BGP AS / ISP Security Ranking

Raphaël Vinot

Chaos Computer Club Trier

Table of contents

Content

Internet and the peering

- Decentralized network
- Many operators
- Different types of peering

Border Gateway Protocol (BGP)

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

Autonomous system

- Identify operators without using IPs
- One or more subnet for each ASN
- Assignation: IANA, RIPE NCC, 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

Datasets

- Arbor ATLAS/Active Threat Feed
- abuse.ch ZeuS Tracker
- Dshield
- Shadowserver

Content

Threats

- Users just do not care. At all.
- Mobile devices and Internet
- Growing business
- *"non-profit" malicious software are dead*, Kaspersky - 2007

Botnet

- Botmaster
- Command & Control Server
- Bots

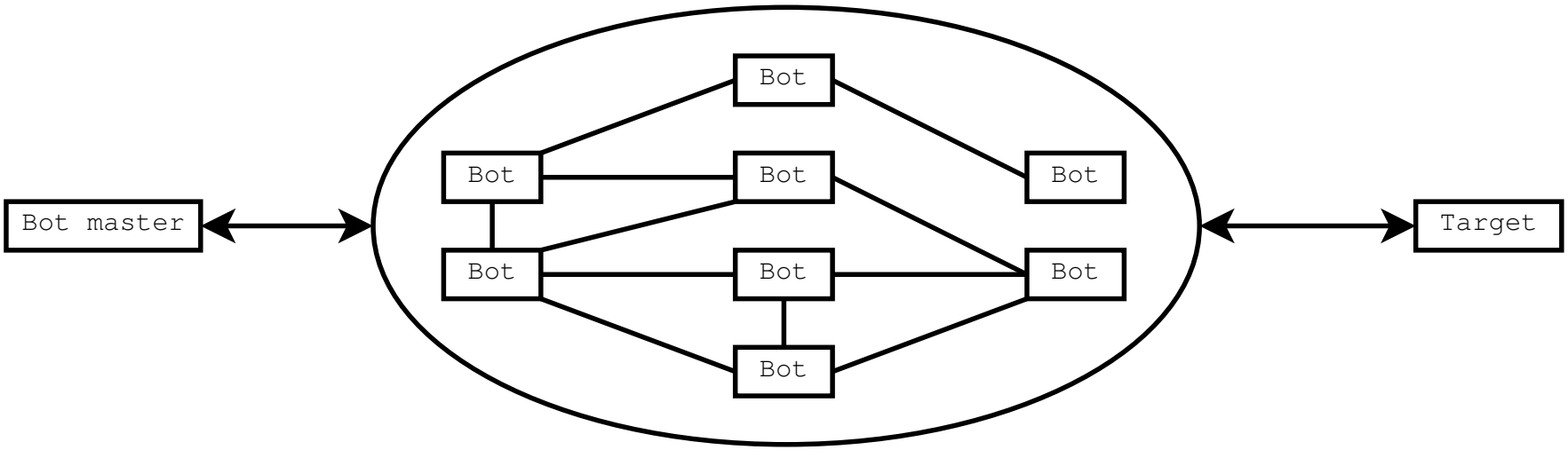


Figure: Botnet - Basics

- DDoS, phishing...

Content

Mitigation

- Traffic shaping
- Blackholing
- Depending on the attack
  - From the AS (DDoS, Command & Control Server)
  - To the AS (Phishing, keylogger)

Information

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

Content

Requirements

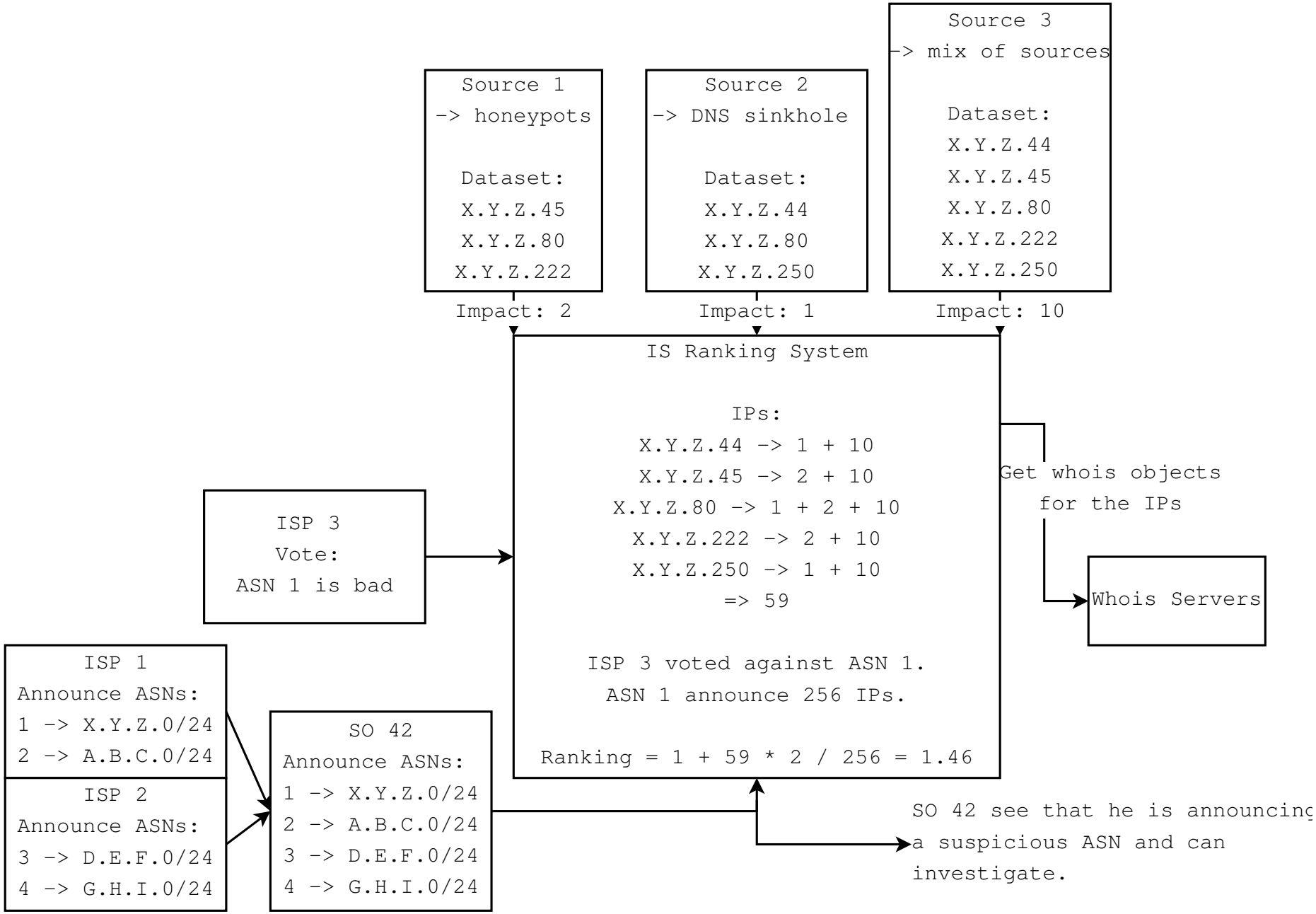
- Opensource
  - Affero GPLv3
- Fast
  - *mapreduce*-like processing

High-level view

- Aggregation
  1. datasets
  2. RIS Whois and Whois entries
- Ranking

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

occur	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


Source 1
-> honeypots
Dataset:
X.Y.Z.45
X.Y.Z.80
X.Y.Z.222
Impact: 2
Source 2
-> DNS sinkhole
Dataset:
X.Y.Z.44
X.Y.Z.80
X.Y.Z.250
Impact: 1
Source 3
-> mix of sources
Dataset:
X.Y.Z.44
X.Y.Z.45
X.Y.Z.80
X.Y.Z.222
X.Y.Z.250
Impact: 10
IS Ranking System
IPs:
X.Y.Z.44 -> 1 + 10
X.Y.Z.45 -> 2 + 10
X.Y.Z.80 -> 1 + 2 + 10
X.Y.Z.222 -> 2 + 10
X.Y.Z.250 -> 1 + 10
=> 59
ISP 3 voted against ASN 1.
ASN 1 announce 256 IPs.
Ranking = 1 + 59 * 2 / 256 = 1.46
ISP 3
Vote:
ASN 1 is bad
Get whois objects
for the IPs
Whois Servers
ISP 1
Announce ASNs:
1 -> X.Y.Z.0/24
2 -> A.B.C.0/24
ISP 2
Announce ASNs:
3 -> D.E.F.0/24
4 -> G.H.I.0/24
SO 42
Announce ASNs:
1 -> X.Y.Z.0/24
2 -> A.B.C.0/24
3 -> D.E.F.0/24
4 -> G.H.I.0/24
SO 42 see that he is announcing
a suspicious ASN and can
investigate.

Third party programs

- Redis
- MySQL
- libbgpdump
- Rgraph
- Cheetah and Cherrypy

Website and first results.

Fragen ?