A2B Internet

The Naughty port Project

May 2016

RIPE72 2016 – Copenhagen, DK

Prepared by:
Erik Bais
ebais@a2b-internet.com

What is our business ??

- Registration of IP addresses and AS numbers
- IP Transit in various Dutch datacenters
- Internet (Fiber) Access & Datacenter Network Services
- 24 * 7 Monitoring and management of BGP infrastructure.
- Specialized consultancy for ISP related topics like vendor selections, network design & implementation.

Currently in the following Dutch datacenters

The original question to solve ..

Results during a DDOS ...

- Customers start calling as their primary traffic link is filled with garbage.
- Not every complaining customer can afford or want to pay for DDOS mitigation plans.
- Customers will complain if they are seeing packetloss …
- Customers will complain quickly if they are offering VoIP or Hosted Desktop or VPN services … (Oh yes .. And gamers …)
- Customers don't want to suffer from a DDOS to another customer.

- The phone lines to the helpdesk are also red-hot during a DDOS …

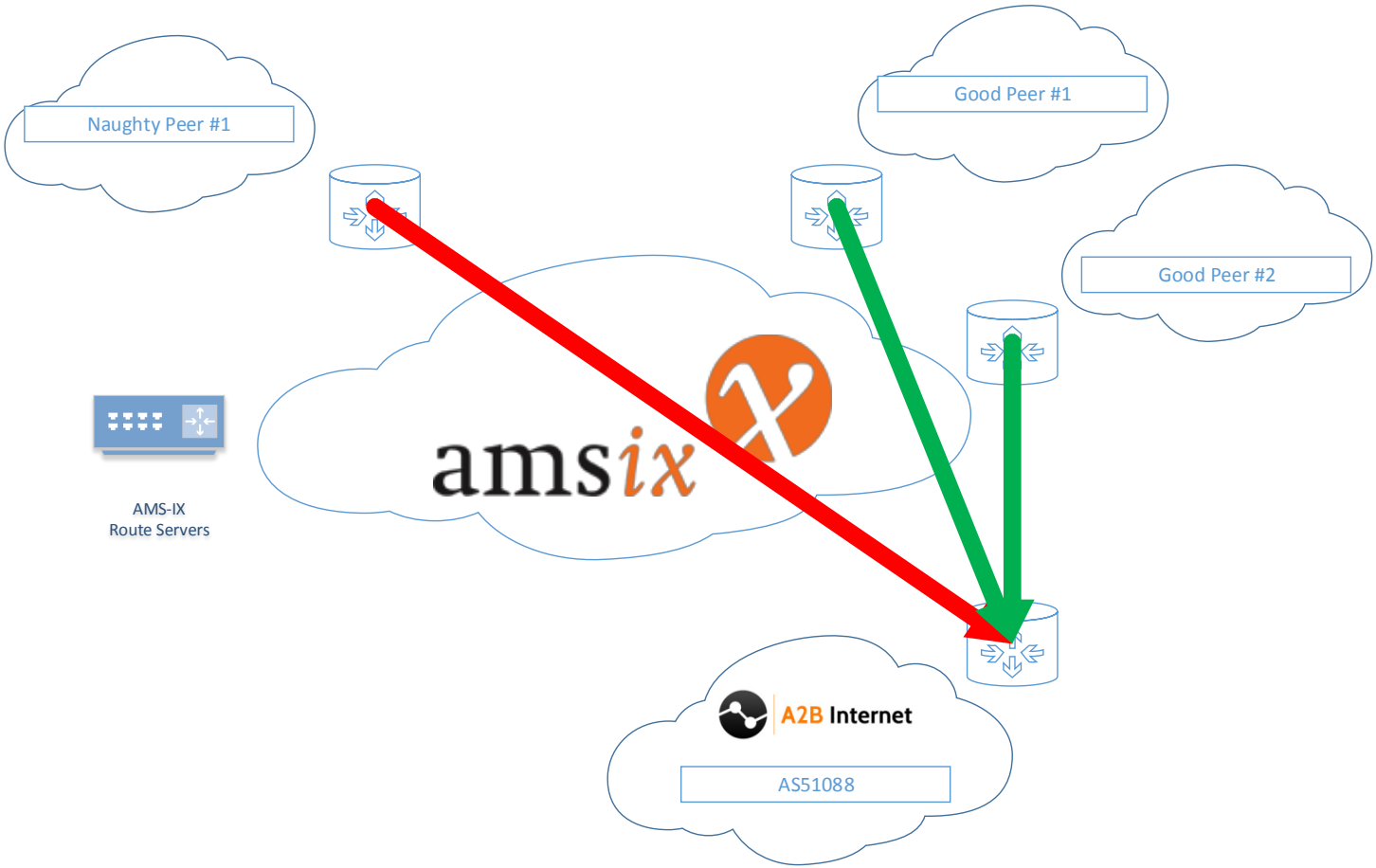
- Customers make it your problem …


One Does Not Simply
Stop DDOS Attacks
mememaker.net

Defining questions :

- Where is the traffic originating from (Which ASn ..)
- Is the (original) traffic Spoofed IP traffic ?
- Can we filter the non-BCP38 traffic ?
  - Should we want to filter this ?
  - Will the used HW actually support such large ACL's ? (Nope..)
- Why are we noticing those Top Speakers only during a DDOS ?
- Will de-peering fix our issue ?

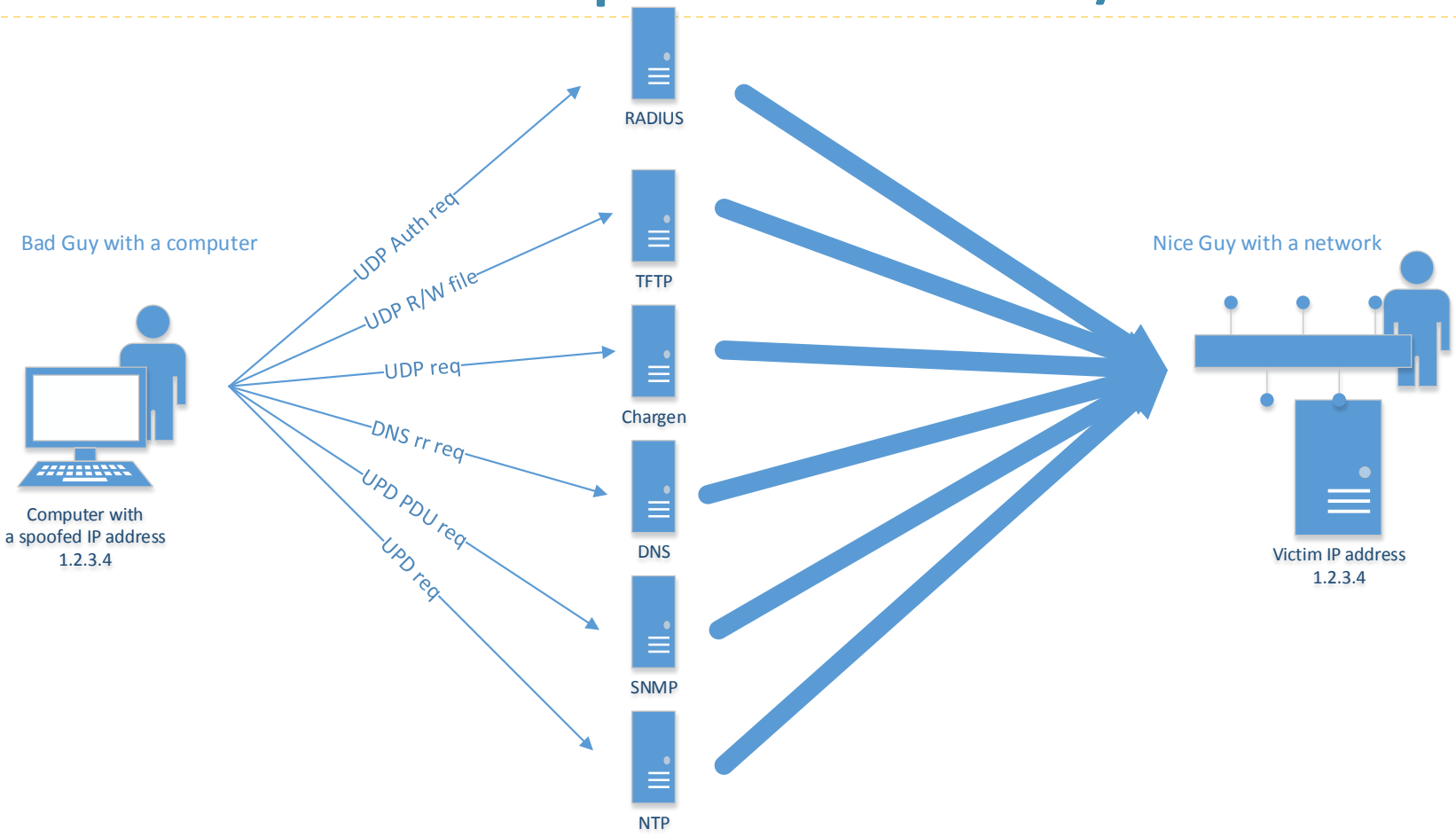
Regular Internet Exchange setup



Let's build a test setup …

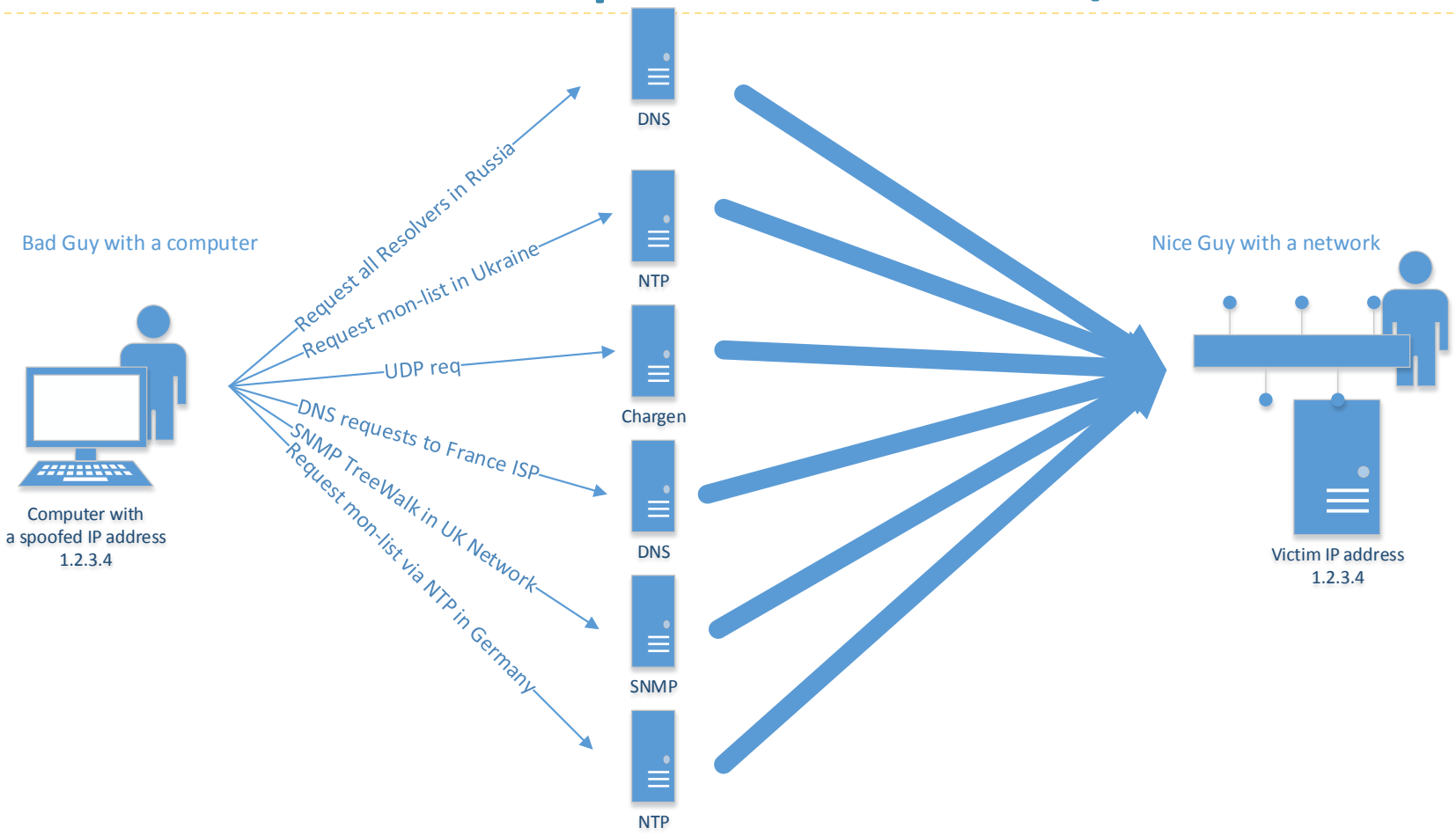
- How do these DDOS Stresser / booter sites work …

DDOS Amplification basics 1/2



Amplification Attacks Basics

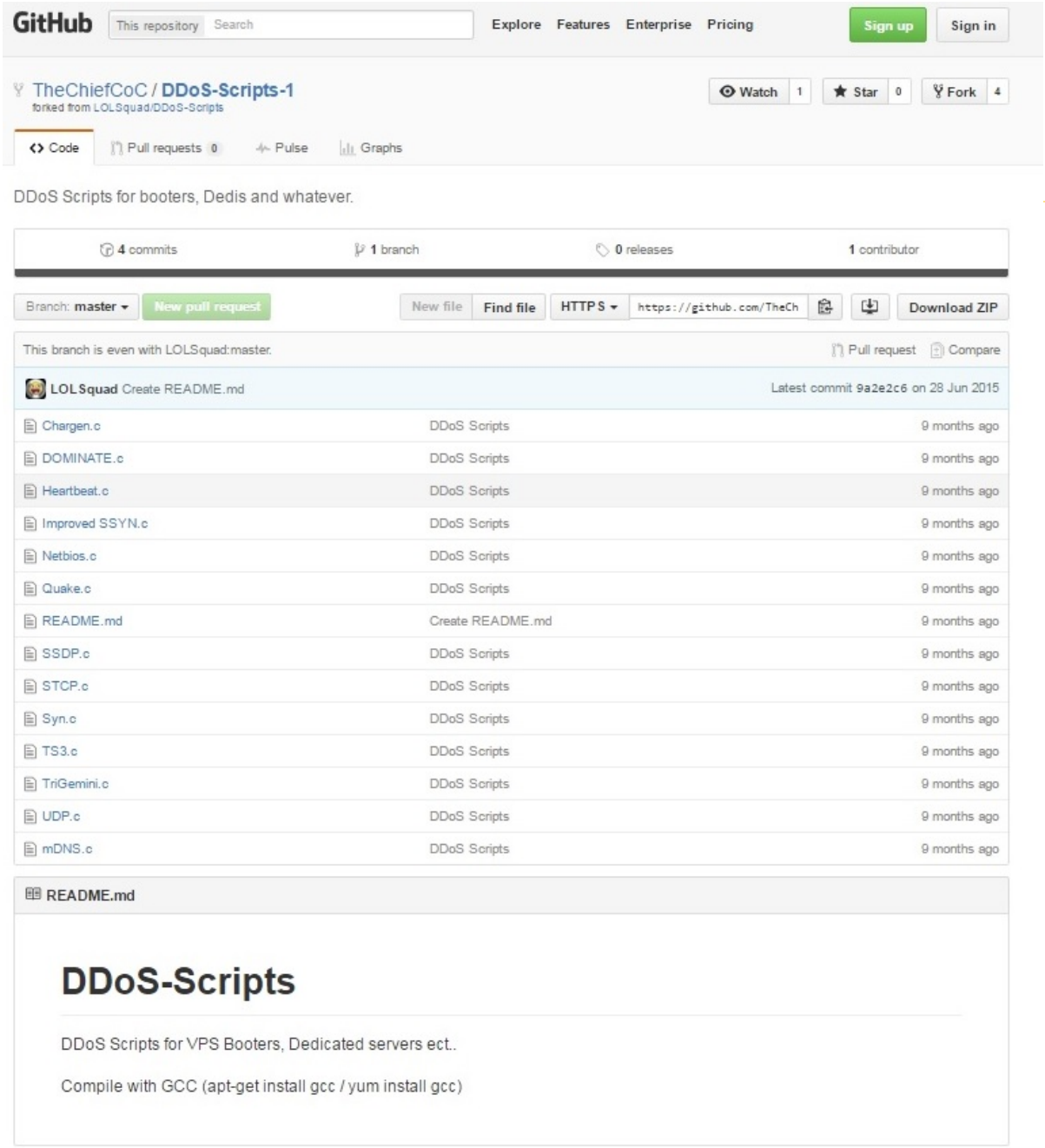
DDOS Amplification basics 2/2



Amplification Attacks Basics

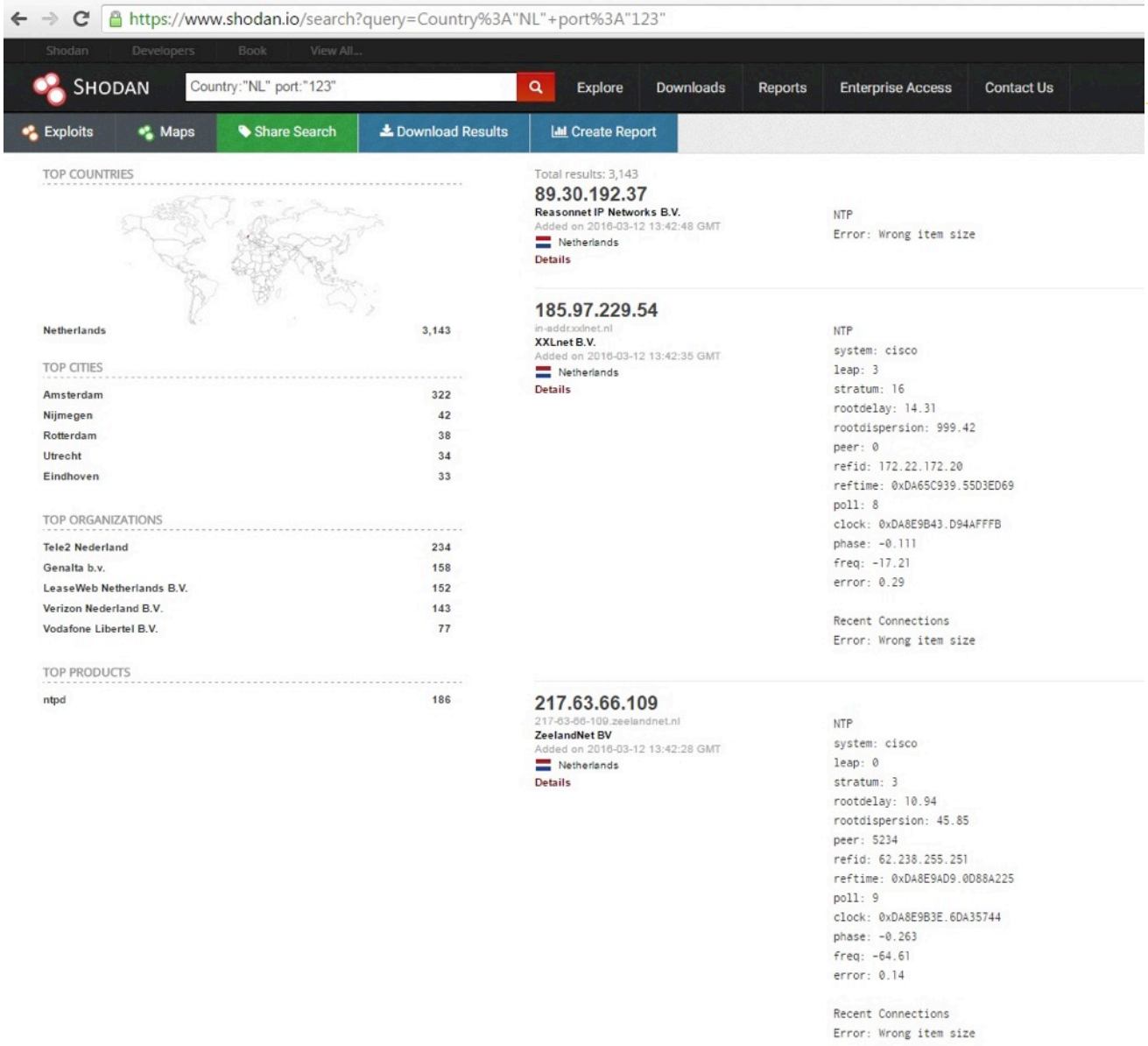
Let's build a test setup …

- How do these DDOS Stresser / booter sites work …
- Enough scripts available on GitHub etc for testing …


GitHub
This repository
Search
Explore
Features
Enterprise
Pricing
Sign up
Sign in
TheChiefCoC / DDoS-Scripts-1
forked from LOLSquad/DDoS-Scripts
Watch 1
Star 0
Fork 4
Code
Pull requests 0
Pulse
Graphs
DDoS Scripts for booters, Dedis and whatever.
4 commits
1 branch
0 releases
1 contributor
Branch: master
New pull request
New file
Find file
HTTPS
https://github.com/TheCh
Download ZIP
This branch is even with LOLSquad:master.
Pull request
Compare
LOLSquad Create README.md
Latest commit 9a2e2c6 on 28 Jun 2015
Chargen.c DDoS Scripts 9 months ago
DOMINATE.c DDoS Scripts 9 months ago
Heartbeat.c DDoS Scripts 9 months ago
Improved SSYN.c DDoS Scripts 9 months ago
Netbios.c DDoS Scripts 9 months ago
Quake.c DDoS Scripts 9 months ago
README.md Create README.md 9 months ago
SSDP.c DDoS Scripts 9 months ago
STCP.c DDoS Scripts 9 months ago
Syn.c DDoS Scripts 9 months ago
TS3.c DDoS Scripts 9 months ago
TriGemini.c DDoS Scripts 9 months ago
UDP.c DDoS Scripts 9 months ago
mDNS.c DDoS Scripts 9 months ago
README.md
DDoS-Scripts
DDoS Scripts for VPS Booters, Dedicated servers ect..
Compile with GCC (apt-get install gcc / yum install gcc)

Let's build a test setup …

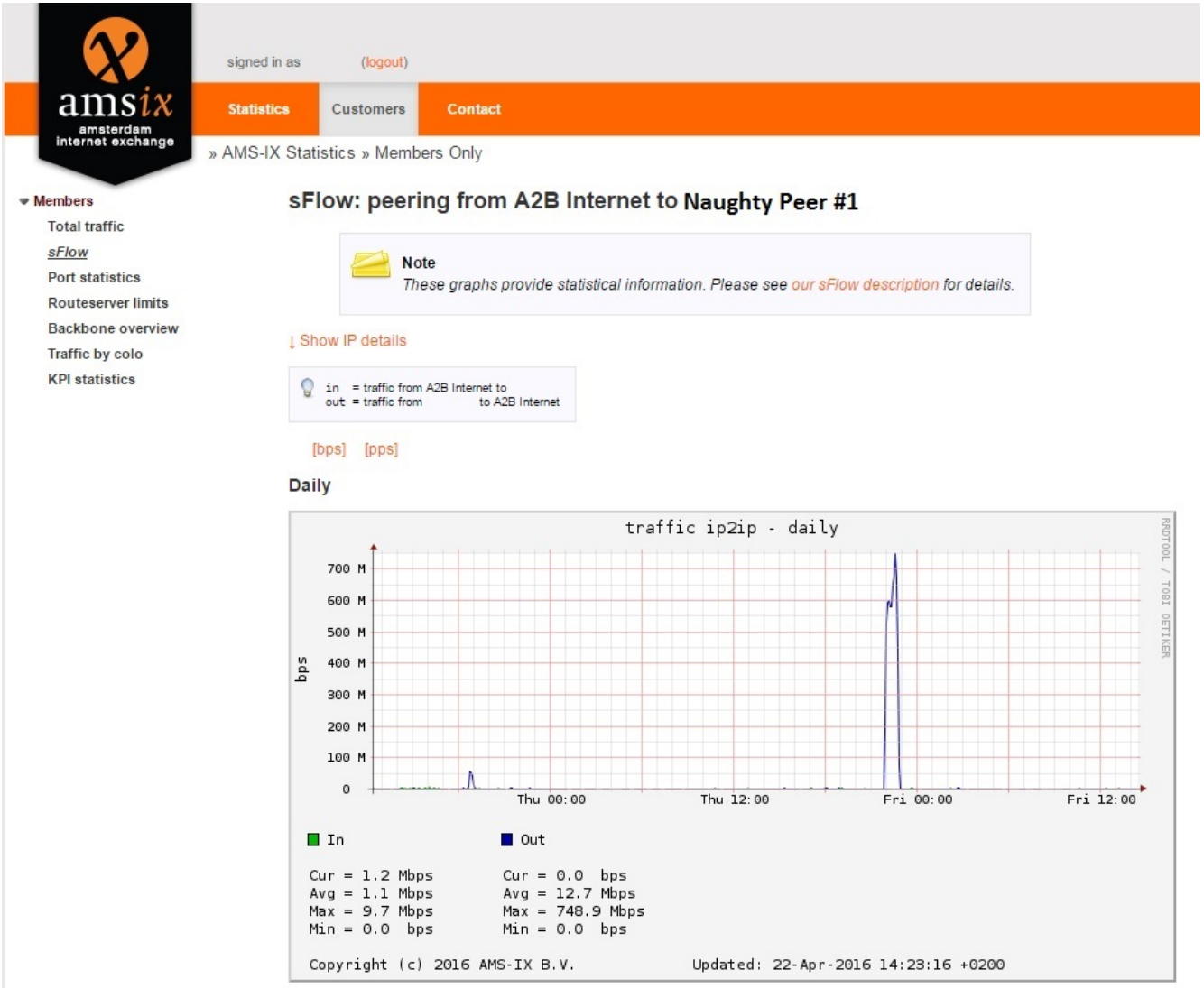
- How do these DDOS Stresser / booter sites work …
- Enough scripts available on GitHub etc for testing …
- And no need to scan the complete internet for vulnerable IP's .. Everything can be parsed from downloads of exports via Shodan.io for example …


https://www.shodan.io/search?query=Country%3A"NL"+port%3A"123"
Shodan
Developers
Book
View All...
SHODAN
Country:"NL" port:"123"
Explore
Downloads
Reports
Enterprise Access
Contact Us
Exploits
Maps
Share Search
Download Results
Create Report
TOP COUNTRIES
Netherlands 3,143
TOP CITIES
Amsterdam 322
Nijmegen 42
Rotterdam 38
Utrecht 34
Eindhoven 33
TOP ORGANIZATIONS
Tele2 Nederland 234
Genalta b.v. 158
LeaseWeb Netherlands B.V. 152
Verizon Nederland B.V. 143
Vodafone Libertel B.V. 77
TOP PRODUCTS
ntpd 186
Total results: 3,143
89.30.192.37
Reasonnet IP Networks B.V.
Added on 2016-03-12 13:42:48 GMT
Netherlands
Details
NTP
Error: Wrong item size
185.97.229.54
in-addr.xxlnet.nl
XXLnet B.V.
Added on 2016-03-12 13:42:35 GMT
Netherlands
Details
NTP
system: cisco
leap: 3
stratum: 16
rootdelay: 14.31
rootdispersion: 999.42
peer: 0
refid: 172.22.172.20
reftime: 0xDA65C939.55D3ED69
poll: 8
clock: 0xDA8E9B43.D94AFFFB
phase: -0.111
freq: -17.21
error: 0.29
Recent Connections
Error: Wrong item size
217.63.66.109
217-63-66-109.zeelandnet.nl
ZeelandNet BV
Added on 2016-03-12 13:42:28 GMT
Netherlands
Details
NTP
system: cisco
leap: 0
stratum: 3
rootdelay: 10.94
rootdispersion: 45.85
peer: 5234
refid: 62.238.255.251
reftime: 0xDA8E9AD9.0D88A225
poll: 9
clock: 0xDA8E9B3E.6DA35744
phase: -0.263
freq: -64.61
error: 0.14
Recent Connections
Error: Wrong item size

Let's build a test setup …

- How do these DDOS Stresser / booter sites work …
- Enough scripts available on GitHub etc for testing …
- And no need to scan the complete internet for vulnerable IP's .. Everything can be parsed from downloads of exports via Shodan.io for example …
- And that insight gives a better view on why we see the following during a DDOS …

AMS-IX Sflow tools



The "We ♥ AMS-IX" page

- Their per peer Sflow graphs & monitoring at the customer portal rocks.
- The AMS-IX Route-servers support RPSL … (important …)
  - RIPE DB export-via / import-via support (YEAH!!)
- Their NOC engineers were very helpful in assisting to get the solution to work. (Thnx Aris & Kostas !!)
- The AMS-IX sales team provided us a flexible "Try and Buy" option contract at the Evoswitch Datacenter

Let's try something else ...

- List all AS's that are only sending traffic DURING a DDOS amplification attack.
- Most of these networks don't send ANY or hardly any traffic during normal operations in our case..
- Can we peer with these parties via the Routeserver on Port X but not via Port Y … Will the Route Server support that .. ??
- Peer with the "Naughty Peers", on a small (1Gb) IXP port.
- Explain the setup to Sales@AMS-IX. Try this out in a setup in production.
  - A "try and buy agreement" for the second port via the AMS-IX EvoSwitch Datacenter Partner.

RIPE RPSL & AMS-IX Routeserver integration

```
Abuse contact info: abuse@a2b-internet.com

aut-num:        AS51088
as-name:        A2B
descr:          A2B IP B.V.
org:            ORG-AIbi1-RIPE
remarks:        ============================================================
remarks:        AMS-IX peering
remarks:        ============================================================
import:         from AS51088:AS-PEERS-AMSIX action pref=80; accept ANY AND NOT {0.0.0.0/0}
export:         to AS51088:AS-PEERS-AMSIX announce AS-A2B
remarks:        ============================================================
remarks:        AMS-IX route server policy
remarks:        ============================================================
import-via:     AS6777 from AS-AMS-IX-RS EXCEPT AS61180:AS-PEERS-AMSIX accept ANY
export-via:     AS6777 to AS-AMS-IX-RS EXCEPT AS61180:AS-PEERS-AMSIX announce AS-A2B
remarks:        ============================================================
remarks:        A2B Internet customers
remarks:        ============================================================
```

Login to update RIPEstat

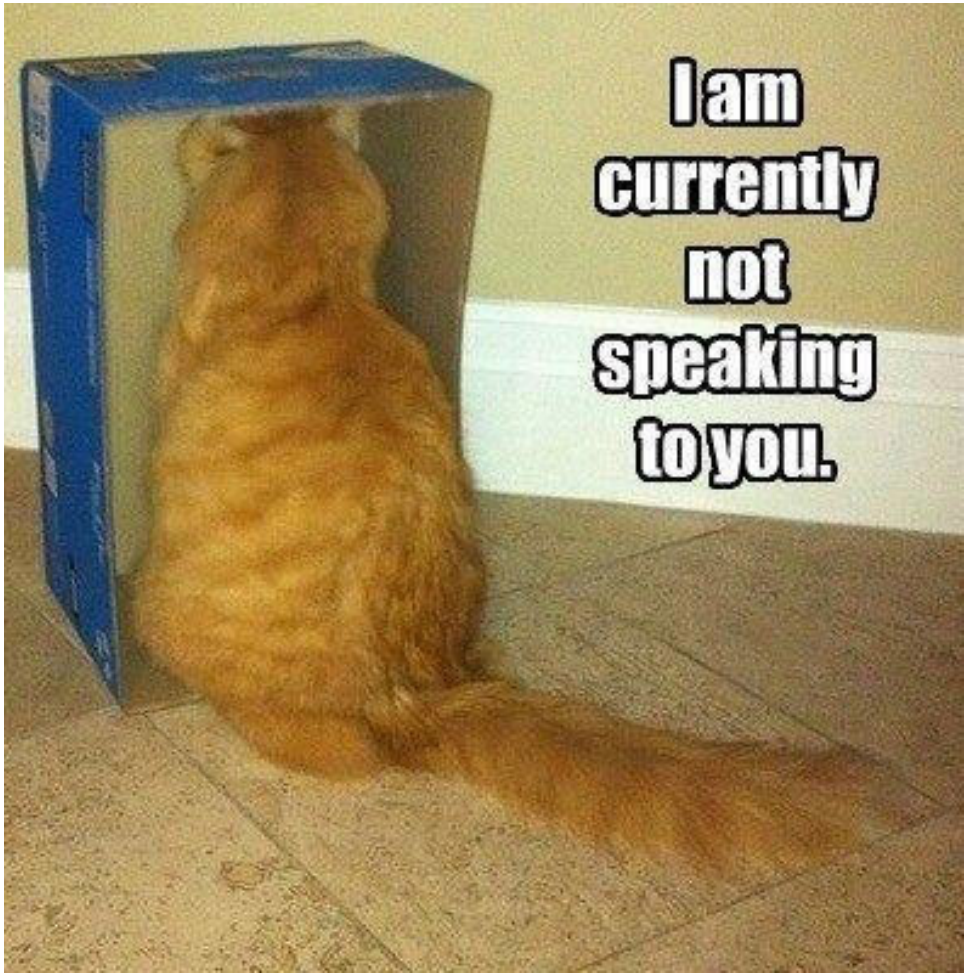
- A simple include / exclude in RIPE RPLS was all it took …

Fun fact …

- AMS-IX had a 2 vendor approach before we started this project.

- But one of the AMS-IX Route Server vendors couldn’t handle the new load on the route-server by the split view with the views via RPSL.

So one of the Routeserver did …



Fun fact …

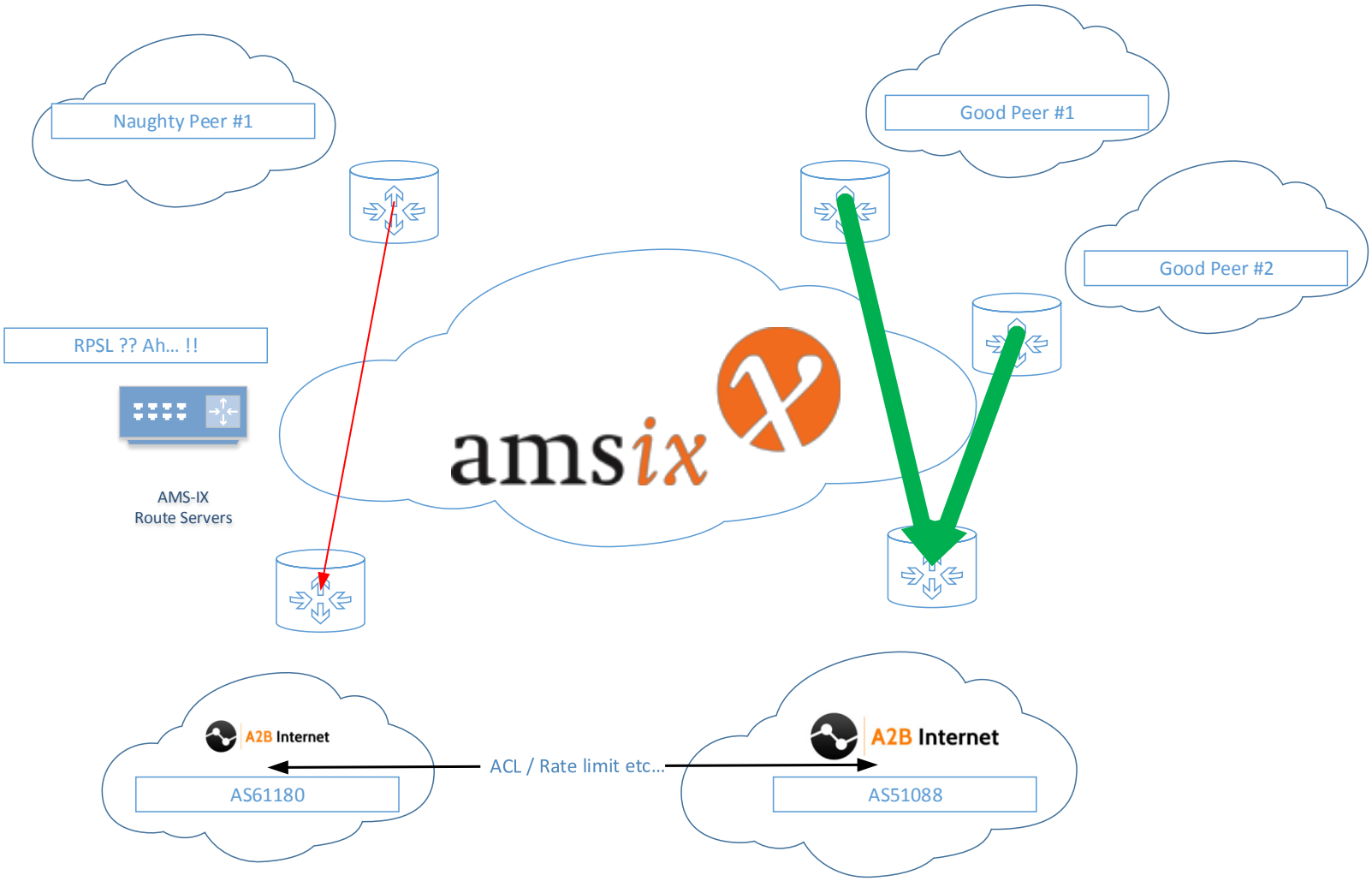
- AMS-IX had a 2 vendor approach before we started this project.
- One of the AMS-IX Route Server vendors couldn't handle the route-server split view with the views via RPSL.
- Famous last words… "Let's put this on production in Friday, what could go wrong…"
  - Resulting in the death of 1 set of route servers over the weekend …

We asked the NOC ….

- Shall we take it off-line ?
- Will that help ? It is not in production anyway (for us..)
- And they kindly declined in order to be able to troubleshoot
  - To have a valid reason to kill those RS …

Kudos

Naughty Port Setup



New questions to ponder …

- Why are some networks on the Naughty list …
- Can we predict who should be on the list …
- Do we have Santa Skills ?

Santa Skillz …

New questions to ponder …

- Why are some networks on the Naughty list …
- Can we predict who should be on the list …
- Do we have Santa Skills ?
  - Can we tell who is Naughty and who is nice ?

New questions to ponder …

- Why are some networks on the Naughty list …
- Can we predict who should be on the list …
- Do we have Santa Skills ?
  - Can we tell who is Naughty and who is nice ?
- What are the benefits of having a Naughty Port …


EUREKA

Rating the Naughty Networks ….

- We've put every AS in a database …
- Uploaded the number of Open resolvers, NTP servers, Chargen, SNMP, SSDP IP's etc per AS in the database.
- Pulled the number of announced IP per AS from the RIPE RIS API's

- A high Naughty Rating, doesn´t mean a bad peer …
  - But is a naughty peer worth the trouble on your premium network link ?
  - Is a peer selection based on 'just' traffic ratio accurate ?

- Ratings can be improved by proper Abuse Management …
  - (Yes it is that simple. . .)

Time for reach-out …

- We've asked several Dutch ISP's if we can name them in this presentation and explain them about the project..

- Most of them responded with :
  - "Yes you may use our name and data…"
  - And … "How do we improve our rating ?"

- And these are their results…

Naughty Port ratings

asn	as_name	amsix_org	naughty_rating	announced_ips	chargen_count	dnsscan_count	ntpscan_count	snmpscan_count	ssdpscan_count
50295		Triple-IT	9.52855747767857	7168	*NULL*	4	63	55	*NULL*
33915	TNF-AS	Vodafone Libertel B.V.	5.58843131414956	174592	2	34	1706	38	9
39647	REDHOSTING-AS	Redhosting B.V. & Voiceworks B.V.	2.37378117487981	53248	1	34	89	124	8
8455	ATOM86-AS	atom86	0.972587719298246	14592	*NULL*	1	20	5	*NULL*
50266		Vodafone Libertel B.V.	0.344392599587912	232960	*NULL*	8	133	8	31
1103	SURFNET-NL	SURFnet	0.0866945765893846	8778240	*NULL*	42	1262	69	485
51088	A2B	A2B Internet	0.0401844671375921	104192	*NULL*	*NULL*	1	6	1
1101	IP-EEND-AS	SURFnet	0.000630294473578056	1903872	*NULL*	*NULL*	*NULL*	2	*NULL*

Naughty Rating interface

Search ASN

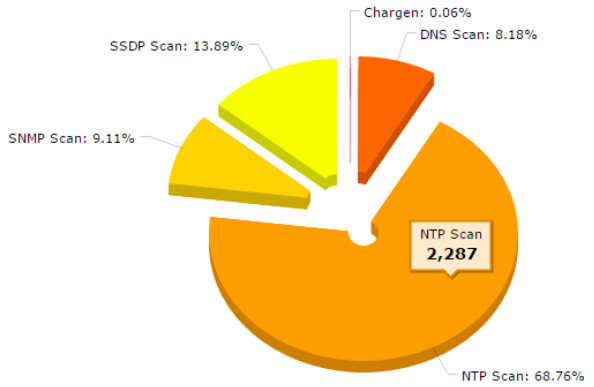
1103

Search ASN

Information

AS Name: SURFNET-NL
AMSIX Org: SURFnet
Naughty Rating: 0.16913
Announced IPs: 8778240
Last Update: 2016-05-15 00:00:00

Pie Chart



How to improve you rating ?

- Implement Abuse.IO … (Yes, it is free.. and Open Source !!)
  - https://abuse.io/
  - For automagic abuse msg parsing and event handling

- Request reports on your network at Shadowserver.org
  - https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork#toc3
    - There is a backlog on network report requests, processing may not be instant.

Would you want your own Naughty Port ?

- We can explain how it works … and how we did it ..
- We can share the data … provide access to the portal.
- All you need is an extra AMS-IX port and an extra AS number.
- And you can decide for yourself who you want on your list.

Triple-IT already proofed it can be fixed …

Search ASN

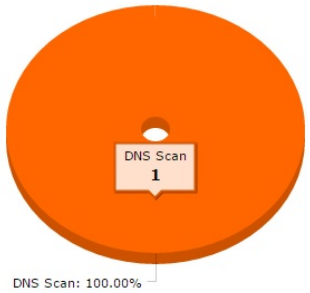
50295

Search ASN

Information

AS Name: TRIPLE-IT
AMSIX Org: Triple-IT
Naughty Rating: 0.00753
Announced IPs: 7168
Last Update: 2016-02-10 00:00:00

Pie Chart



Next steps :

- Publish the Naughty Rating Search interface on a website.
  - We want the data to be open for all peering managers.
- Check/discus what needs to be added .. ? TFTP ? Others ?
- Checks per AS-SET's as well as AS number.

Who has a question ?

Email to: ebais@a2b-internet.com
Or call : +31 – 85 – 90 20 410