190.76.0/23 - 91.207.58.0/23 RuTube NCC, Moscow
46940	IAC-VZ-ABOVENET-BGP IAC/INTERACTIVECORP	63.119.10.0/23 http://www.iac.com/
39660	NETTRANS-AS Integrated Transport Network, Ltd. AS	Announce 15872 IPv4 Svjatoslav Komarov, Russian Federation
36493	36493295CA-TOR-ASN 3757277 Canada Inc.	Announce 20992 IPv4 TOR(onto) :)

- Contains the 100 IPs found the most often in the daily list
- Note: the same IP found more than one time in a dataset is skipped

Ranking: Zeustracker

ASN	AS Description	Comments
34528	YALTAINFO-AS YaltaInfo ISP	193.41.38.0/24 Rostislav Sokolov, Ukraine
50134	SOFTEL Softel Consulting s.r.o.	193.104.146.0/24 Milan Puzik, Czech Republic
50793	ALFAHOSTNET Alfa-Host LLP.	193.105.207.0/24 Romanov Artem Alekseevich, Kazakhstan
48876	INTERA-AS Takomi Ltd	194.79.250.0/23 Alexey Tingaev, Russia
43181	K2K-AS Contel 2000 Ltd.	193.27.232.0/23 Dmitry Ermolaev, Russia
25052	ORION-AS ORION ISP	193.201.192.0/23 Alik Grigorchook, Ukraine

- ... :-)

Content

FIRE: FInding RoguE Networks - maliciousnetworks.org

The top ten		
ASN	Description	IPv4 announced
36408	ASN-PANTHER Panther Express	50176
21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	1538560
26496	PAH-INC - GoDaddy.com, Inc.	923392
24940	HETZNER-AS Hetzner Online AG RZ	436992
36057	WEBAIR-AMS Webair Internet Development Inc	24576
32475	SINGLEHOP-INC - SingleHop	197632
4134	CHINANET-BACKBONE No.31,Jin-rong Street	101040384
27715	LocaWeb Ltda	50944
14618	AMAZON-AES - Amazon.com, Inc.	331776
11388	MAXIM - Peer 1 Dedicated Hosting	135168

- Seems different but all the AS are also in BGP Ranking
- In BGP Ranking:
  - AS4134: more than 20.000 IPs per day
  - AS21844: around 300 IPs per day

Content

Conclusion

- Some differences in the algorithm
- Usage of different sources
- BGP Ranking can report more precisely the “real” bad guys...
- ... but you will only see the small ones.

Interested by the system?

- BGP Ranking is opensource (AGPLv3). Code available on gitorious and github:
  - *http://gitorious.org/bgp-ranking*: testing, it works, most of the time.
  - *http://github.com/Rafiot/bgp-ranking*: more stable.

Next steps

- Implement other rankings:
  - FIRE-like: based on the number of IP for each ASN
  - By subnet: based on the number of IP for each subnet (WIP)
    - ⋆ Generate blacklists for firewalls (WIP)
- Improve the website :-)
  - I'm looking for a web developer...
- Use other sources
  - I just need the format of the file
- Any other (crazy) ideas you may have!

Any Questions, ideas?

Do you want to test with your own ASNs?

213.169.106.146

Thank you for your attention.