
WELCOME
TO Fabulous
LAS VEGAS
NEVADA
copyright 1999 philg@mit.edu

July 31st – August 2nd 2008


A couple of months ago in Las Vegas …
T.Kapela
A.Pilosov

Pirates of the Internet

Blackholing, Hijacking and other nasty tricks

Carlos Fragoso Mariscal

CESCA

Pirates of the Internet

- Internet & BGP 101
- Attacks
- Countermeasures

Pirates of the Internet

- **Internet & BGP 101**
  - How it works
  - Threats
- Attacks
- Countermeasures


Allocated
Unallocated
Internet Land ☺ …
LOCAL
PUBLIC DATA NETS
HP
DEC
FORD
CSC
DDN-RVN
GENERAL ELECTRIC
XEROX
BELL LABS
APPLE
MIT
DISA
BBN INC
DoD INTEL
CABLE TV
UK MoD
ARMY AISC
IBM
VPNs
DSI
SITA
MERC
CAP DEBIS CCS
NORSK
MERIT
USPS
BOEING
duPONT
DLA
HALLIBURTON
PSI
UK SOCIAL SECURITY
INTEROP
ELI LILY
ARINC
PRUDENTIAL
BELL NORTH
HAM RADIO
JAPAN INET
MULTICAST
ASIA-PACIFIC
EUROPE
NORTH AMERICA
US DEPARTMENT OF DEFENSE
JAPAN
VARIOUS
REGISTRARS
AFRICA
LATIN AMERICA & CARIBBEAN
CANADA
EUROPE (UNUSED)
AMERICA
EUROPE

Autonomous System

AS Number (ASN)

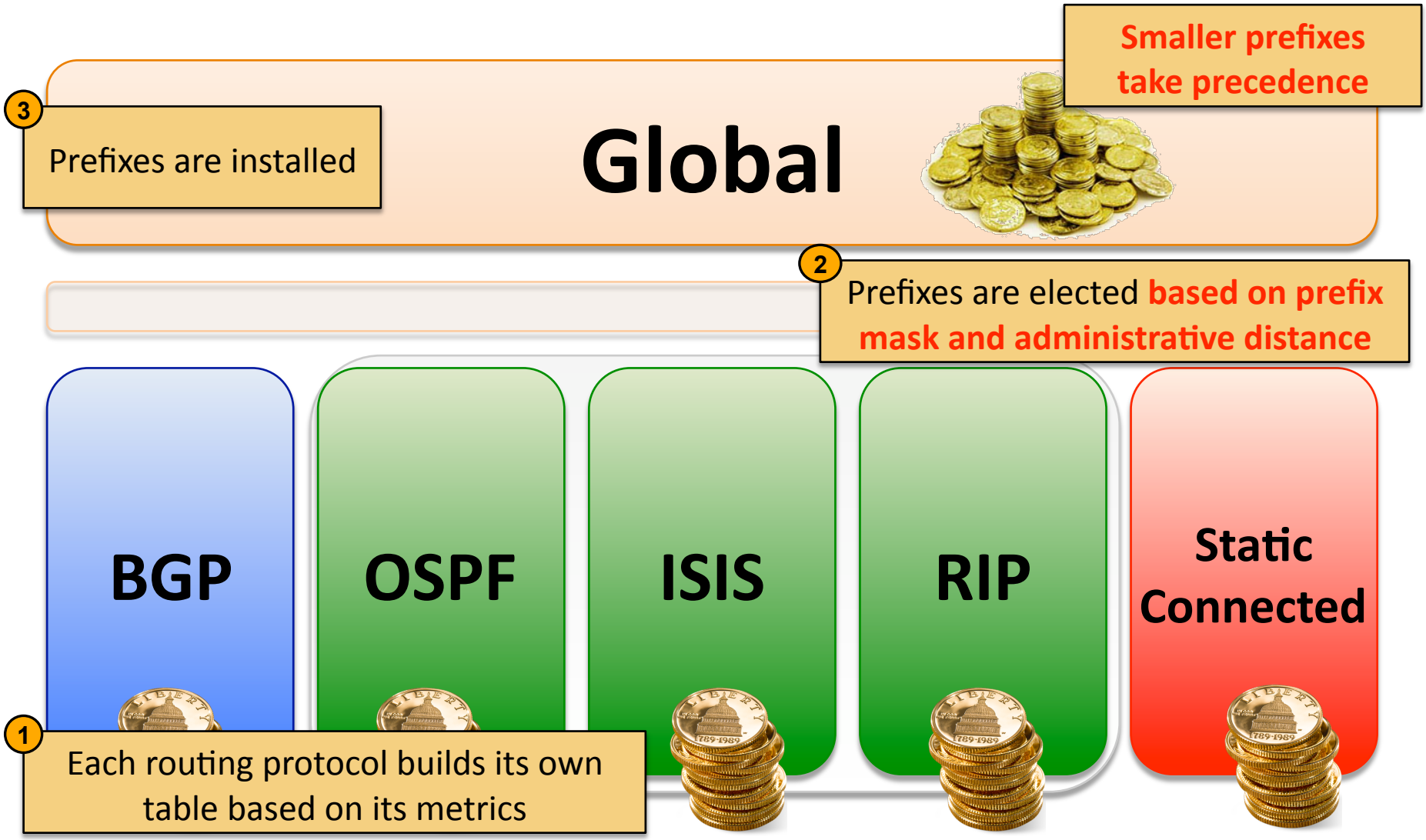
+

Network prefixes


BGPv4
RFC1771

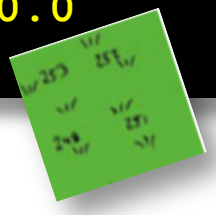
Carriers
IXP

How routing tables work ?



BGP table

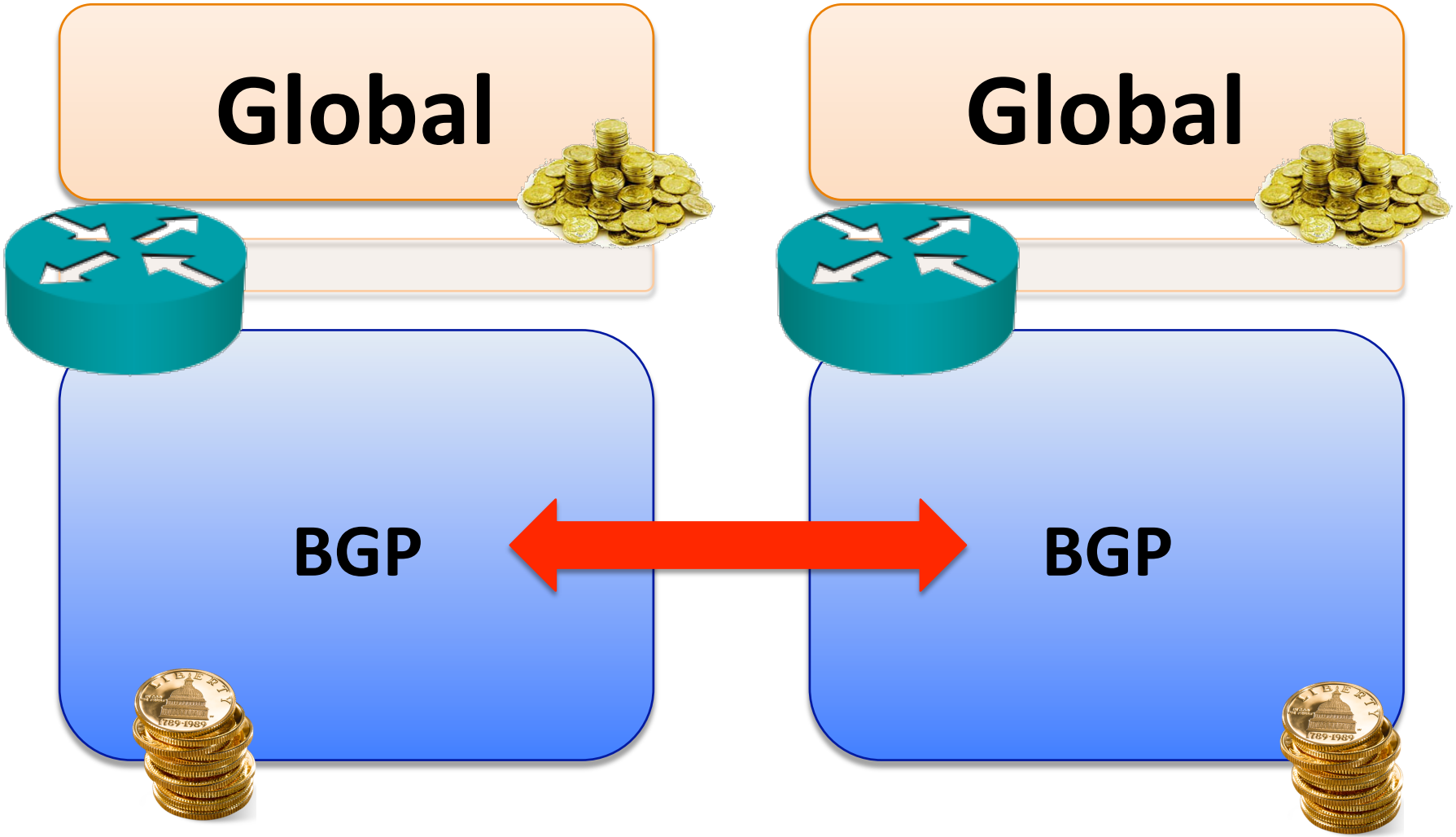
```
BGP table version is NNNNNNNN, local router ID is A.B.C.D
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  3.0.0.0          12.123.17.244            0 7018 2914 9304 80 i
*                   12.123.134.124           0 7018 2914 9304 80 i
```



Global table

```
Routing entry for 3.0.0.0/8
  Known via "bgp 65000", distance 20, metric 0
  Tag 7018, type external
  Last update from 12.123.134.124 1d00h ago
  Routing Descriptor Blocks:
  * 12.123.134.124, from 12.123.134.124, 1d00h ago
      Route metric is 0, traffic share count is 1
      AS Hops 4
      Route tag 7018
```

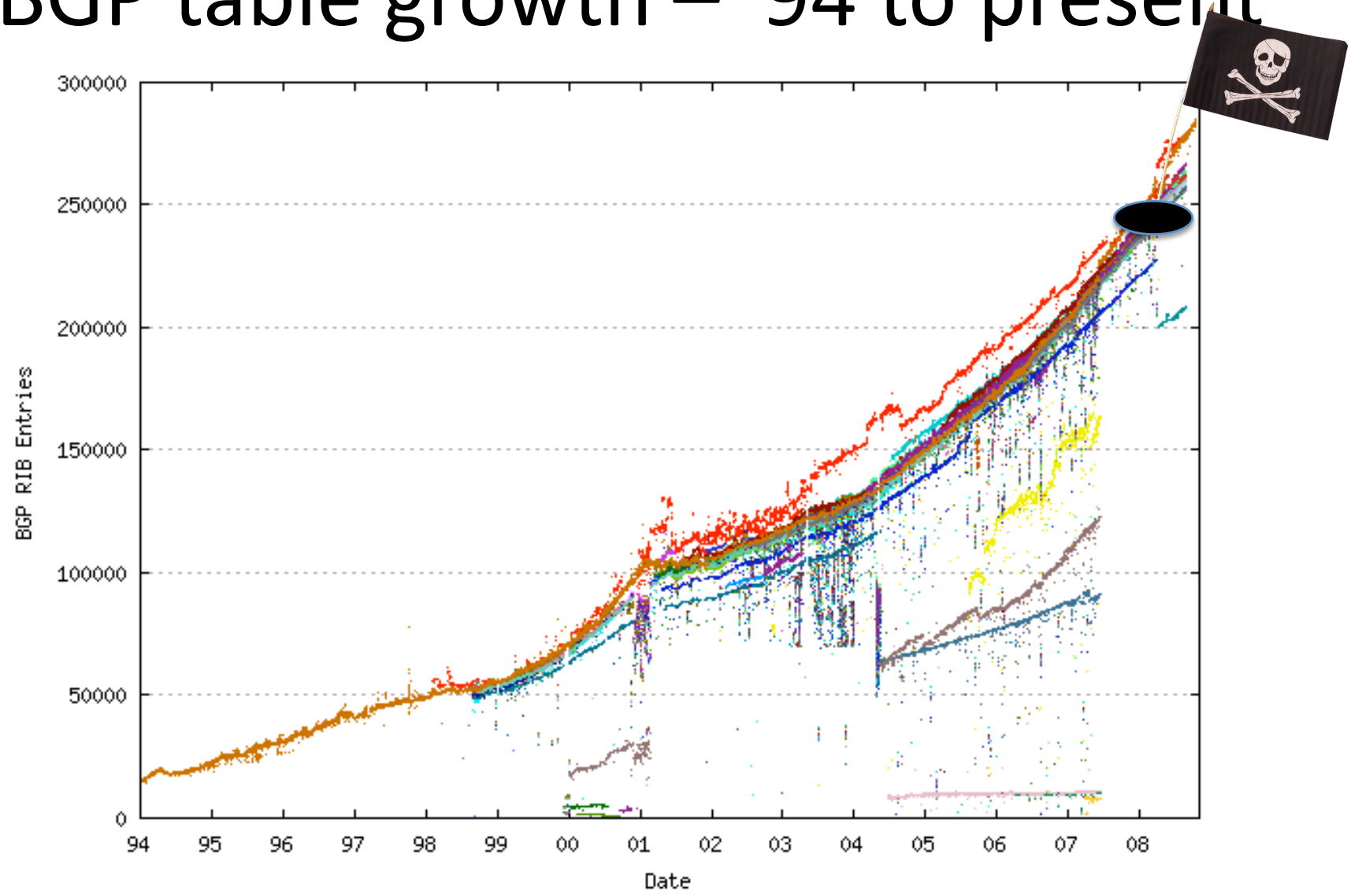
Router peering



BGP Selection Algorithm

1. Highest Local Preference
2. Locally originated, aggregated, redistribution…
3. **Shortest AS-PATH**
4. Lowest origin type
5. Lowest Multi Exit Discriminator (MED)
6. eBGP over iBGP paths
7. Lowest IGP metric to next-hop
8. Received first

BGP table growth – ‘94 to present



Source: Geoff Houston – http://www.potaroo.netº

Internet Routing Registry (IRR)

- Route registration
- Routing Policy description (RFC 2622)
- Common objects
  - route / route-set
  - aut-num / AS-Set
  - Peering-set
- Most well-known
  - RADB
  - RIPE

```
route:      84.88.0.0/16
descr:      Anella Cientifica
origin:     AS13041
mnt-by:     CESCA-MNT
source:     RIPE # Filtered
```

```
as-set:     AS-ANELLA
descr:      Anella Cientifica RREN
remarks:      --- ( ANELLA )—
members:      AS13041
remarks:      --- ( UOC )—
members:      AS15633
remarks:      --- ( CATSALUT )—
members:      AS16153
remarks:      --- ( XTEC )—
members:      AS21193
remarks:      ---( UAB-PIC )—
members:      AS43115
tech-c:     CNOC6-RIPE
admin-c:    MH3879-RIPE
mnt-by:     CESCA-MNT
source:     RIPE # Filtered
```

Source: RIPE Whois Database – http://www.ripe.net/db/whois.html

```
From: db-admin@altdb.net
To: xxx@wyltk-llc.com
ReplyTo: db-admin@altdb.net
Subject: Forwarded mail.... (fwd)
Sent: Aug 7, 2008 9:48 PM

Your transaction has been processed by the
IRRd routing registry system.

Diagnostic output:

-----------------------------------------------
----------

The submission contained the following mail
headers:

- From: xxx@wyltk-llc.com
- Subject: Forwarded mail.... (fwd)
- Date: Thu, 7 Aug 2008 21:48:53 -0400 (EDT)
- Msg-Id: <Pine.LNX.xxx@wyltk-llc.com>

ADD OK: [route] 24.120.56.0/24 AS26627


---------------------------------------
If you have any questions about ALTDB,
please send mail to db-admin@altdb.net.
```

Protect your database objects

Some threats

- Internet is a chain of trust
  - *"A chain is only as strong as its weakest link"*
- Weak peer filtering policies
- Routing infrastructure compromise
- Unauthorized route registration at IRR

Pirates of the Internet

- Internet & BGP 101
- **Attacks**
  - Blackholing
  - Hijacking
- Countermeasures

What are they looking for ?

- Money, money and money $$$$
- Control over an IP prefix allows them …
  - Spam injection
  - Extortion
  - Traffic interception (MITM)

Blackholing

- Poisoning a more specific route
  - Ex: /24 overlapping main /19
- Traffic is dropped at destination
  - Route to Null0
- Not very effective for small prefixes (</24)
  - Depends on policies

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

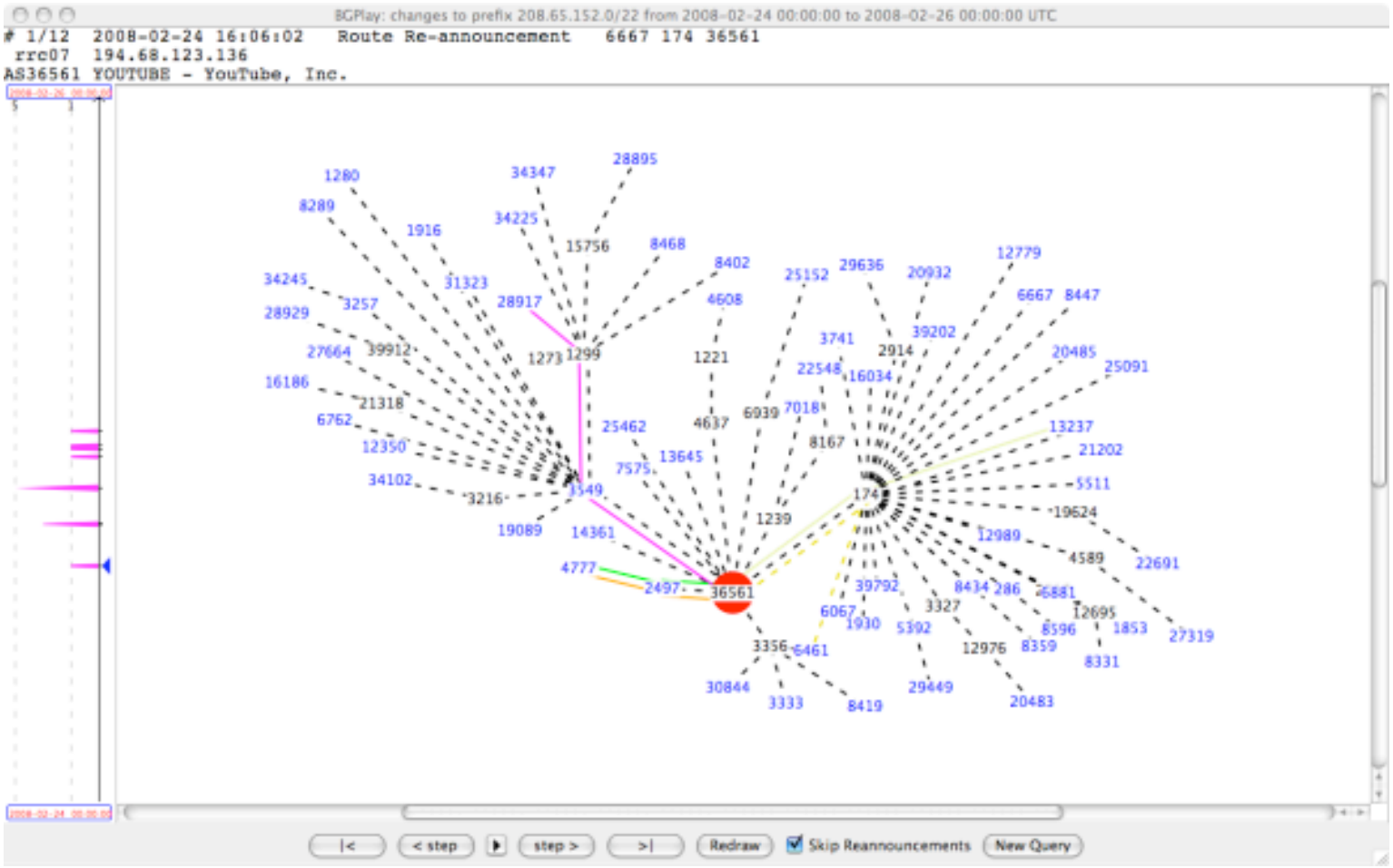
I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

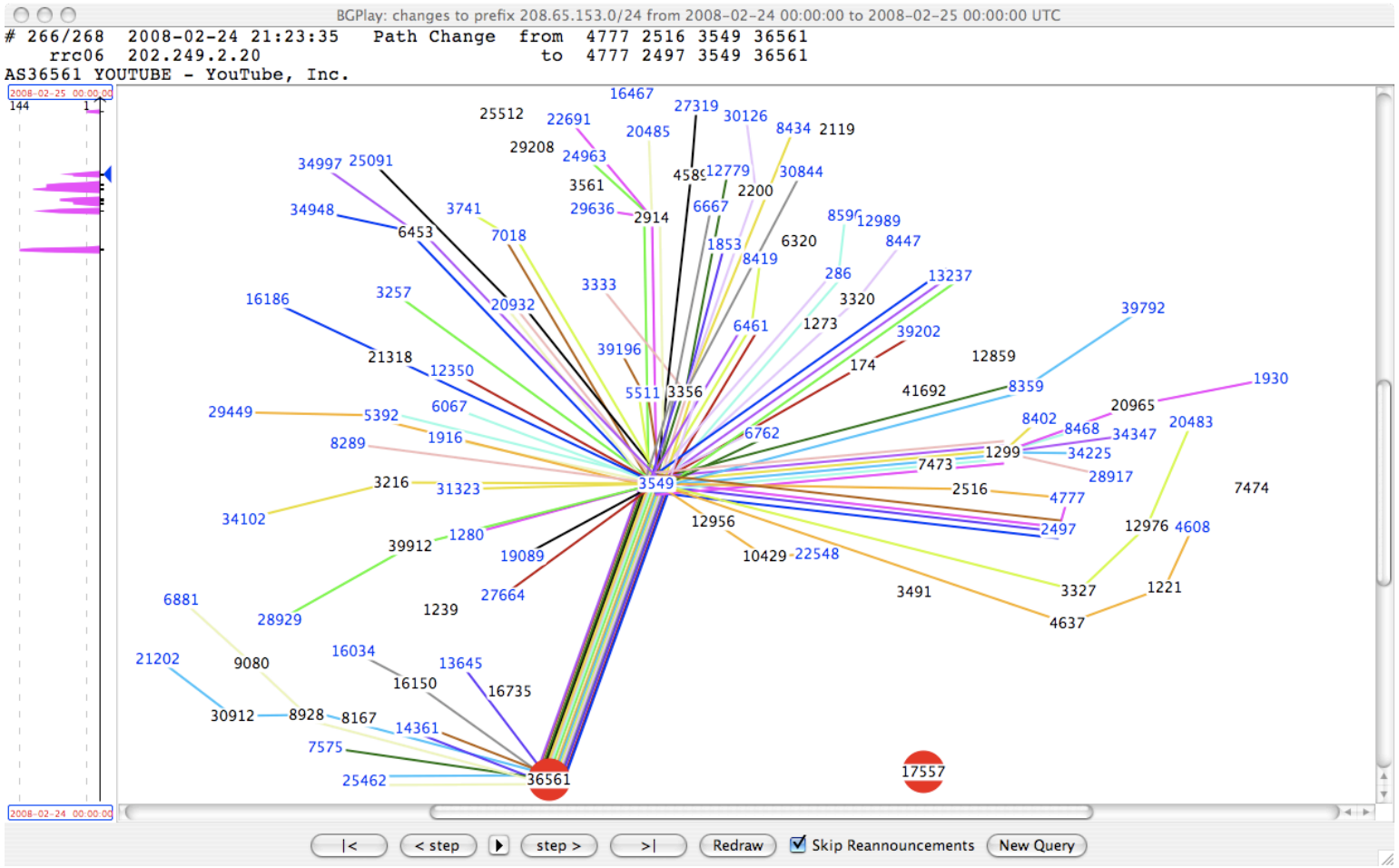
Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

YouTube before BH incident



Source: RIPE-NCC – http://www.ripe.net/news/study-youtube-hijacking.html

YouTube during BH incident



Source: RIPE-NCC – http://www.ripe.net/news/study-youtube-hijacking.html

Full Hijacking

- Poisoning
  - Specific BGP prefix injection
- Reply path
  - Plan reply path (note ASN's)
  - AS-PATH prepend reply path ASN's
  - Policy routing to nail next-hop on
- Forwarding and abusing!!!
- Obfuscation
  - TTL additive partially hides "*pirate*" path
  - No anonymity → AS-PATH will show origin

Poison route injection

- **route-map hijacked permit 10**
  - **match ip address prefix-list NET**
  - **set as-path prepend 10 20 200**

route-map hijacked permit 10
match ip address prefix-list NET
set as-path prepend 10 20 200

2 Traffic is abused (i.e.sniff) and sent back using AS10 (policy routing)

Attacker ASN 100

AS10

AS40

AS60

AS20

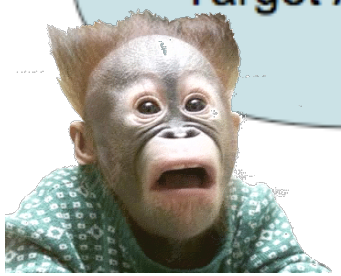
AS30

AS50

1 Inject specific prefix (poison) including "return path ASN's" on AS-PATH forces traffic sending to Attacker

3 Traffic is received by victim without noticing abusive activity.

Target ASN 200



Source: "Stealing the Internet" Defcon Talk – http://www.defcon.org

Original traceroute

```
 2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 8 msec 8 msec 8 msec
 4 12.122.99.17 [AS 7018] 8 msec 4 msec 8 msec
 5 12.86.156.10 [AS 7018] 12 msec 8 msec 4 msec
 6 tge1-3.fr4.sjc.llnw.net (69.28.171.66) [AS 22822] 68 msec 56 msec 68 msec
 7 ve5.fr3.sjc.llnw.net (69.28.171.209) [AS 22822] 56 msec 68 msec 56 msec
 8 tge1-1.fr4.lax.llnw.net (69.28.171.117) [AS 22822] 64 msec 64 msec 72 msec
 9 tge2-4.fr3.las.llnw.net (69.28.172.85) [AS 22822] 68 msec 72 msec 72 msec
10 switch.ge3-1.fr3.las.llnw.net (208.111.176.2) [AS 22822] 60 msec 60 msec 60 msec
11 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 60 msec 60 msec 60 msec
12 66.209.64.85 [AS 23005] 64 msec 60 msec 60 msec
13 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 60 msec 64 msec 60 msec
14 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 60 msec 60 msec 60 msec
```

Source: "Stealing the Internet" Defcon Talk – http://www.defcon.org

Traceroute during hijacking

```
 2 12.87.94.9 [AS 7018] 4 msec 4 msec 8 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 4 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 8 msec 4 msec 8 msec
 5 192.205.35.42 [AS 7018] 4 msec 8 msec 4 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 24 msec 16 msec 28 msec
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 28 msec 28 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 28 msec 32 msec 32 msec
10 colo-69-31-40-107.pilosoft.com (69.31.40.107) [AS 26627] 32 msec 28 msec 28 msec
11 tge2-3-103.ar1.nyc3.us.nlayer.net (69.31.95.97) [AS 4436] 32 msec 32 msec 32 msec
12 * * *   (missing from trace, 198.32.160.134 - exchange point)
13 tge1-2.fr4.ord.llnw.net (69.28.171.193) [AS 22822] 32 msec 32 msec 40 msec
14 ve6.fr3.ord.llnw.net (69.28.172.41) [AS 22822] 36 msec 32 msec 40 msec
15 tge1-3.fr4.sjc.llnw.net (69.28.171.66) [AS 22822] 84 msec 84 msec 84 msec
16 ve5.fr3.sjc.llnw.net (69.28.171.209) [AS 22822] 96 msec 96 msec 80 msec
17 tge1-1.fr4.lax.llnw.net (69.28.171.117) [AS 22822] 88 msec 92 msec 92 msec
18 tge2-4.fr3.las.llnw.net (69.28.172.85) [AS 22822] 96 msec 96 msec 100 msec
19 switch.ge3-1.fr3.las.llnw.net (208.111.176.2) [AS 22822] 84 msec 88 msec 88 msec
20 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 84 msec 88 msec 88 msec
21 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
22 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 88 msec 88 msec 88 msec
23 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 84 msec 84 msec
```

Source: "Stealing the Internet" Defcon Talk – http://www.defcon.org

Traceroute during hijacking with TTL additive technique

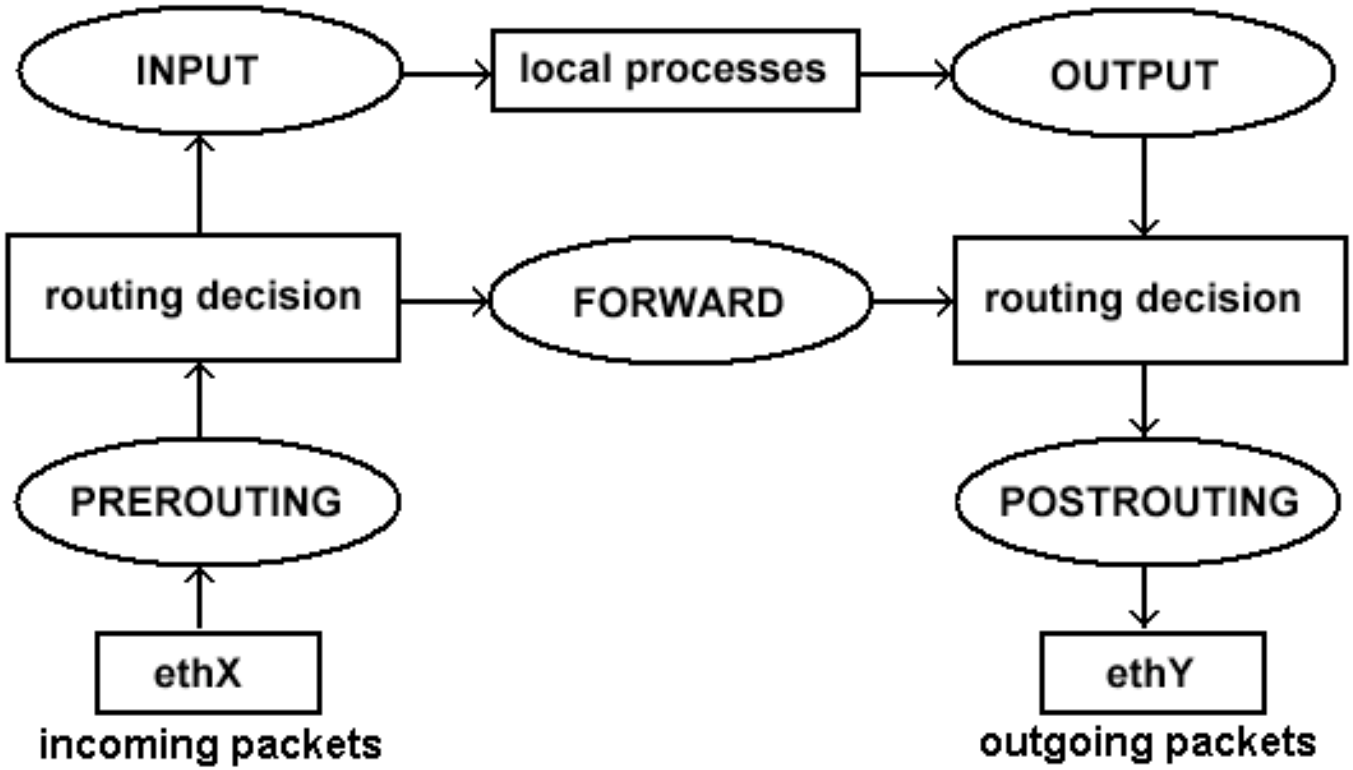
```
 2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 8 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 4 msec 8 msec 4 msec
 5 192.205.35.42 [AS 7018] 8 msec 4 msec 8 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 16 msec 12 msec *
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 32 msec 32 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 32 msec 32 msec 32 msec
10 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 88 msec 88 msec 84 msec
11 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
12 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 84 msec 84 msec 88 msec
13 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 88 msec 88 msec
```

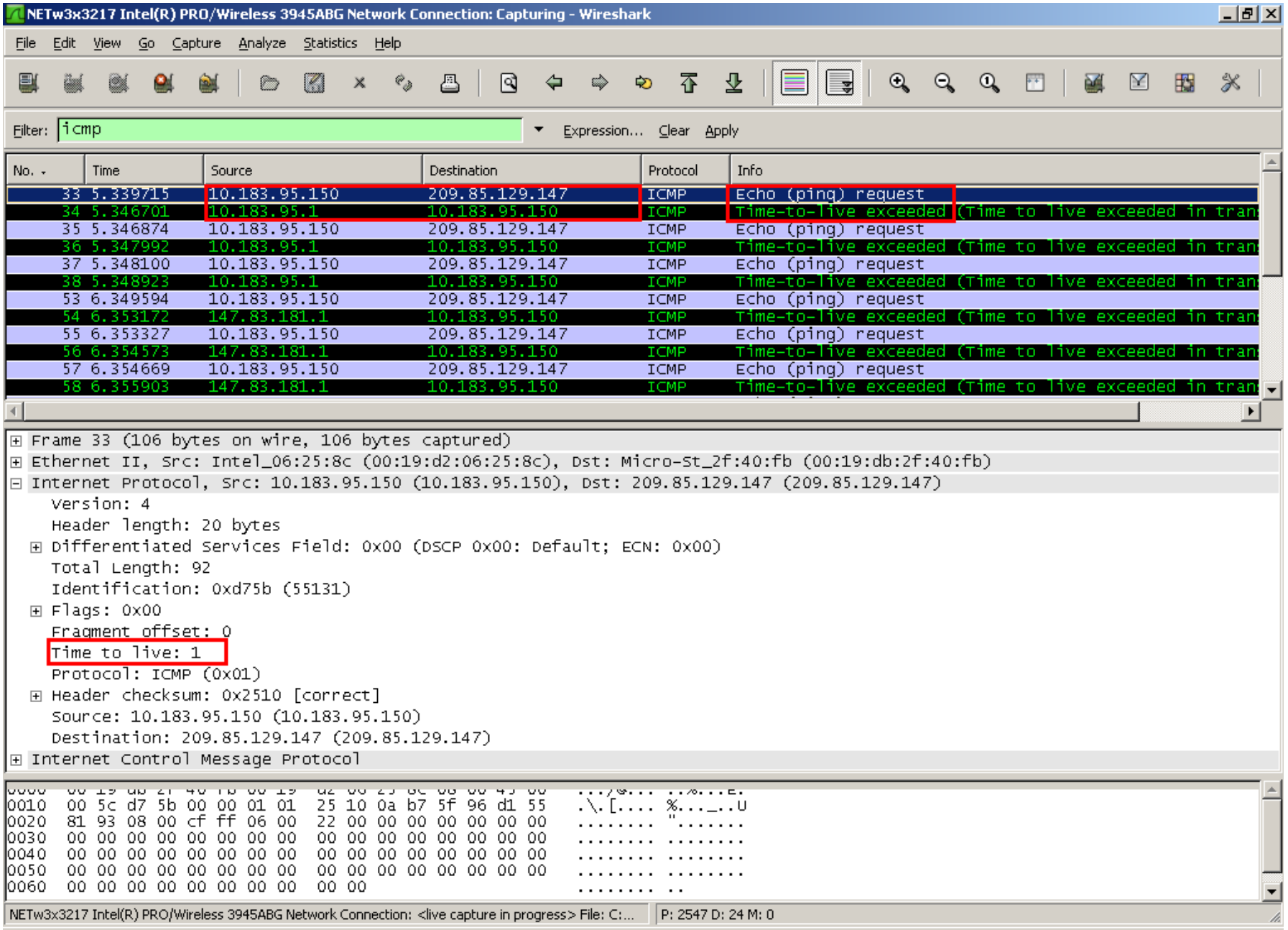
+ 10

Source: "Stealing the Internet" Defcon Talk – http://www.defcon.org

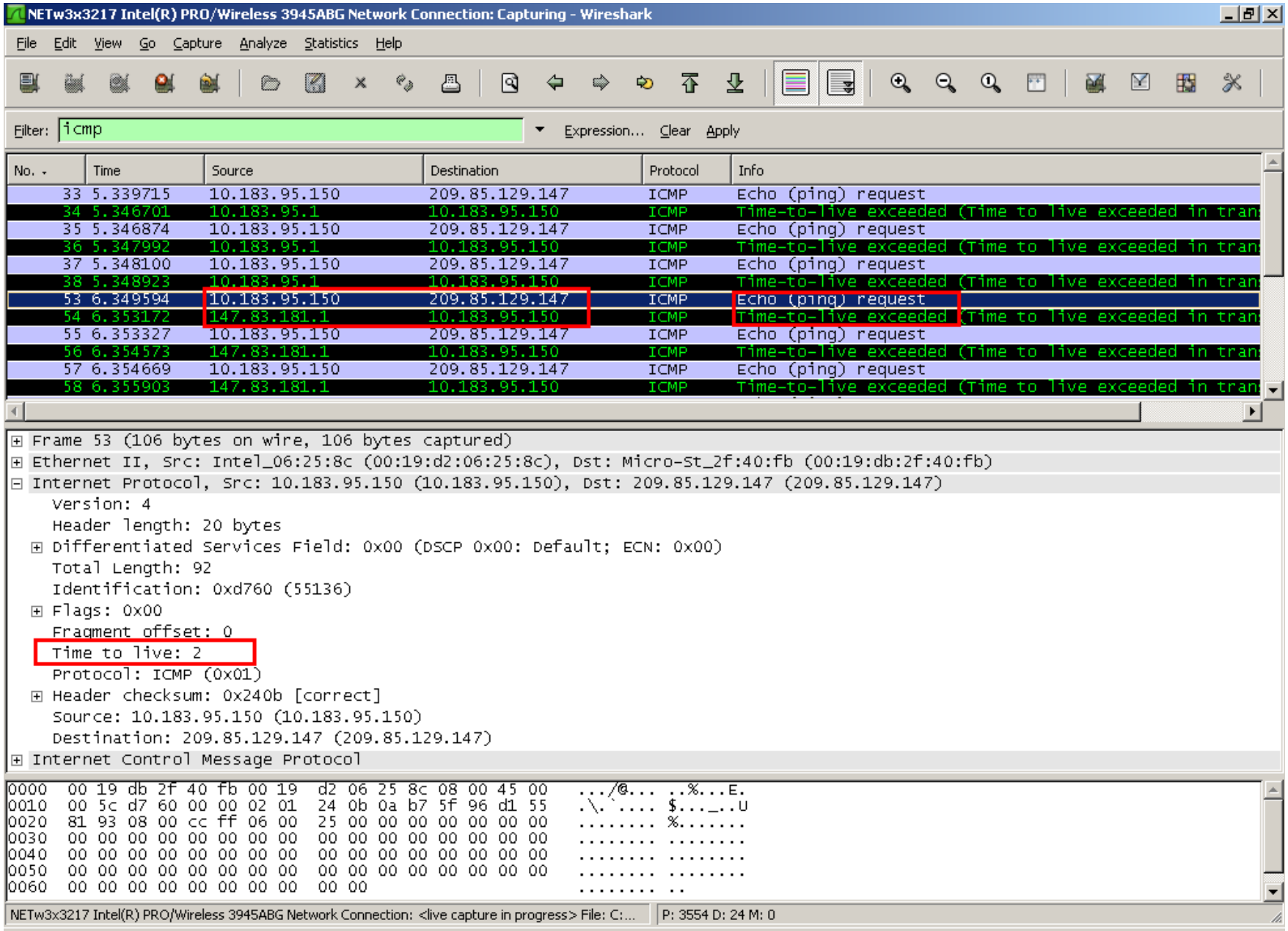
TTL additive using Linux NetFilter

- iptables -t mangle -I PREROUTING -i eth1 -j TTL --ttl-inc 1
- iptables -t mangle -I POSTROUTING -o eth1 -j TTL --ttl-inc 1





Source: Juan Vazquez – TB-Security



Source: Juan Vazquez – TB-Security

Unallocated space hijacking

- Used temporarily by attackers to hide their activity and avoid abuse notifications
- Nowadays mostly used for spam but could be used for other dirty issues (terrorism)
- Who is responsible for something that doesn’t belong to anyone?

Pirates of the Internet

- Internet & BGP 101
- Attacks
- Countermeasures
  - Protection
  - Detection
  - Reaction

Protection

Detection

Reaction

Protection

Protection / prevention

- Review your peer route filtering
- Register and protect your objects on IRR DB
- Take Routing Registry RIPE-NCC training
- Set up antispoofing (ACL's or RPF) and infrastructure (ACL's) filtering
- Peering hardening
- Have beers with other NOC teams
  - Join mailing lists instead ☹

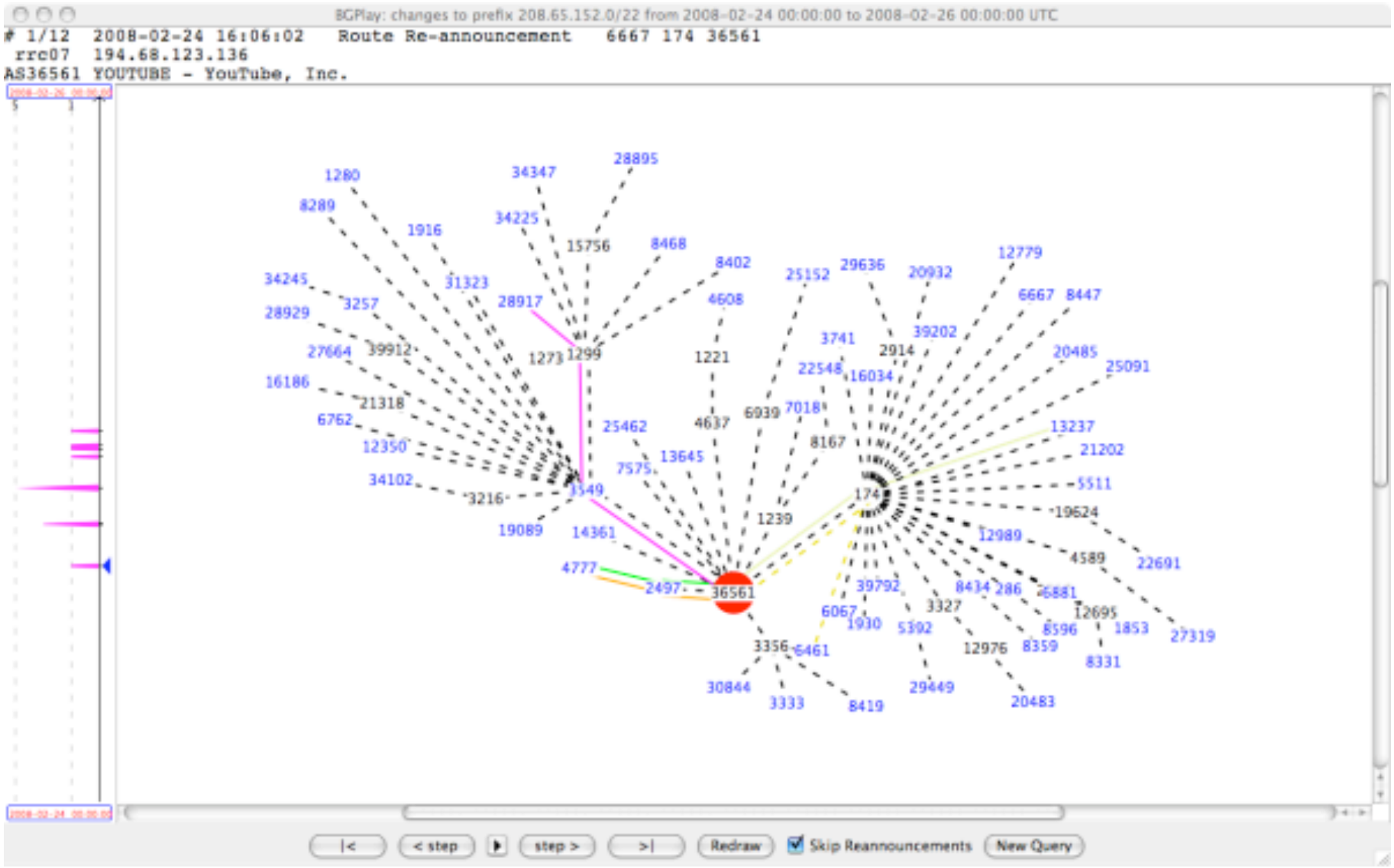
Peer route filtering

- Where ?
  - Customer side
  - Internet Exchange Points / Private peerings
  - Transit providers
- What ?
  - Maximum number
  - AS-Path
  - Prefixes (static or dynamic)
- Some tips'n'tricks
  - IRRToolset tool (RIPE-NCC, ISC)
  - Bogon Route Servers (Cymru)
  - BGP configuration guides (Cymru, NIST)

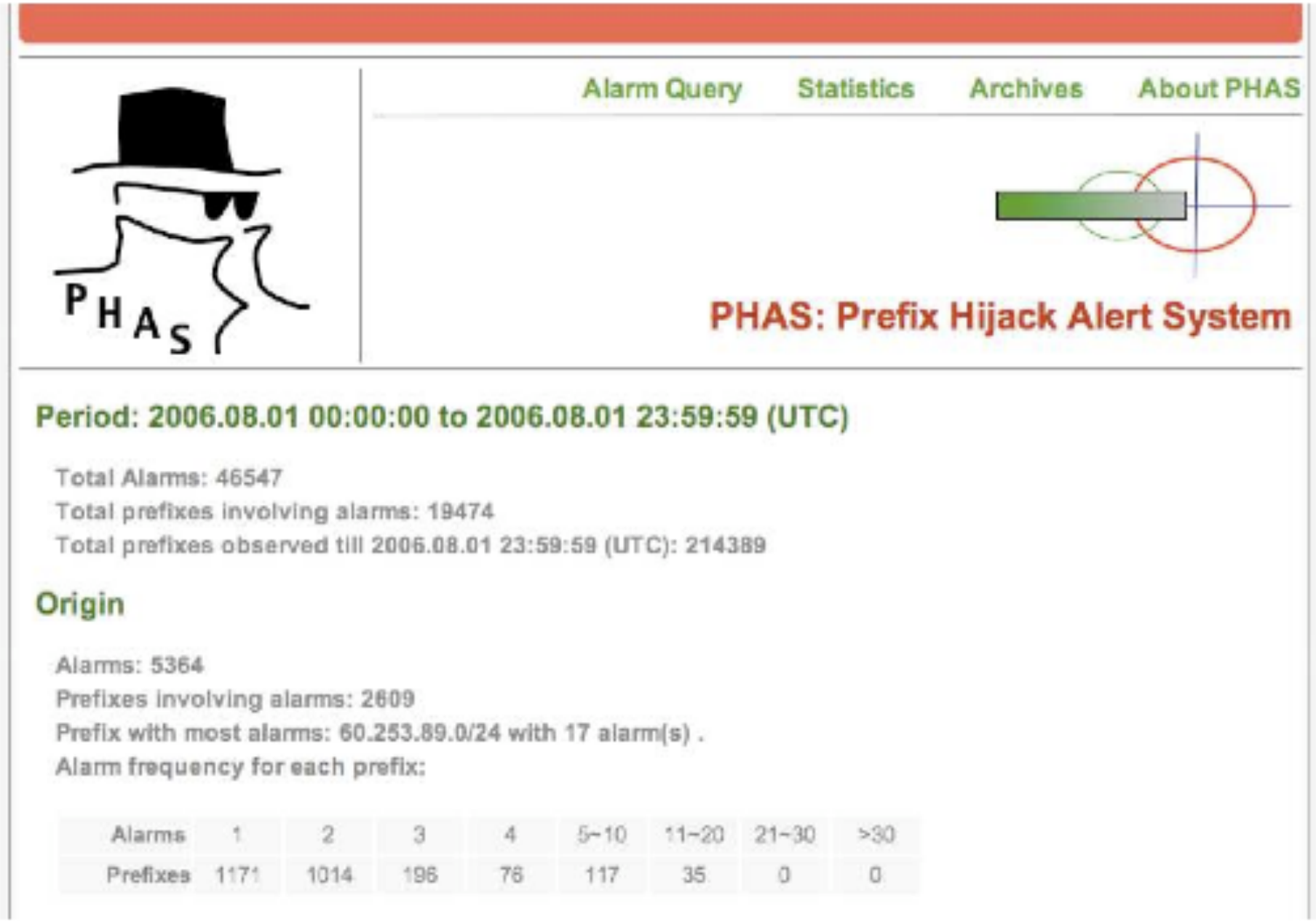
Detection

Detection

- Alerting Systems
  - Prefix-based NIDS
- Useful tools:
  - RIPE MyASN
  - Prefix Hijack Alert System (PHAS)



Source: RIPE RIS– http://www.ris.ripe.net



Source: Colorado State University – http://netsec.cs.colostate.edu/phas/

Reaction

Reaction

- You are allowed to cry and scream
- Contact upstreams and related mates
  - Remember them you paid their beers
- Pray for a prompt response
  - From hours to days
  - Depends on how important you are
- Notify Law Enforcement Organizations if necessary

Pirates of the Internet

- Internet & BGP 101
- Attacks
- Countermeasures

References 1/2

- **“Stealing the Internet”**

  A.Pilisov, T.Kapela – Defcon 16 Conference (Las Vegas)

  http://www.defcon.org/html/links/defcon-media-archives.html#dc_16

- **“BGP Routing Security”**

  D.Wendlandt – Carnegie Mellon University

  http://www.cs.cmu.edu/~dwendlan/routing/

- **“BGP Security resources”**

  http://www.bgp4.as/security

References 2/2

- **“BGP Vulnerability Testing”**

  S.Convery Matthew Franz

  http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf

- **“Hacking Cisco Networks Exposed”**

  A.Vladimirov, A.Mikhailovsky – McGraw Hill

  ISBN: 0-07-225917-5

cfragoso@cesca.es
http://www.cesca.es

THANKS!