State of BGP Security

Alexander Azimov <aa@qrator.net>

Not a Long Time Ago…

In a galaxy that is already far away…

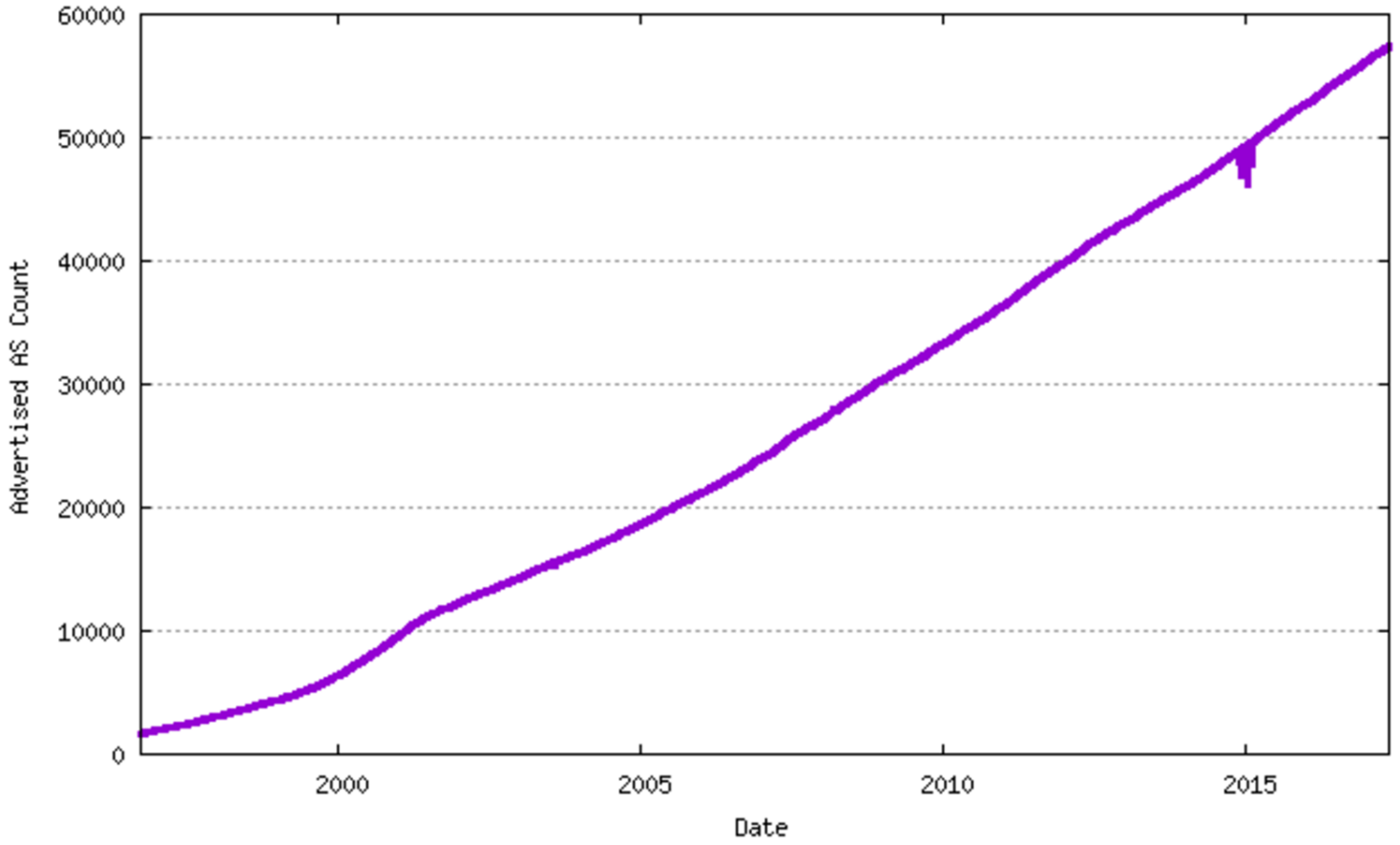
Was invented inter-domain routing protocol BGP

BGP: Key Principles

BGP: Key Principles

- Absence of hierarchy;
- Openness;
- Mutual respect;
- Flexibility;

Advertised AS Count

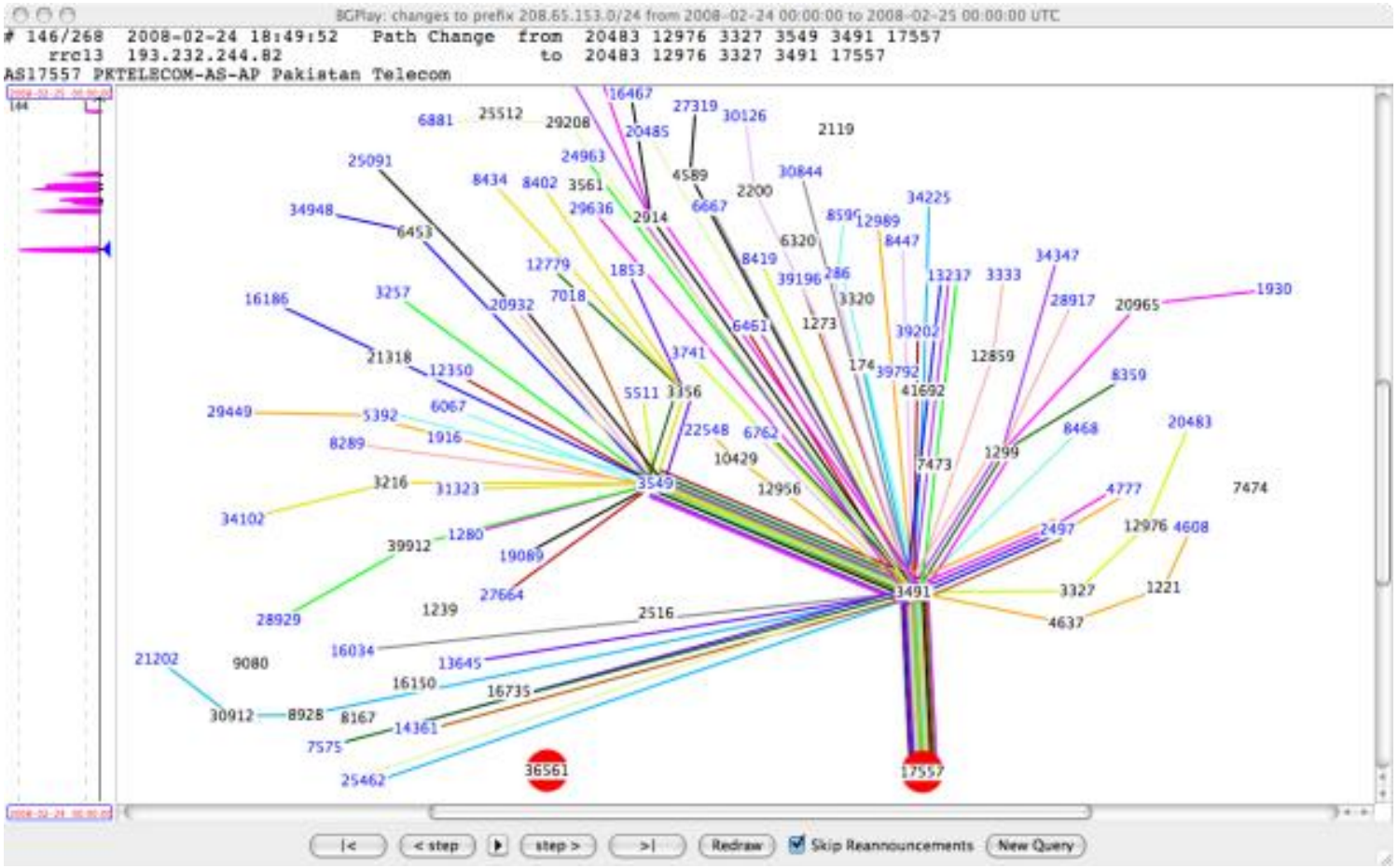


Source: http://www.potaroo.net/tools/asn32/

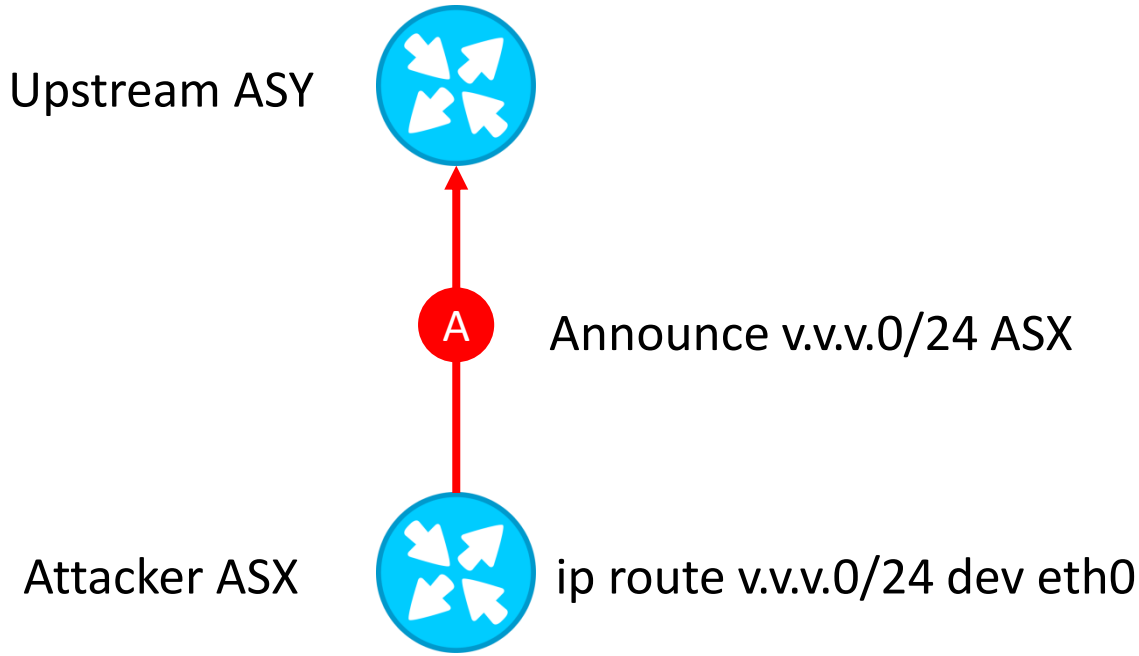
Consequences

- Hijacks
- Route Leaks
- Bogons

Hijacks: Youtube



Leak Of Static Routes

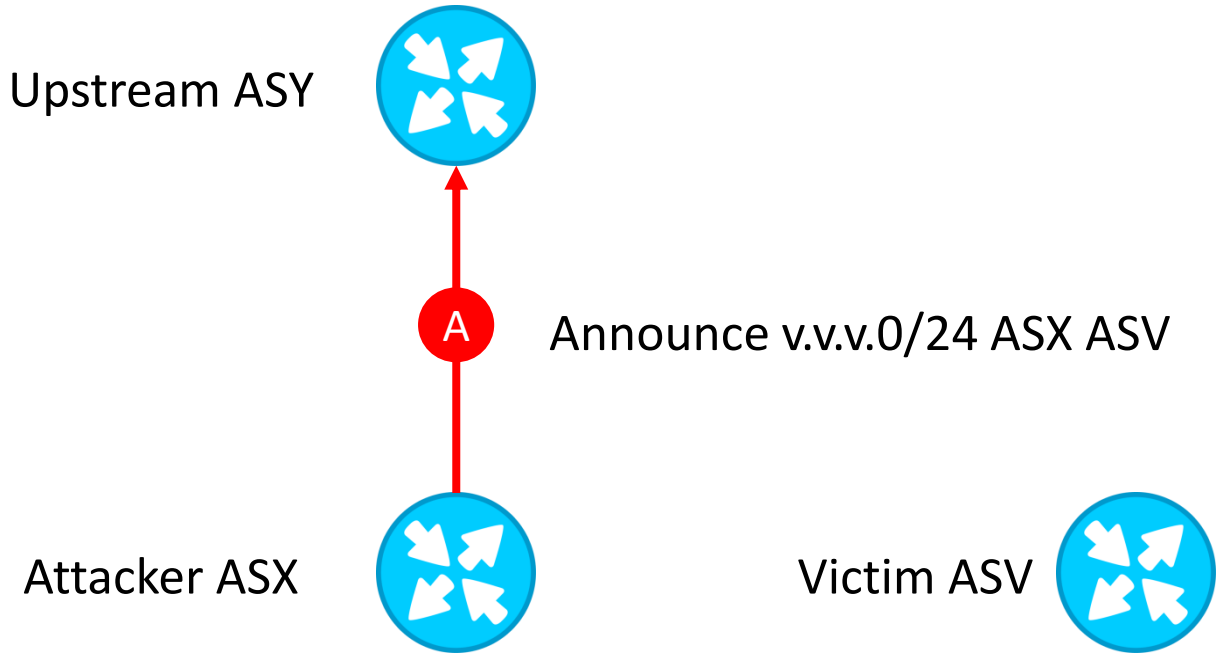


Route Objects / RPKI

route: 178.248.232.0/23
descr: "HLL" LLC
origin: AS197068
mnt-by: MNT-QRATOR
created: 2012-11-22T21:07:45Z
last-modified: 2012-11-22T21:07:45Z
source: RIPE # Filtered

Origin validation, but does it enough?

Hijacks: Bypass of Origin Validation



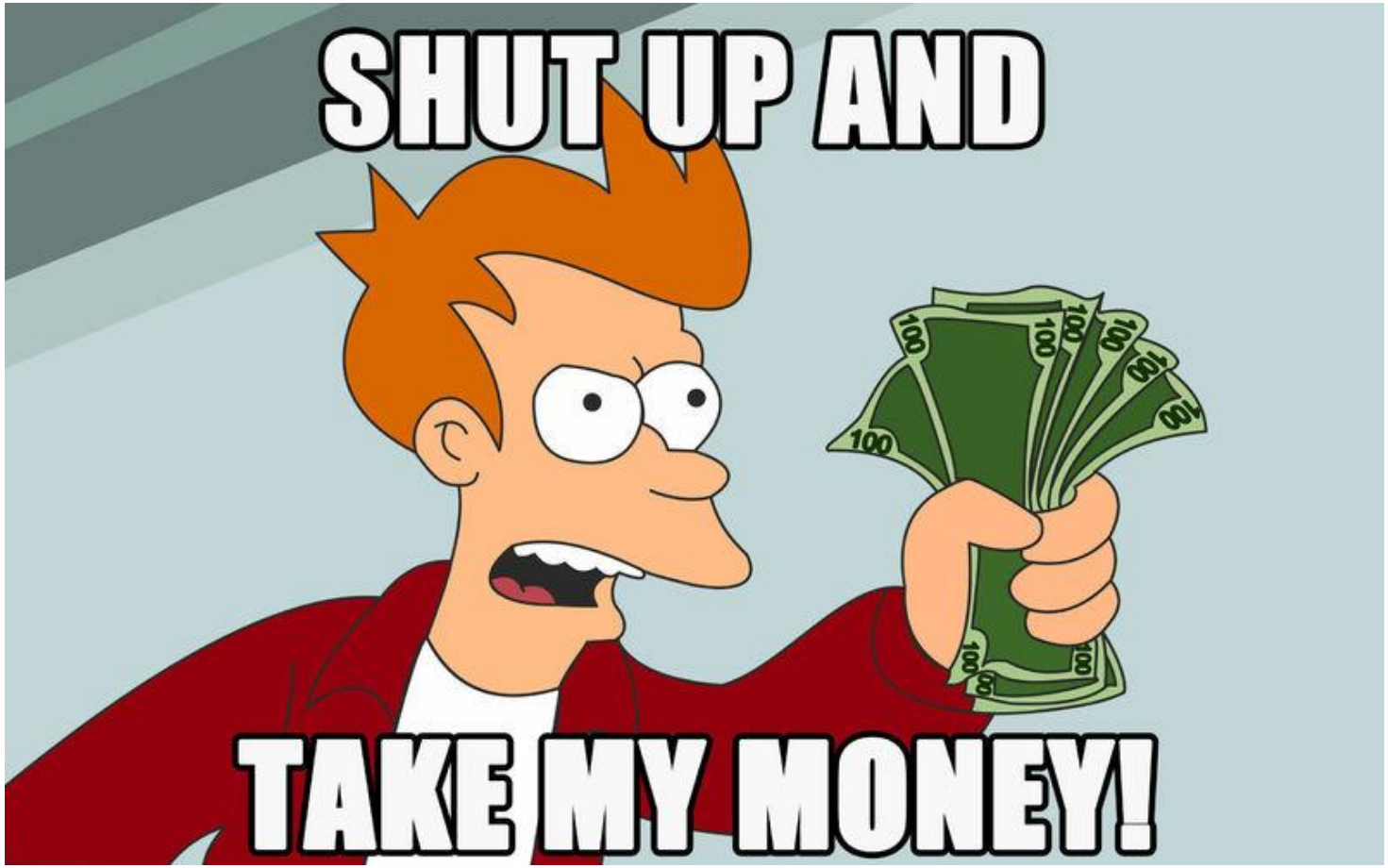
Add ASV to AS-SET o copy its record

Filtering & Regulation

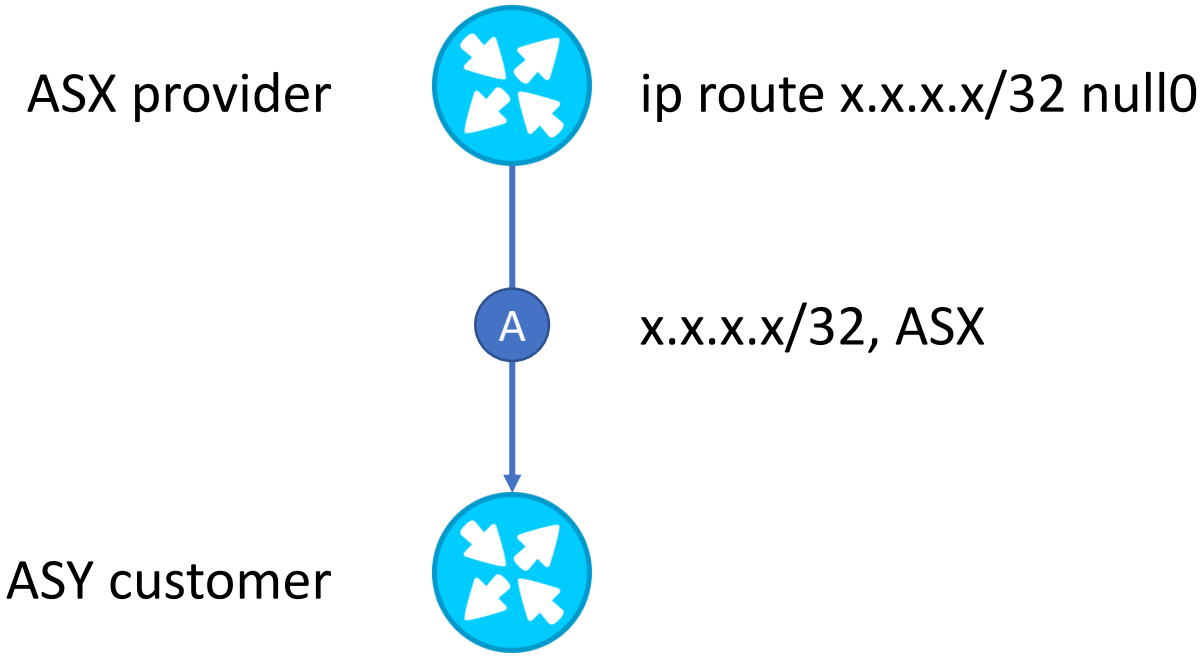
Implementing Regulation: Common Practice

- Null route;
- ACL;
- Different types of resets;
- DNS spoof;
- and…. hijacks!

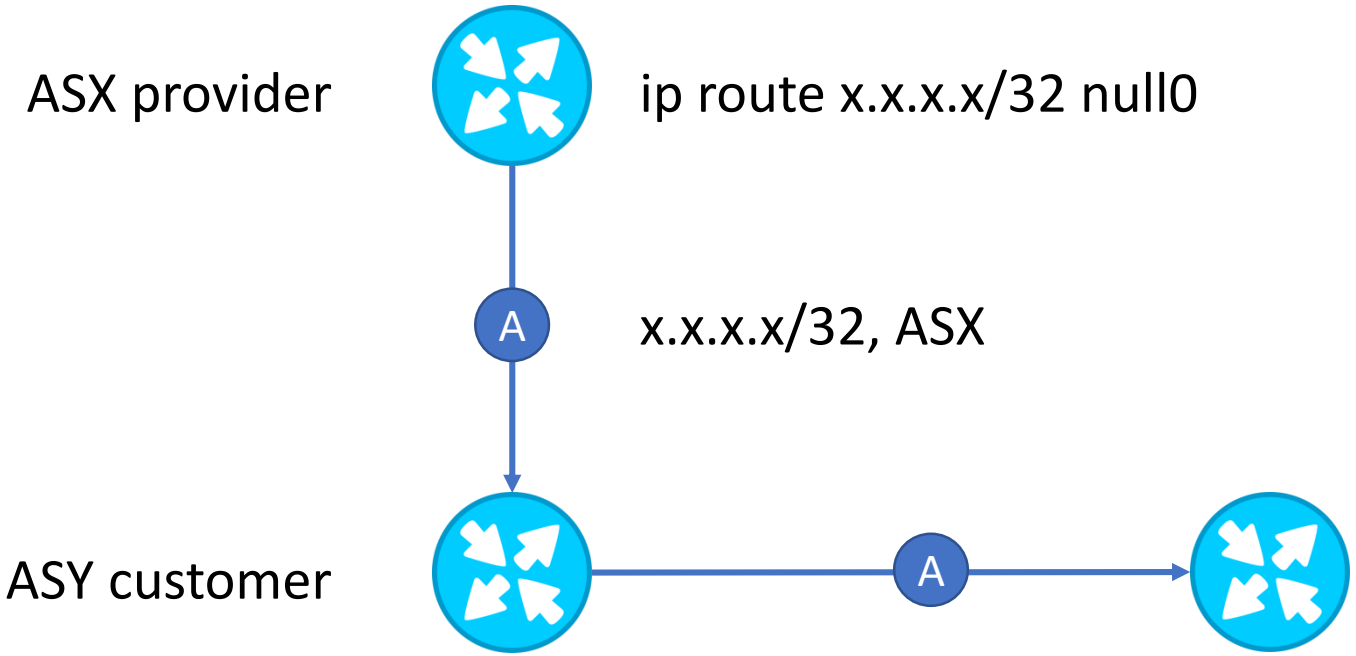
Hijack as a Service



Hijack as a Service

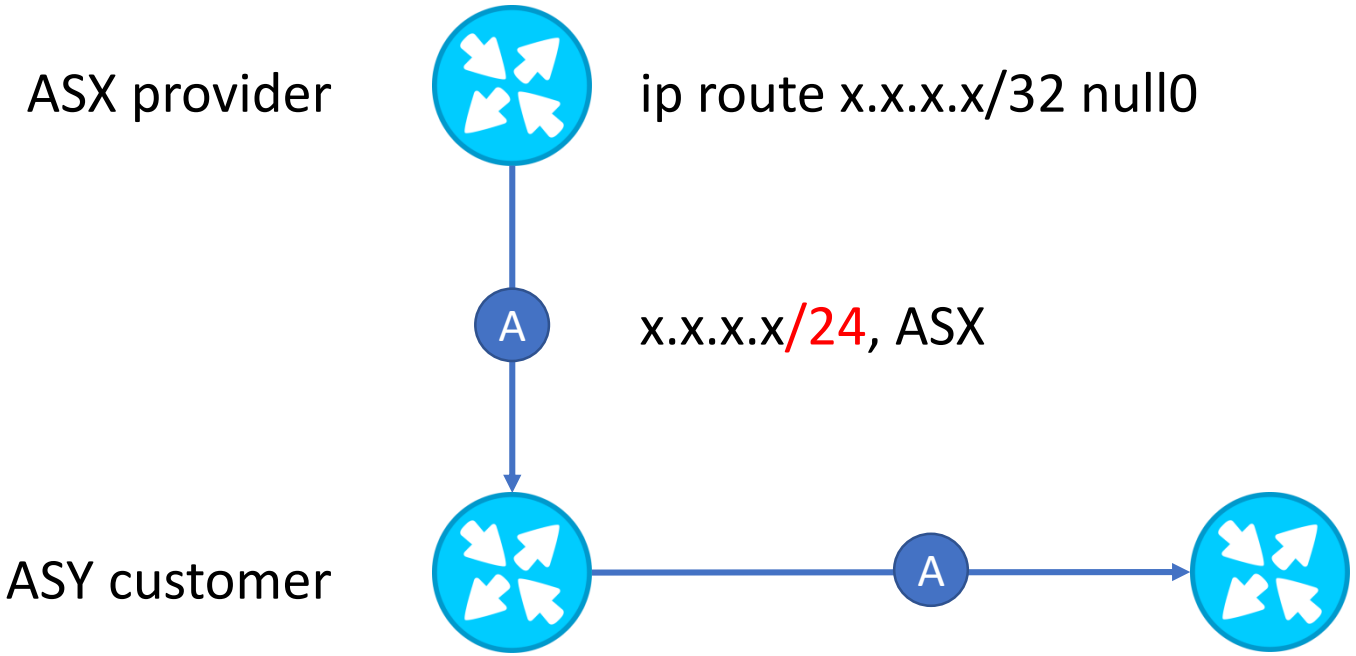


Hijack as a Service



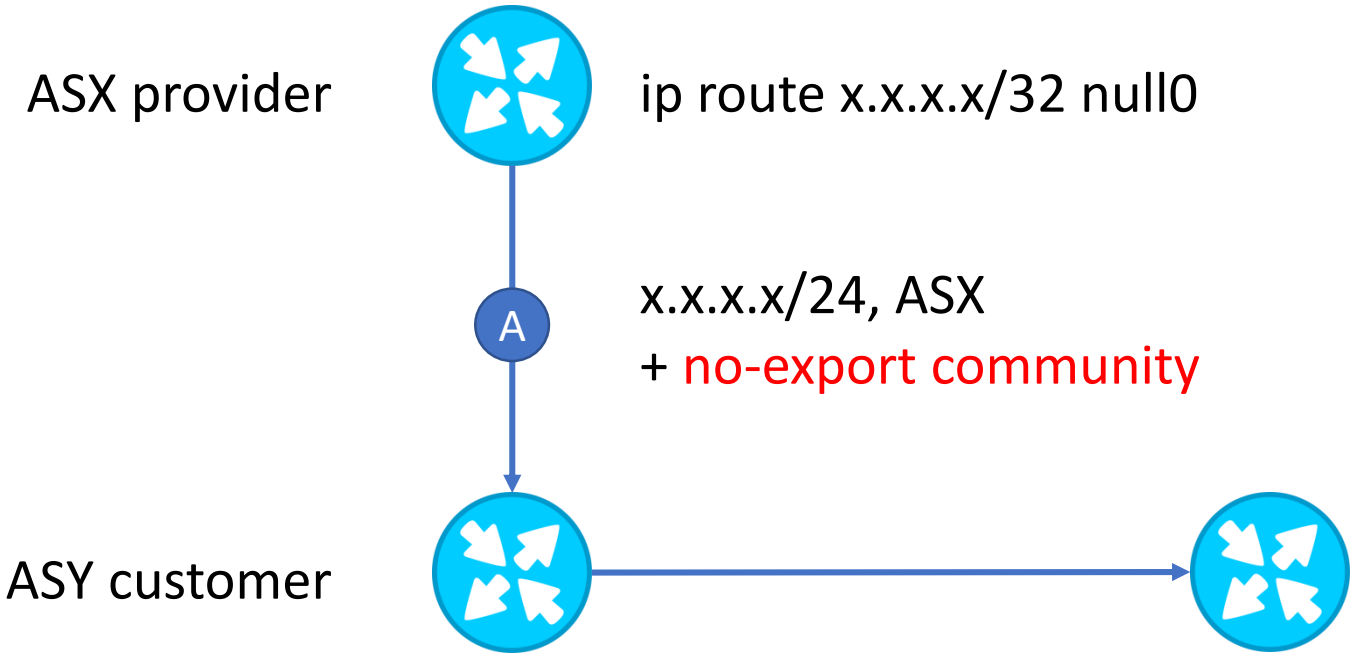
In case of route leak, can result in global problems.

Hijack as a Service



In case of route leak, can result in global problems.

Hijack as a Service



At least no unpredictable consequences

Consequences

- Hijacks

DoS, hijack as a service, mistakes

- Route Leaks

- Bogons

Route Leaks

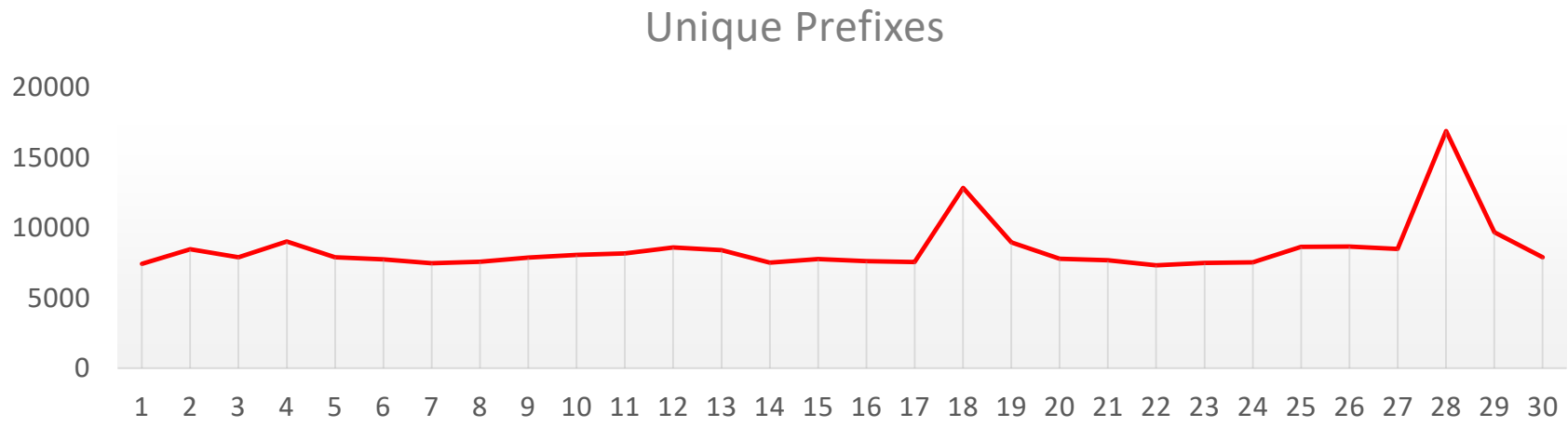
Route Leaks are propagation of BGP prefixes which violate assumptions of BGP topology relationships; e.g. passing a route learned from one peer to another peer or to a transit provider, passing a route learned from one transit provider to another transit provider or to a peer.

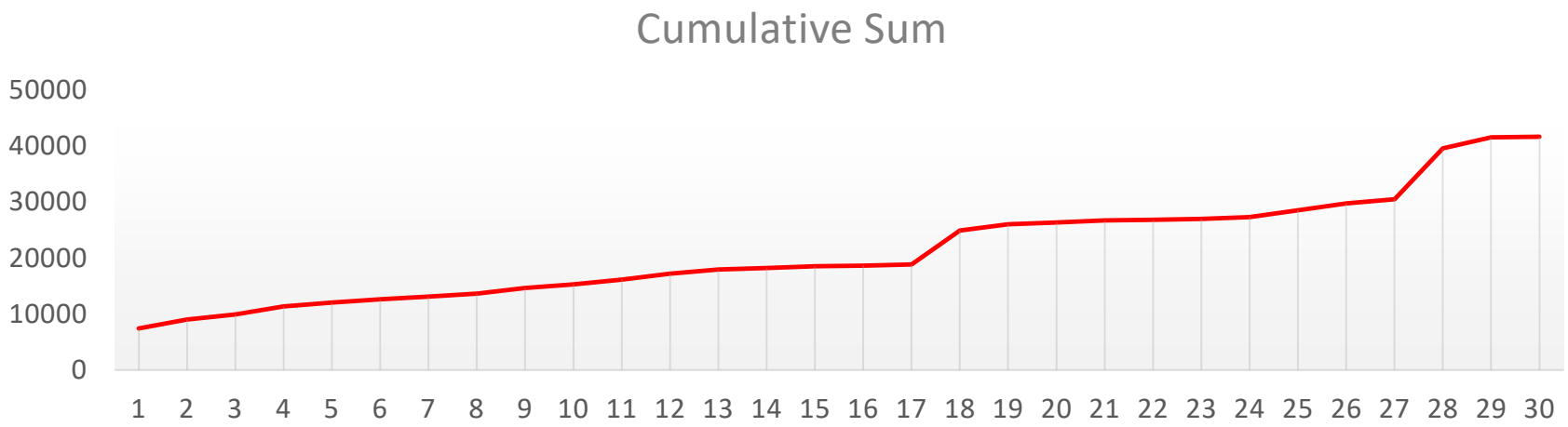
Leaked Prefixes

If your prefixes are leaked:

1. Increased delays;
2. DoS;
3. MiTM attack.

Leaked Prefixes



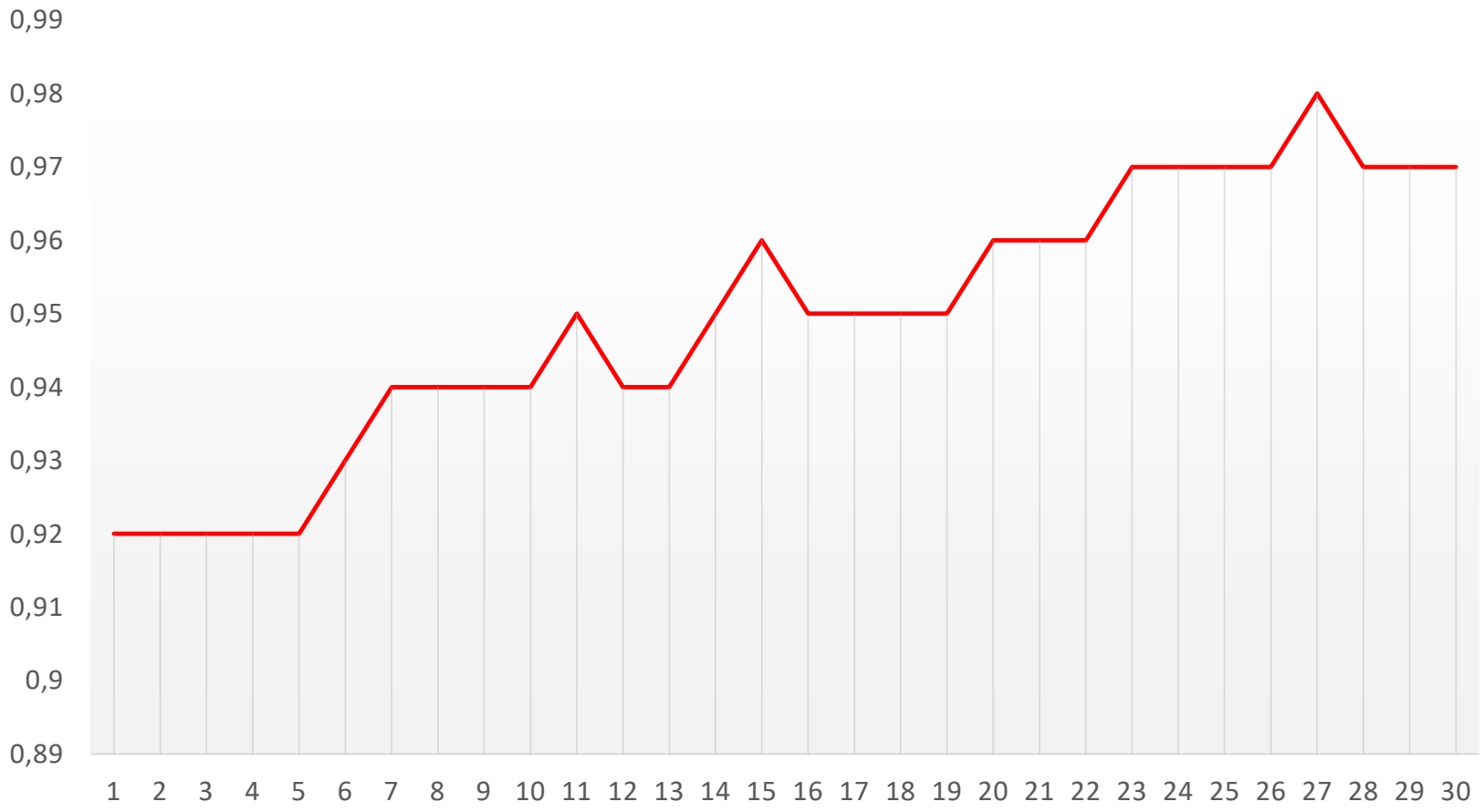


Accepting Leaked Prefixes

If your AS accepts leaked prefixes:

1. Increased delays;
2. DoS;
3. MiTM attack.

Accepting Leaked Prefixes

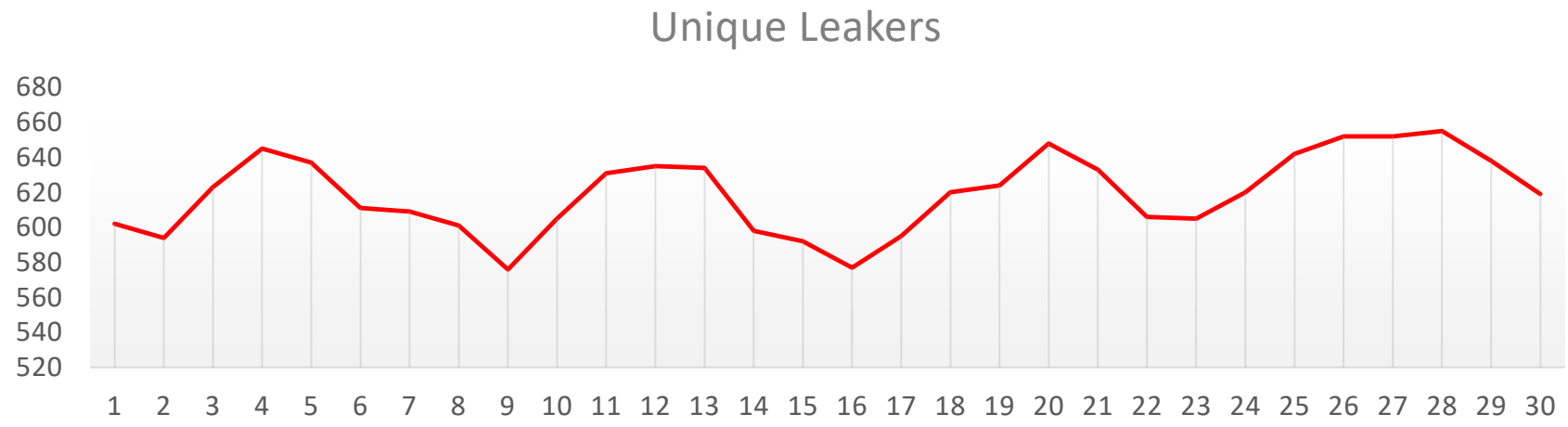


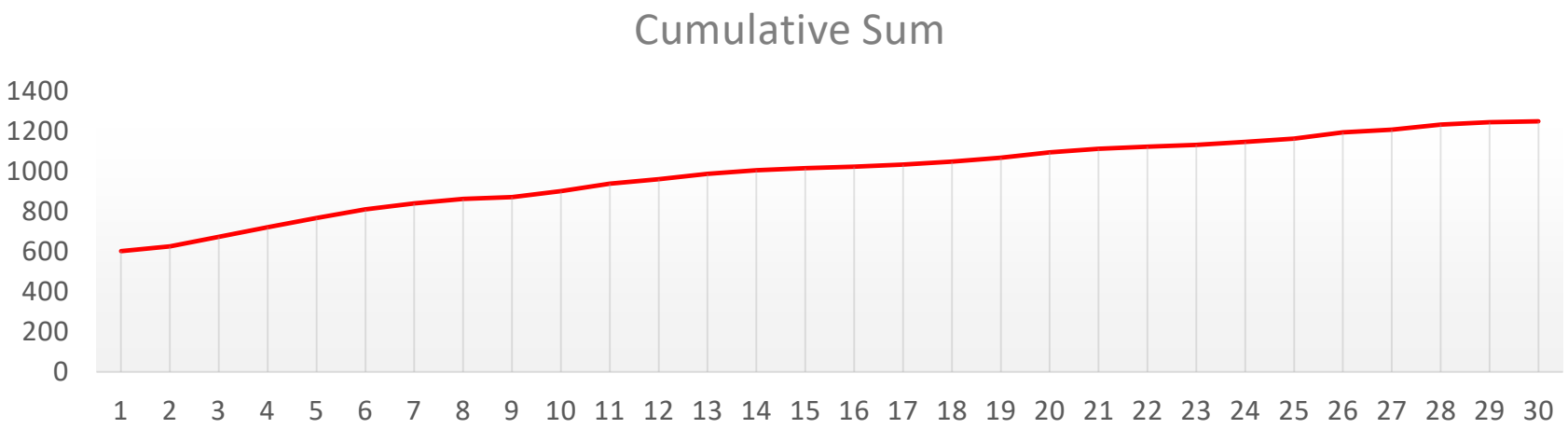
Leakers

If your AS leaks prefixes:

1. DoS attack, was it your goal?
2. MiTM attack, was it your goal?
3. If not, money loss, packet loss, reputation loss.

Leakers


Unique Leakers
680
660
640
620
600
580
560
540
520
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30


Cumulative Sum
1400
1200
1000
800
600
400
200
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Consequences

- Hijacks

DoS, hijack as a service, mistakes

- Route Leaks

MiTM, mistakes

- Bogons

Bogon Prefixes

```
IPv4: [
    ('0.0.0.0/8', 'this'),
    ('10.0.0.0/8', 'private'),
    ('100.64.0.0/10', 'shared'),
    ('127.0.0.0/8', 'loopback'),
    ('169.254.0.0/16', 'link-local'),
    ('172.16.0.0/12', 'private'),
    ('192.0.0.0/24', 'ietf'),
    ('192.0.2.0/24', 'test-net-1'),
    ('192.88.99.0/24', '6to4'),
    ('192.168.0.0/16', 'private'),
    ('198.18.0.0/15', 'testing'),
    ('198.51.100.0/24', 'test-net-2'),
    ('203.0.113.0/24', 'test-net-3'),
    ('224.0.0.0/4', 'multicast'),
    ('240.0.0.0/4', 'reserved'),
    ('255.255.255.255/32', 'broadcast'),
]
```

```
IPv6: [
    ('::/128', 'unspecified'),
    ('::1/128', 'loopback'),
    ('::ffff:0:0/96', 'ipv4-mapped'),
    ('::/96', 'ipv4-compatible'),
    ('100::/64', 'blackhole'),
    ('2001:10::/28', 'orchid'),
    ('2001:db8::/32', 'documentation'),
    ('fc00::/7', 'ula'),
    ('fe80::/10', 'link-local'),
    ('fec0::/10', 'site-local'),
    ('ff00::/8', 'multicast')
 ]
```

Bogon ASNs

asn == 0 or

asn == 23456 or

64512 <= asn <= 131071 or

4200000000 <= asn <= 4294967294

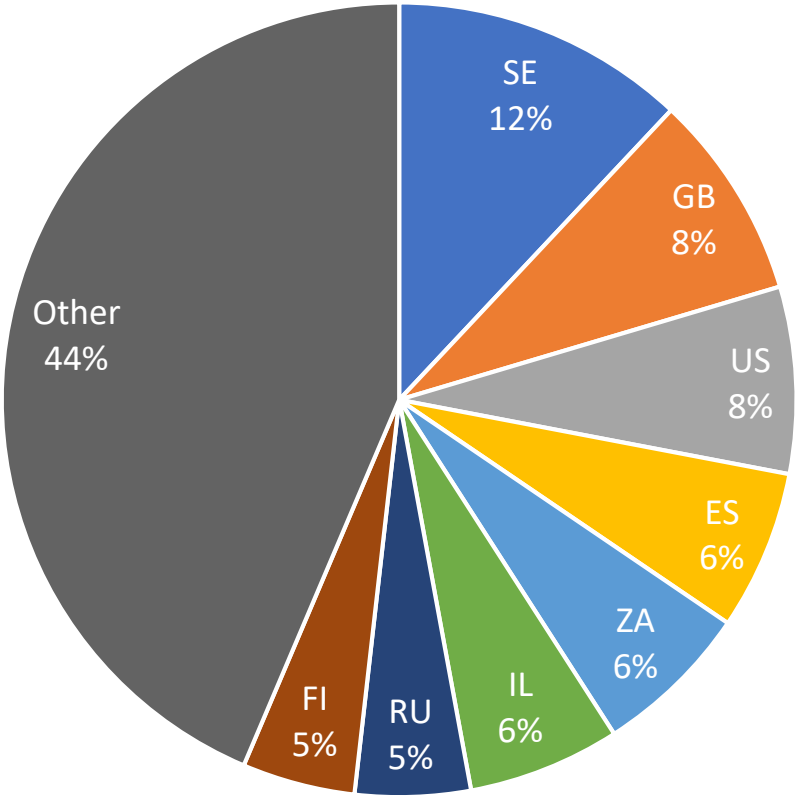
Bogon ASNs: Crusade

On Tue, Jun 14, 2016 at 04:51:40PM +0300, Alexander Azimov wrote:
> But I have security consideration that filtering isn't a proper mechanism
> to reach this goal. Imagine next situation - if transit accidently prepends
> its paths with private AS number it will result in DoS for all stub
> networks connected to this transit.

This is good. A transit ISP stupid enough to make such mistakes need
to pay in blood and money.

Bogon ASNs: Statistics

More then >12000 prefixes are affected



Consequences

- Hijacks

DoS, hijack as a service, mistakes

- Route Leaks

MiTM, mistakes

- Bogons

DoS, mistakes

Monitoring

- BGPStream + Caida AS Relations;
- DYN/Renesys;
- BGPMon;
- Radar by Qrator.

Consequences

- Hijacks

DoS, hijack as a service, mistakes

- Route Leaks

MiTM, mistakes

- Bogons

DoS, mistakes

IETF: Key Principles

- Absence of hierarchy;
- Openness;
- Mutual respect;
- Flexibility;

Qrator Initiatives

BGP Roles with automation of route leak prevention and detection

initiatives.qrator.net/details/route-leak-mitigation

ASN Union

initiatives.qrator.net/details/asn-union

Instruction

Read the draft:
datatracker.ietf.org/doc/draft-ymbk-idr-bgp-open-policy

Read the thread:
ietf.org/mail-archive/web/idr/current/msg18149.html

Vote:

1. Subscribe to IETF mailing list ietf.org/mailman/listinfo/idr;
2. Share your support or objectives at mailing list idr@ietf.org;

Summary

- If you are providing SaaS hijacks – at least use no-export communities;
- If you need reachability/availability of you services – you should monitor your prefixes;
- Collaborate with IETF!
- Visit init.qrator.net for more details.