A2B Internet

Why are we still seeing DDOS traffic ??

We can fix most of this …

right ??

Short intro

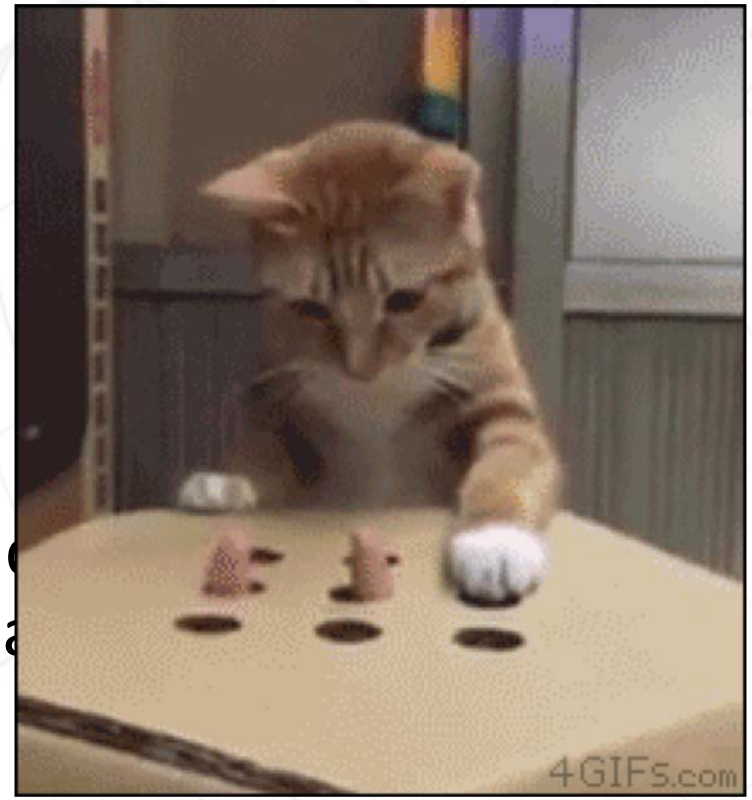
- A2B Internet is a Dutch network provider.
  - Providing datacenter connectivity (transit) and internet access on fiber.

- We created a rating system for ISP Networks to see if we can predict from whom we are getting DDOS traffic.. the Naughty Rating.
  - See RIPE72 archive presentation : https://ripe72.ripe.net/archives/video/116/

- We rebuild the backend for it, it now has an API.
  - And yes you can request a user-id if you like to get access to it.

Intro

- Amplification DDOS attacks are still an issue these days..
  - NTP, DNS, SSDP, Chargen, SNMP, Memcached etc
- The same networks are still the largest DDOS years ago …
- DDOS stresser sites are still present. But as fa the real issue ... Hunting them is just “whack a



Some applications are worse than others

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—

Source: https://www.us-cert.gov/ncas/alerts/TA14-017A

We are our own biggest issue …

SHODAN port:123

Exploits | Maps | Share Search | Downloa

TOTAL RESULTS

10,718,931

TOP COUNTRIES

United States	1,985,759
China	1,949,835
Italy	1,239,259
Russian Federation	519,680
Germany	461,680

TOP ORGANIZATIONS

Telecom Italia	743,567
Hangzhou Alibaba Advertising Co.,Ltd.	216,588
Telecom Italia Business	215,832
Korea Telecom	159,751
China Telecom jiangsu	130,381

SHODAN port:53

Exploits | Maps | Images | Share Search

TOTAL RESULTS

11,719,203

TOP COUNTRIES

China	2,696,070
United States	2,318,540
Brazil	547,856
Taiwan	424,071
Russian Federation	418,801

TOP ORGANIZATIONS

HiNet	385,575
Vodafone Spain	335,755
HEXIE Information technology Co.	221,911
OVH SAS	190,577
Turk Telekom	173,565

SHODAN port:11211

Exploits | Maps | Like 18 | Download Re

TOTAL RESULTS

58,782

TOP COUNTRIES

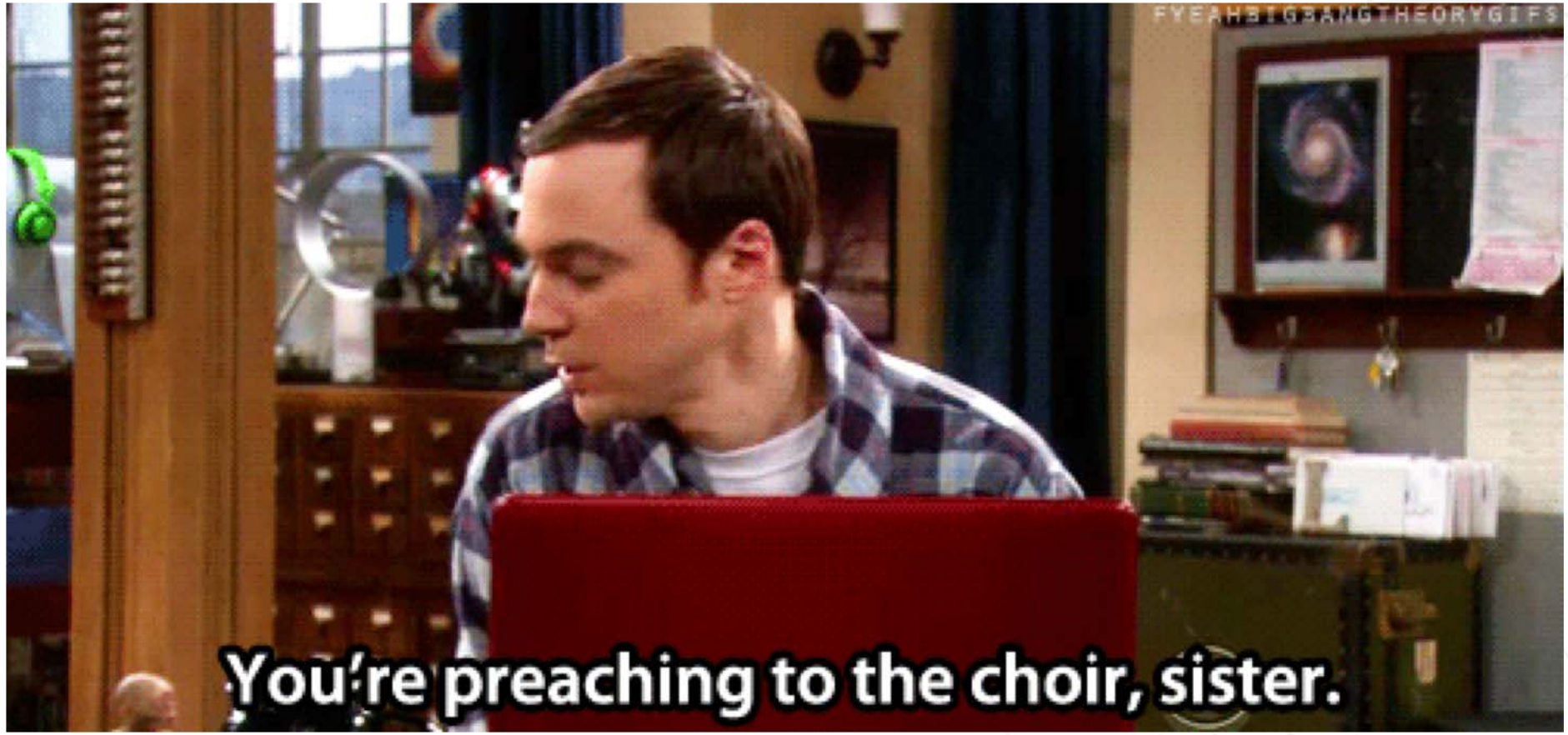
United States	16,670
China	16,487
France	2,306
Netherlands	2,188
Russian Federation	1,727

TOP ORGANIZATIONS

Hangzhou Alibaba Advertising Co.,Ltd.	6,335
Enzu	1,827
OVH SAS	1,803
CloudRadium L.L.C	1,694
Amazon.com	1,672

A2B Internet

So what are we doing here ?



Top Naughty Rating based on EPF 2017 attendees

asn	naughty_rating	ips
31500	73.02023655	9216
20764	42.56748968	13568
50324	37.04549632	8704
27796	21.37901563	12800
63949	19.51937611	506624
47232	17.37853516	20480
38001	14.80267094	29952
12714	13.75894502	1387264
31287	13.63963995	29440
29208	13.18456215	263424

Number 10 is the first network actually to be a regular RIPE meeting visitor … looking on last 8 RIPE meetings

Some of ‘us’ are more “Naughty” than others..

API Root / ASN List / ASN Instance

ASN Instance

```
GET /api/asns/3320/
```

```
HTTP 200 OK
Allow: GET, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "asn": 3320,
    "name": "DTAG",
    "set": "",
    "descr": "Internet service provider operations",
    "org": "https://naughty.a2b-internet.com/api/organiza
    "naughty_rating": 0.768243860851253,
    "ip_space_count": 36286464,
    "vulnerabilities": {
        "qotd": 39,
        "mdns": 2093,
        "ntp": 45553,
        "char_gen": 52,
        "snmp": 2829,
        "portmap": 2002,
        "telnet": 17728,
        "dns": 4191,
        "ssdp": 2547,
        "memcached": 2,
        "netbios": 4343
    }
}
```

API Root / ASN List / ASN Instance

ASN Instance

```
GET /api/asns/6830/
```

```
HTTP 200 OK
Allow: GET, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "asn": 6830,
    "name": "LGI-UPC",
    "set": "",
    "descr": "
    "org": "https://naughty.a2b-internet.com/api/
    "naughty_rating": 0.340432886485767,
    "ip_space_count": 22366464,
    "vulnerabilities": {
        "qotd": 49,
        "mdns": 4094,
        "ntp": 7906,
        "char_gen": 1,
        "snmp": 4248,
        "portmap": 4665,
        "telnet": 8824,
        "dns": 4219,
        "ssdp": 18,
        "memcached": 11,
        "netbios": 1496
    }
}
```

API Root / ASN List / ASN Instance

ASN Instance

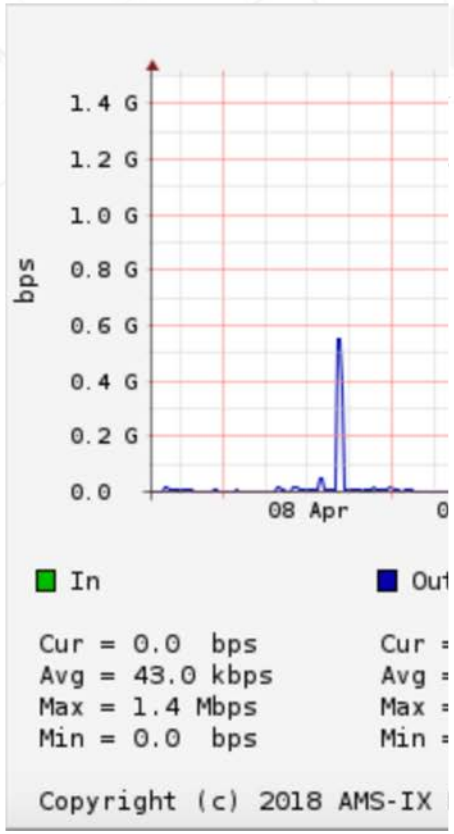
```
GET /api/asns/8708/
```

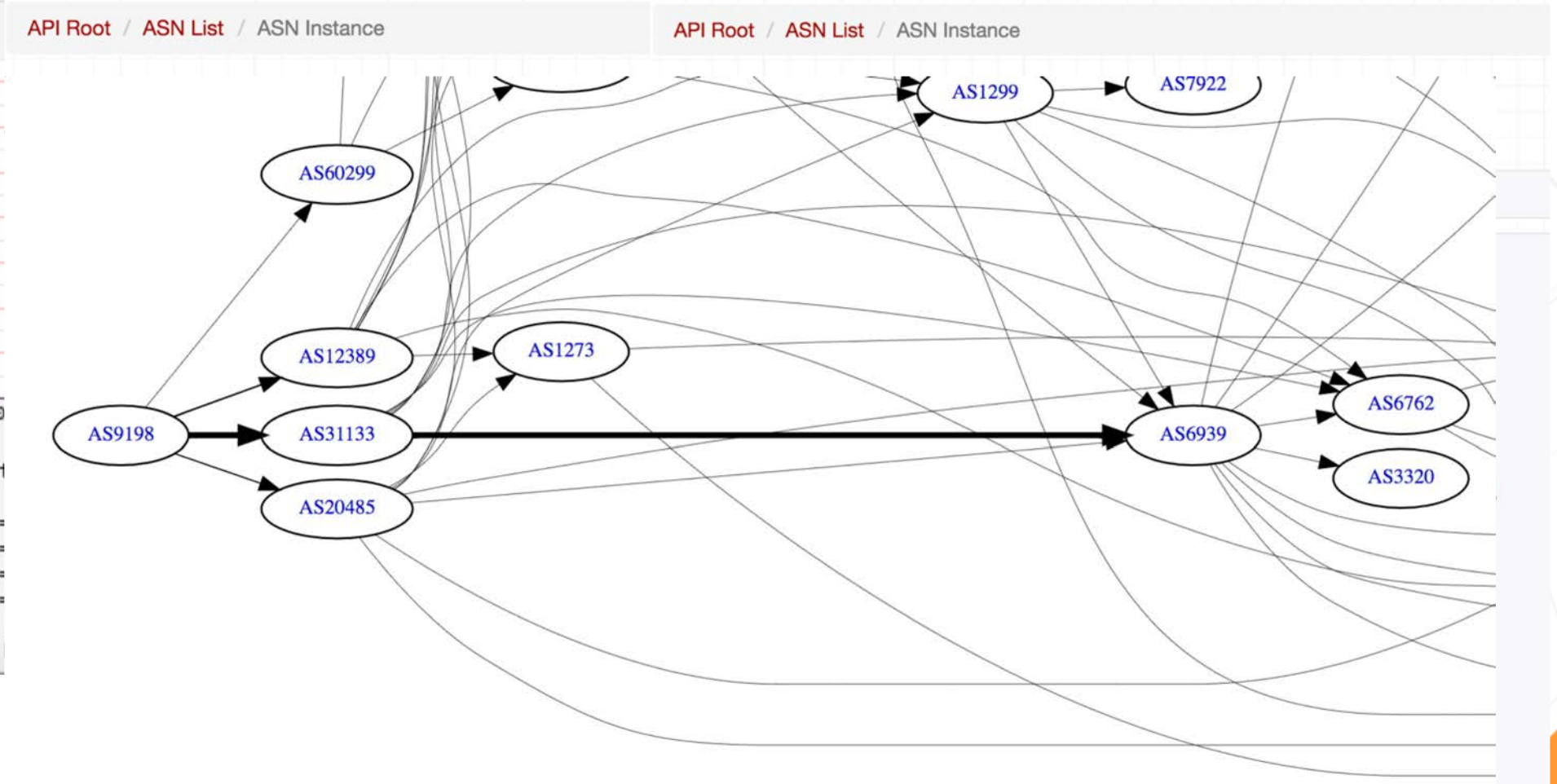
```
HTTP 200 OK
Allow: GET, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "asn": 8708,
    "name": "RCS-RDS",
    "set": "",
    "descr": "Bucharest, ROMANIA",
    "org": "https://naughty.a2b-internet.com/api/organizations/ORG-RA18-RIPE/",
    "naughty_rating": 2.75277078880724,
    "ip_space_count": 2185984,
    "vulnerabilities": {
        "qotd": 13,
        "mdns": 697,
        "ntp": 4029,
        "char_gen": 10,
        "snmp": 939,
        "portmap": 1838,
        "telnet": 51559,
        "dns": 29077,
        "ssdp": 29075,
        "memcached": 15,
        "netbios": 1786
    }
}
```

A2B Internet

Weird results in Sflow vs API or counts …





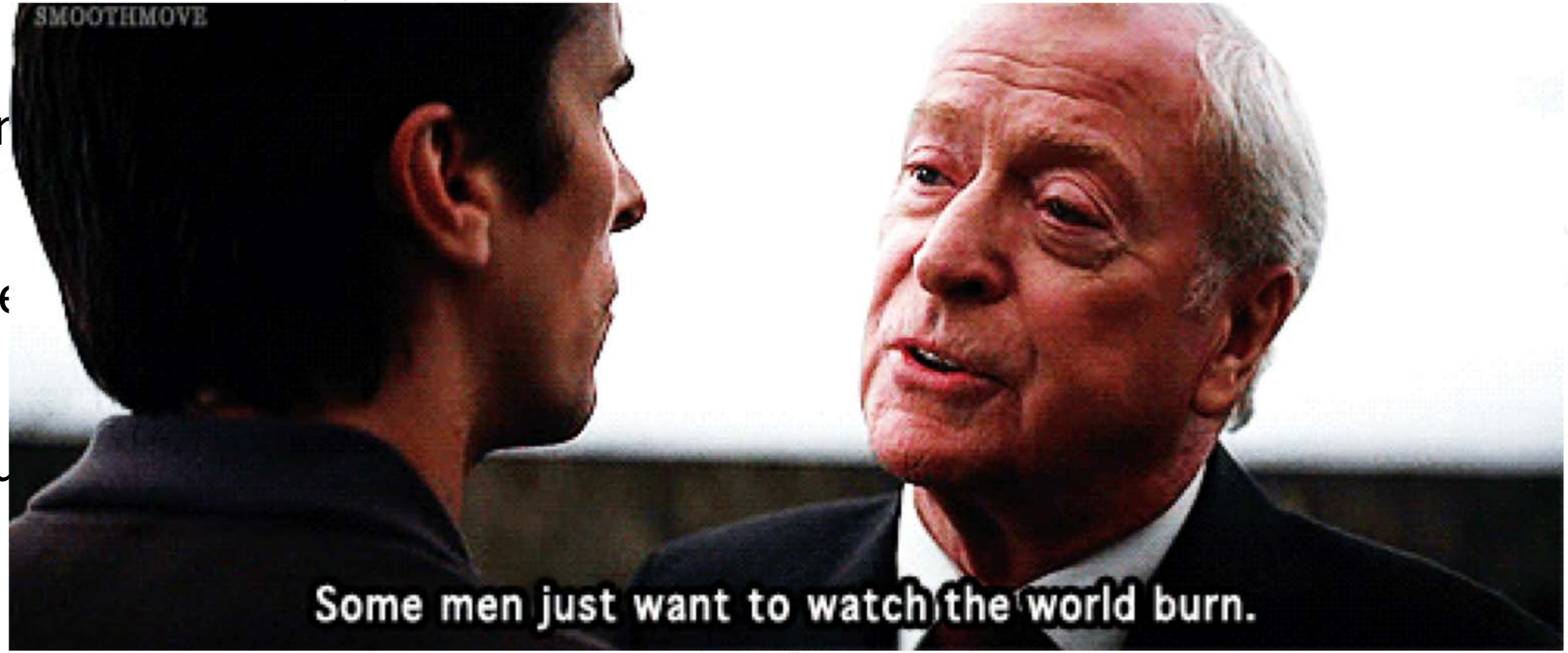
A2B Internet

So, are you afraid yet of …

- your own paying (unhappy) customers
- or
- Are you waiting to fix your shizzle, until capability in your own network against

Or do you have shares in …

- Other cor
- Companie
- Or do you



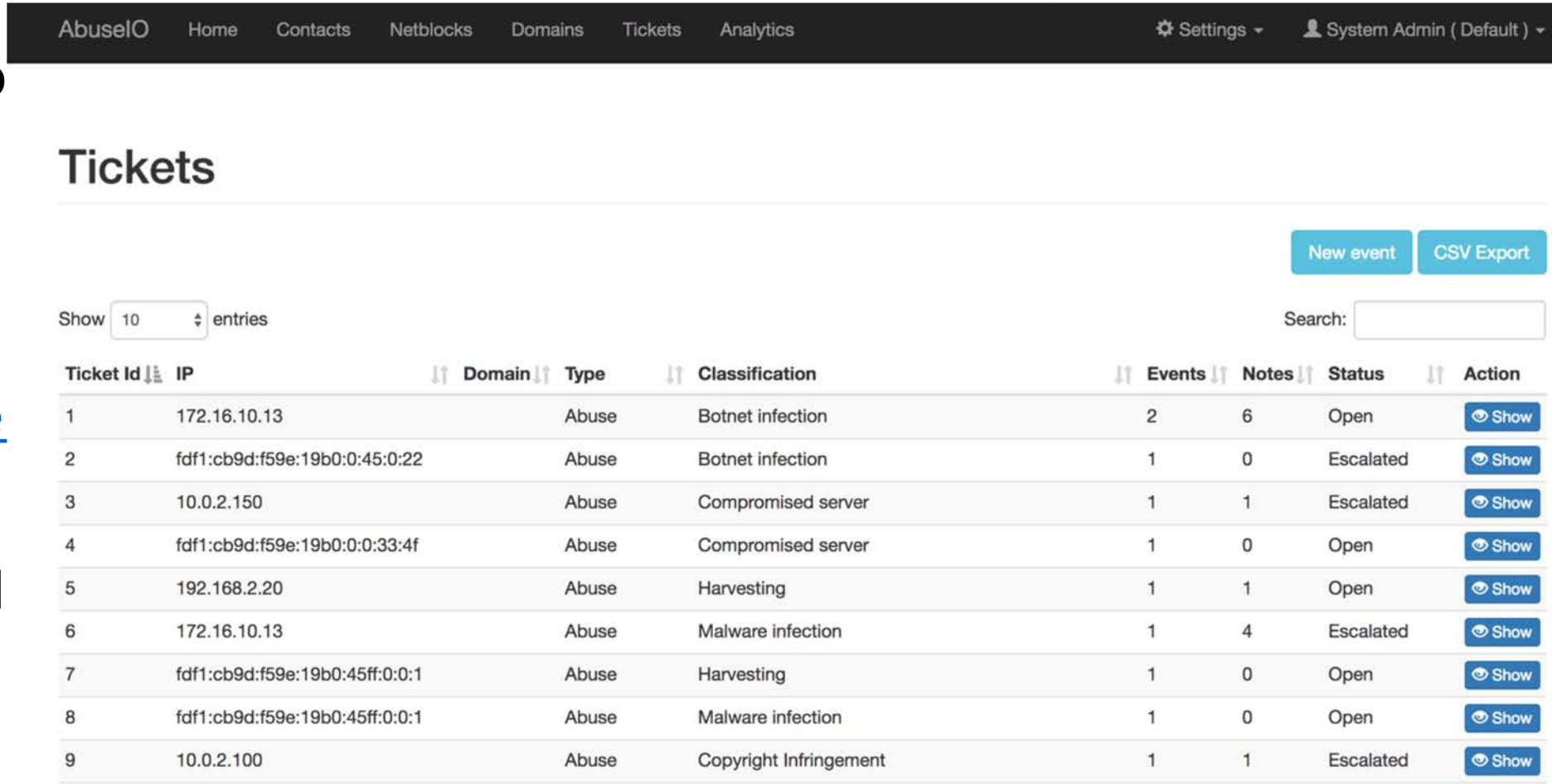
A2B Internet

Time for action from you …

- Administrate all your IP’s and customers in an IPAM ..
  - Like nipap or Digital Ocean’s Netbox (Both open source)
- Use a single source for your IP’s and customers email addresses.
  - Several solutions possible to link your customer debit number to your IPAM and have a contact mail address. This isn’t hard to fix ..
- And then …

Automate your abuse-feeds !!

- Install abuse.io
- Get your feeds
  - https://abuse
- Link it to your I



A2B Internet

See it then process feeds from ….

- Shadowserver.org
- Clean-mx.de
- Spamcop
- Spamexperts
- WebIron
- Google Safe Browsing
- Any RFC compliant ARF formatted msg.
- Any RFC compliant FBL Messages (Feedback Loop)
- Any DNS based RBL
- Netcraft
- Project Honeypot

- And many more !! And more to come …

What is the result ?

- Happy customers …
- Happy managers …
- Happy peers …
- Everybody wins …

Questions ?