BGPMON

A LOOK AT RECENT BGP ROUTING INCIDENTS

NANOG63

BGPMON

AGENDA

HIJACKING FOR MONETARY GAIN

The Bitcoin Hijack

- **Originally detected by Dell secure works**
- **Between Oct 2013 and May 2014**
- **Hijacker was a Canadian ISP**
- **Originating more specifics for various c**

HIJACKING FOR MONETARY GAIN

- ***Scope and Impact***

Scope limited to IX peers (Torix)

$83,000 stolen

Hijacked blocks included: AWS, OVH, Digit
ServerStack, Choopa, LeaseWeb and more

HIJACKING FOR CENSORSHIP

Turkey Hijacking IP addresses for popular Global DNS providers

- **March 28 – 30 Election in Turkey**
- **Started with a hard null route, which broke 'the Internet'**
- **Turk Telekom brought up DNS servers and redirected DNS traffic**
- **MITM Affected Google, OpenDNS, Level3,…**

HIJACKING FOR CENSORSHIP

Turkey Hijacking IP addresses for popular Global DNS providers

```
show router bgp routes 8.8.8.8
===============================================================================
BGP Router ID:212.156.116.127 AS:9121 Local AS:9121
===============================================================================
Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best, b - backup

===============================================================================
BGP IPv4 Routes
===============================================================================
Flag Network LocalPref MED
Nexthop Path-Id VPNLabel
As-Path
-------------------------------------------------------------------------------
u*>? 8.8.8.8/32 100 None
212.156.253.130 None -
No As-Path
*? 8.8.8.8/32 100 None
212.156.253.130 None -
No As-Path
-------------------------------------------------------------------------------
Routes : 2
===============================================================================
```

We would expect to see 8.8.8.0/24 here originated by AS 15169.
This is the proof of Turk Telekom hijacking Google DNS.

HIJACKING FOR CENSORSHIP

Turkey Hijacking IP addresses for popular Global DNS providers

Youtube.com lookup at Google's 8.8.8.8 DNS server 8.8.8.8 from Turk Telekom

```
;; ANSWER SECTION (1 record)
youtube.com.     86064    IN       A     195.175.254.2
                                                ^^^^^^^^^^^^^^^^^
                                        Not a real Youtube IP address
```

Youtube.com lookup at Google's 8.8.8.8 DNS server from The Netherlands

```
;; ANSWER SECTION:
youtube.com.        299    IN A   74.125.136.93
youtube.com.        299    IN A   74.125.136.91
youtube.com.        299    IN A   74.125.136.136
youtube.com.        299    IN A   74.125.136.190
                                    ^^^^^^^^^^^^^^^^^
                                Normal Youtube IP addresses
```

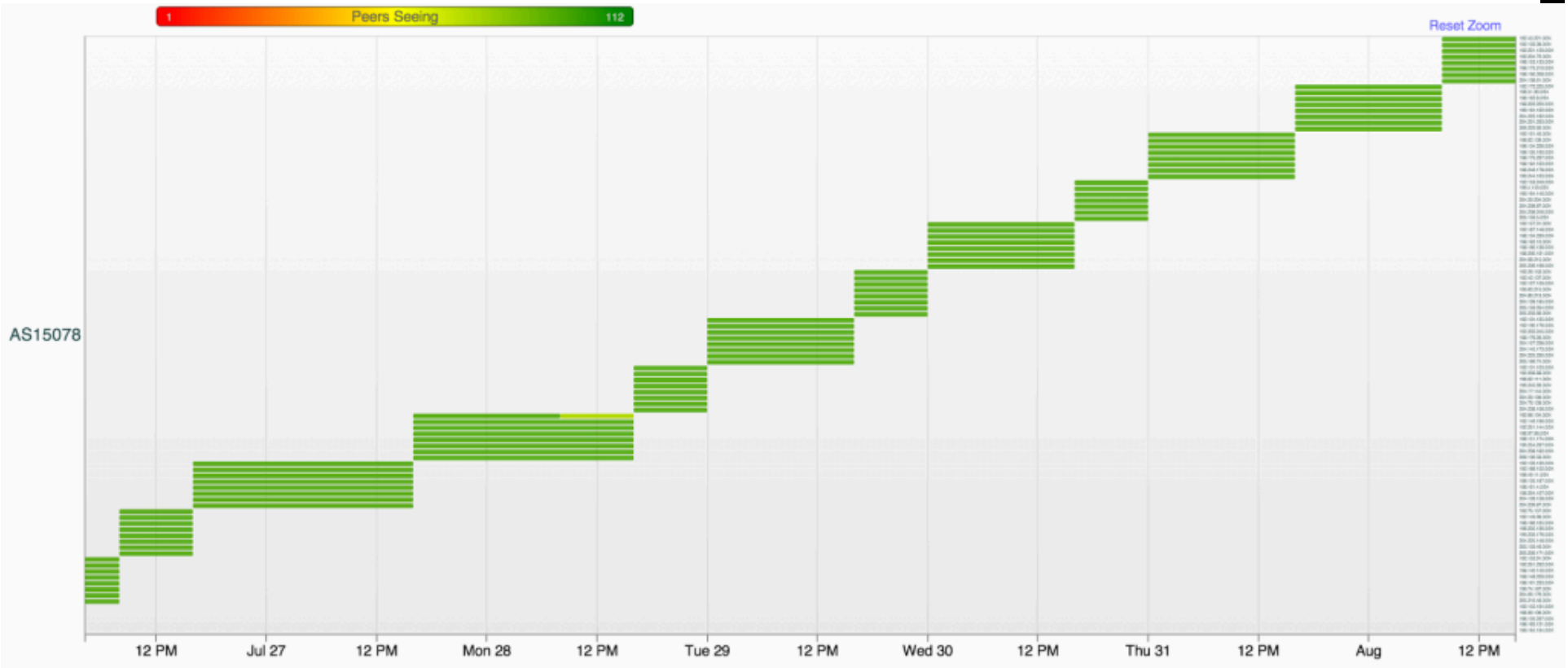
HIJACKING FOR SPAMMING

IP squatting by spammer

- Using un-announced address space to send spam
- Find unused space & announce for few hours and send spam
- Rinse and Repeat

HIJACKING FOR SPAMMING

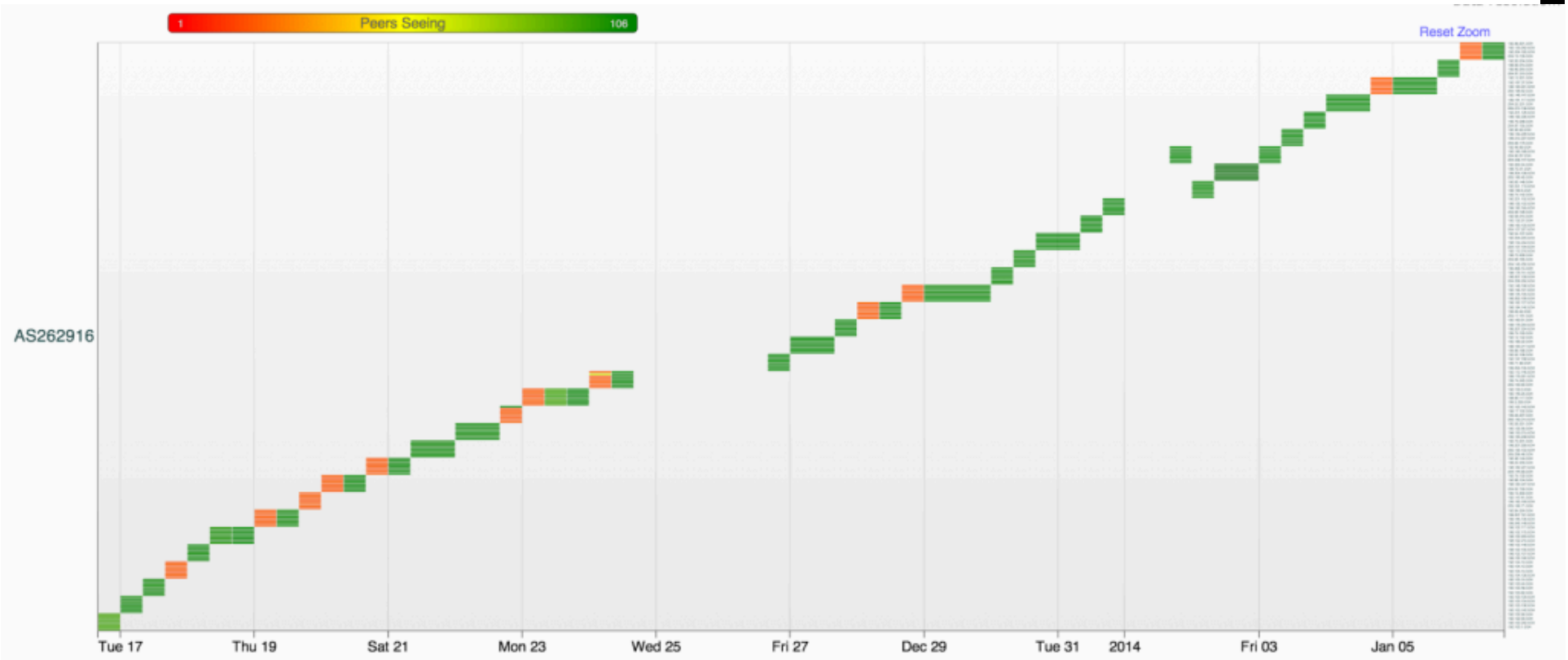
- Multiple Asns used, all with similar fingerprint
- Valid RADB route objects
- Few hours life time, 8 prefixes at a time



HIJACKING FOR SPAMMING

Spammers take vacation as well…

No announcements over christmas and new year



TALKING ABOUT SPAMMING

When Spamhaus gets in the way

The 300G DDOS that almost broke the Internet… sure there were a lot of bits, but also a BGP hijack

Note the /32 announcement, marking everything as spam

```
router# show ip bgp 204.16.254.40
BGP routing table entry for 204.16.254.40/32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  [redacted]
  34109 51787 1198
    193.239.116.204 from 193.239.116.204 (84.22.127.134)
     Origin IGP, metric 10, localpref 140, valid, external, best
      Last update: Tue Jan  5 11:57:27 1971
```

HIJACKING BY SYRIA TELECOM

- Syrian national Telecommunications Establishment (STE) mis-originated 1480 prefixes
- 306 unique Autonomous Systems
- Some for a few minutes, some for a few hours
- Intentional or not… traffic was affected

BGPMON

ROUTE LEAKS

- Essentially a MITM, smaller provider inserts itself between large ones and gets overwhelmed..
- Typically accidents
- Can cause serious outages
- Recent leaks in The Philippines & Argentina affected AWS and Cloudflare

INCIDENT OR INTENTIONAL?

Many are 'fat fingered'

- BGP > OSPF > BGP
- BGP traffic optimizers (Stealthy events):
  - http://www.bgpmon.net/accidentally-stealing-the-internet/
- AS path Prepending (AS2, AS3, AS4)

Some are suspicious

- Bitcoin hijack
- Turkey censorship
- Belarus event (seems targeted)
- Spamhaus

QUESTIONS