BISHOP FOX

Homebrew Censorship Detection

BY BGP ANALYSIS

July 16, 2015

About Me

ZACHARY JULIAN

- Sr. Security Analyst @ Bishop Fox
- Enterprise Security team
- Clarkston, MI -> Phoenix, AZ

Background & Motivation

WHY MONITOR BGP DATA?

- Interest in the digital aspect of the Syrian Civil War
  - State-sponsored malware
  - Internet censorship
- Internet censorship via BGP manipulation during the Arab Spring
  - Egypt
  - Libya
- How can I alert myself to Syrian BGP changes?

www.syriabgp.net

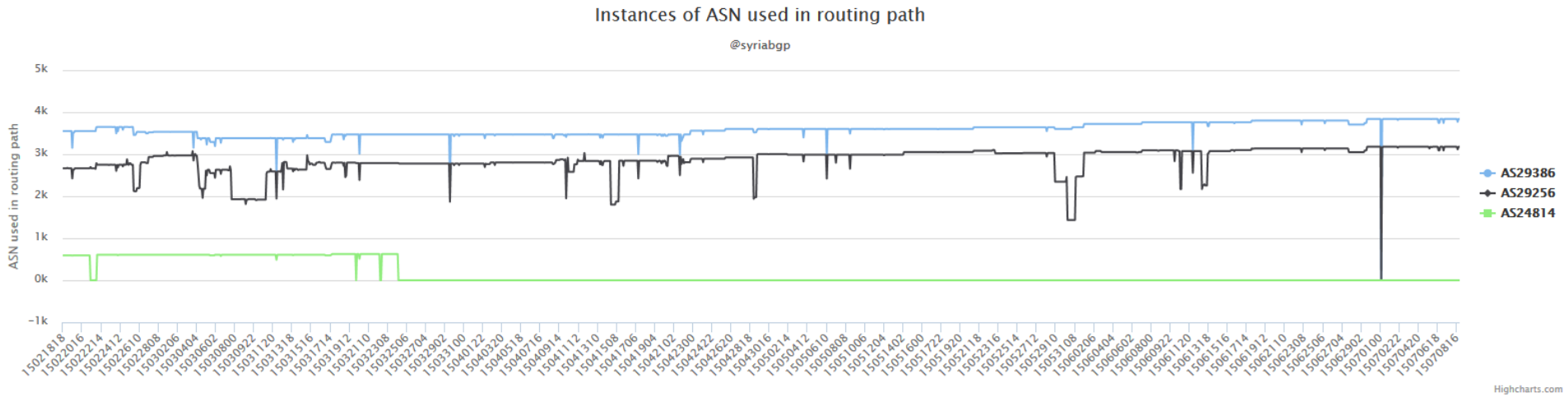
VISUALIZE AND REPORT SYRIAN BGP CHANGES OVER TIME

LATEST SYRIAN BGP CHANGES BY AUTONOMOUS SYSTEM

AS29386: **0%**

AS29256: **0%**

AS24814: **-100%**



BORDER GATEWAY PROTOCOL

A BRIEF OVERVIEW

Border Gateway Protocol (BGP)

WHAT IS IT?

- Critical to the operation of the Internet
- Used to exchange routing information between Autonomous Systems (AS)
- Commonly used to determine a path between ISPs
- Announces IP prefixes

Autonomous Systems

WHAT ARE THEY?

- A collection of IP prefixes (ranges) under control of one network operator
- Each AS is assigned an ASN by IANA
- For instance, in Phoenix:

AS Number	Operator	IP Prefixes
AS209	Qwest Communications Company, LLC	... 198.185.174.0/24 198.185.175.0/24 198.185.176.0/24 198.185.177.0/24 ...

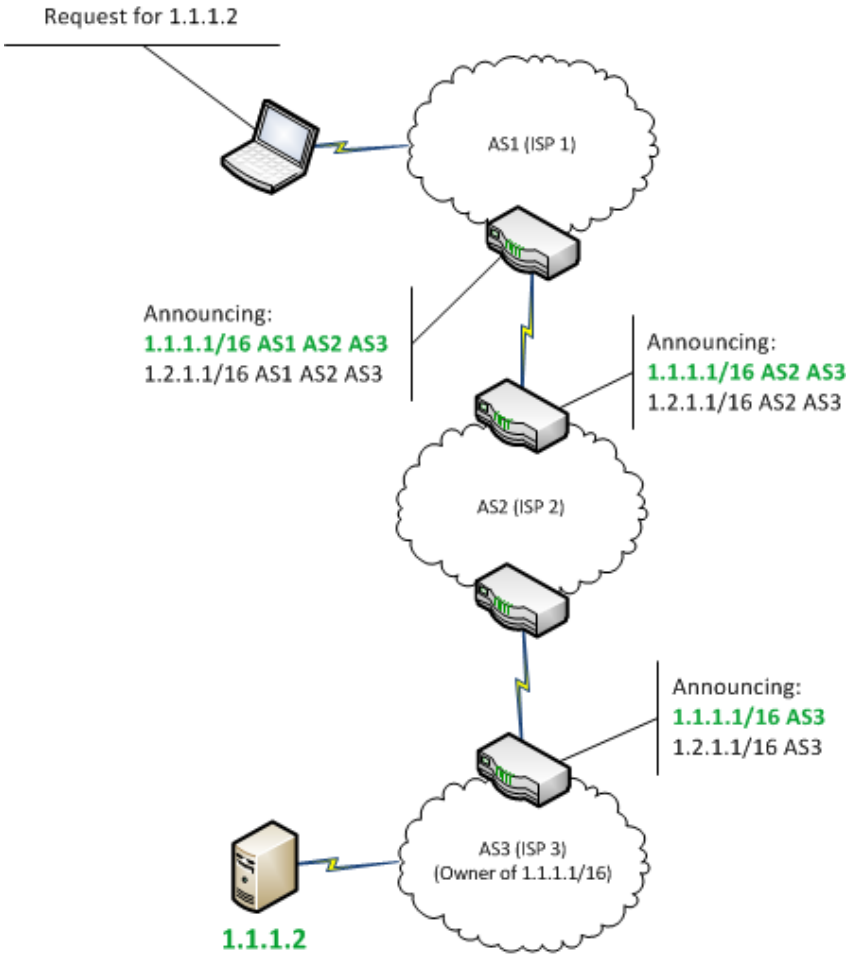
Prefixes

ONE MORE DEFINITION

- Each prefix is advertised by one or more edge routers.
- These routers broadcast BGP advertisements to peers.
- If all edge routers stop advertising, prefixes are not routable to the Internet.

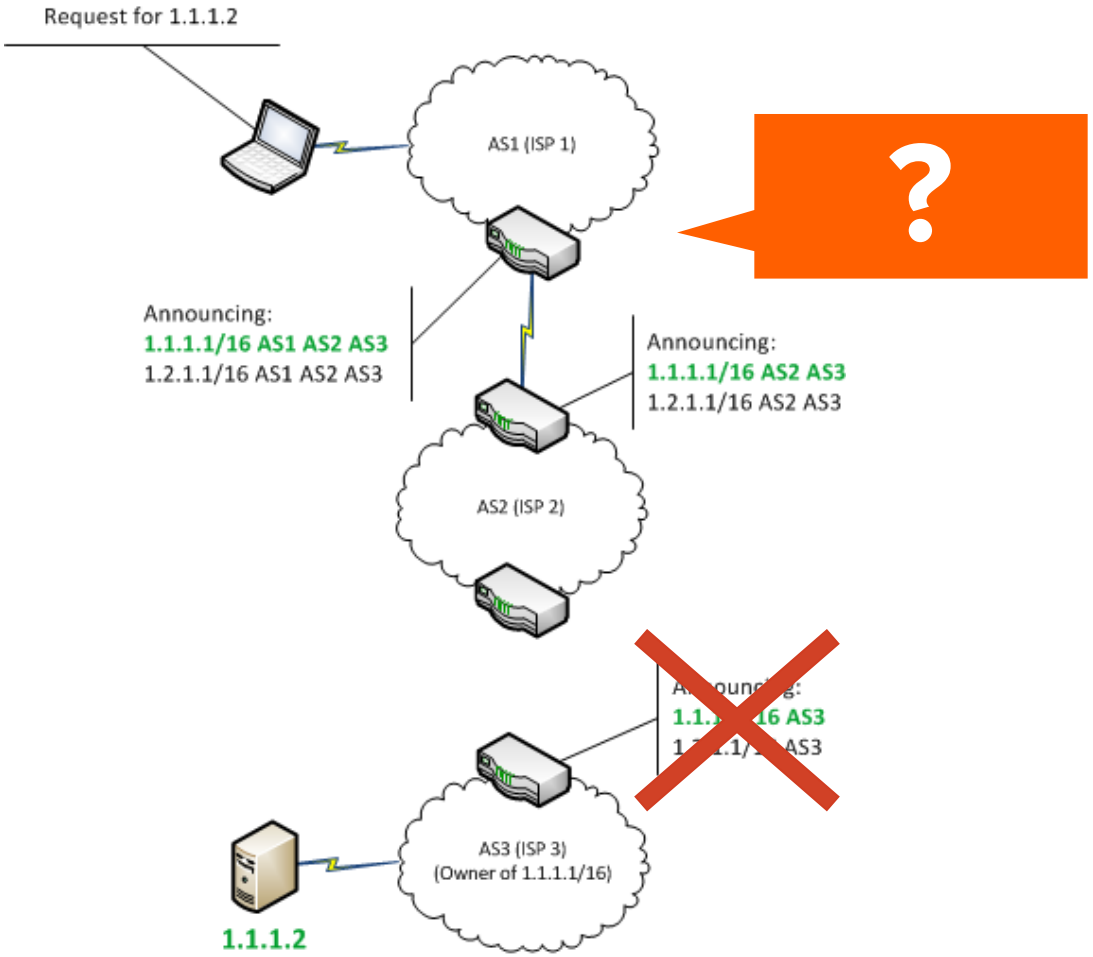
Border Gateway Protocol

AT A HIGH LEVEL



Border Gateway Protocol

AT A HIGH LEVEL



Internet Censorship via BGP

EASIER THAN YOU THINK

- Many countries have state-owned telecommunications infrastructure
- They operate only a few Autonomous Systems
- Trivial to order Internet shutdown by ceasing BGP route advertisements

MONITORING BGP DATA

HOMEBREW INTERNET ANALYSIS

The Route Views Project

WWW.ROUTEVIEWS.ORG

- University of Oregon - Advanced Network Technology Center
- Aggregates BGP data from participating AS'
- Provides updated BGP data every two hours
  - ~50MB .bz2 archive
  - Available over HTTP, FTP, telnet

http://www.routeviews.org/

How Can We Use Route Views' Data?

A LOOK AT THE FORMAT

```
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
*  0.0.0.0/0        203.189.128.233          0      0      0 23673 9902 i
*  0.0.0.0/0        103.247.3.45             0      0      0 58511 2764 i
*  1.0.0.0/24       198.129.33.85            0      0      0 293 15169 i
*  1.0.0.0/24       134.222.87.1           750      0      0 286 15169 i
*  1.0.0.0/24       213.144.128.203          1      0      0 13030 15169 i

*  178.253.104.0/22 147.28.7.1               0      0      0 3130 2914 3491 29386 29256 i
*  178.253.104.0/22 67.17.82.114          2523      0      0 3549 3356 3491 29386 29256 i
*  178.253.104.0/22 89.149.178.10           10      0      0 3257 3491 29386 29256 i
*  178.253.104.0/22 137.164.16.84            0      0      0 2152 11164 3491 29386 29256 i
*  178.253.104.0/22 195.22.216.188         100      0      0 6762 29386 29386 29386 29386 29386 i
```

IP PREFIX ANNOUNCEMENT

IP ADDRESS BROADCASTING ANNOUNCEMENT

MULTI EXIT DISCRIMINATOR LOCAL PREFERENCE WEIGHT

ADVERTISED PATH TO PREFIX

How Can We Use Route Views' Data?

A LOOK AT THE FORMAT

```
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
*  0.0.0.0/0        203.189.128.233          0      0      0 23673 9902 i
*  0.0.0.0/0        103.247.3.45             0      0      0 58511 2764 i
*  1.0.0.0/24       198.129.33.85            0      0      0 293 15169 i
*  1.0.0.0/24       134.222.87.1           750      0      0 286 15169 i
*  1.0.0.0/24       213.144.128.203          1      0      0 13030 15169 i

*  178.253.104.0/22 147.28.7.1               0      0      0 3130 2914 3491 29386 29256 i
*  178.253.104.0/22 67.17.82.114          2523      0      0 3549 3356 3491 29386 29256 i
*  178.253.104.0/22 89.149.178.10           10      0      0 3257 3491 29386 29256 i
*  178.253.104.0/22 137.164.16.84            0      0      0 2152 11164 3491 29386 29256 i
*  178.253.104.0/22 195.22.216.188         100      0      0 6762 29386 29386 29386 29386 29386 i
```

HOW MANY TIMES IS OUR TARGET ASN ANNOUNCED IN A ROUTING PATH?

```
user@ubuntu:~$ grep '29386' oix-full-snapshot-latest.dat | wc -l
3840
```

How Can We Use Route Views' Data?

A LOOK AT THE FORMAT

```
user@ubuntu:~$ grep '29386' oix-full-snapshot-latest.dat | wc -l
3840
```

- How many times is our target ASN announced in a routing path?
- How does that compare to two hours ago?
- ((Current Total / Total 2 Hours Ago)-1) = Change
- ((2687/2852)-1) = -0.057 or a 6% decrease

routeviews-py

A PYTHON SCRIPT FOR RECORDING ROUTE VIEWS DATA

- Input comma-separated list of ASNs
- Downloads latest Route Views data
- Compares changes from last iteration for each ASN
- Output to CSV or SQLite
  - Timestamp, ASN, Count, Change
- Available on GitHub:
  `https://github.com/tprime-/routeviews-py`

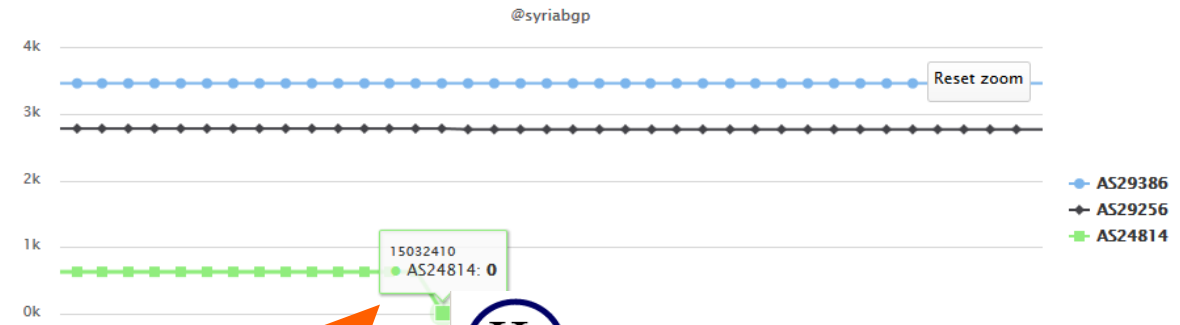
routeviews-py

A PYTHON SCRIPT FOR RECORDING ROUTE VIEWS DATA

```
user@ubuntu:~$ ./routeviews-py.py -h

Usage: ./routeviews-py.py -a <comma-separated
list of ASNs> -o <sqlite,csv>

Example: ./routeviews-py.py -a 100,200,300 -o
csv

Notes: -a flag is required. -o flag is
optional. Default output is SQLite.
```

An Accurate Metric

COMPARED TO PROFESSIONAL BGP MONITORING SOLUTIONS



ASN24814 GOES OFFLINE MARCH 24, 2015.

HURRICANE ELECTRIC INTERNET SERVICES

Search

AS24814 Syrian Computer Society, scs

http://bgp.he.net/AS24814

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

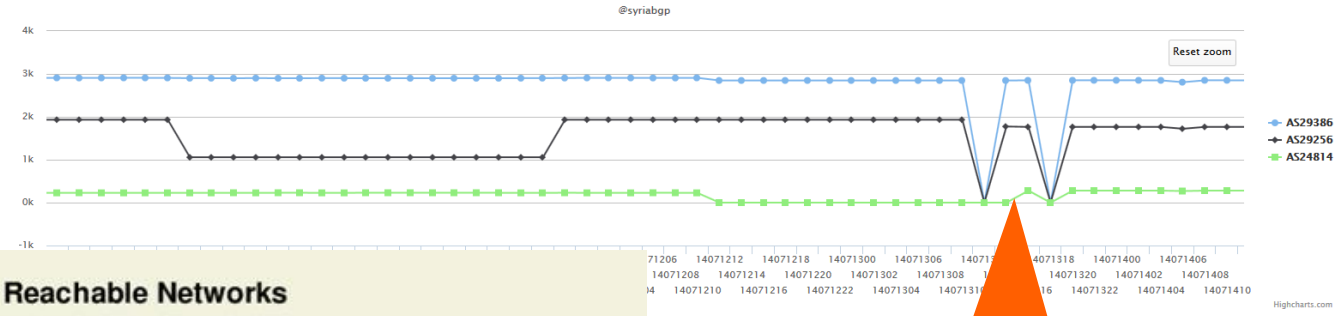
AS Info | Graph v4 | Prefixes v4 | Peers v4 | Whois | IRR

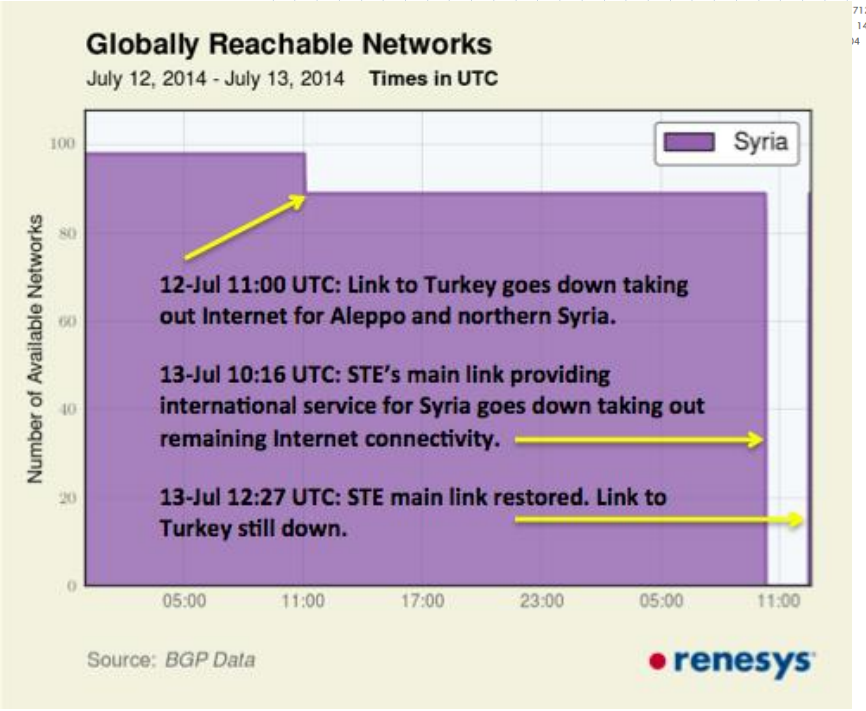
AS24814 has not been visible in the global routing table since March 24, 2015
The information displayed is from that time.

Country of Origin:	Syrian Arab Republic		
Prefixes Originated (all): 16		Prefixes Announced (all): 0	
Prefixes Originated (v4): 16		Prefixes Announced (v4): 0	
Prefixes Originated (v6): 0		Prefixes Announced (v6): 0	
BGP Peers Observed (all): 1		IPs Originated (v4): 0	
BGP Peers Observed (v4): 1		AS Paths Observed (v4): 0	
BGP Peers Observed (v6): 0		AS Paths Observed (v6): 0	
Average AS Path Length (all): 0.000			
Average AS Path Length (v4): 0.000			
Average AS Path Length (v6): 0.000			

An Accurate Metric

COMPARED TO PROFESSIONAL BGP MONITORING SOLUTIONS





SYRIAN INTERNET GOES DOWN July 12, 2014

https://twitter.com/DynResearch/status/488305381765304320

HOW TO MONITOR BGP AT HOME

USING ROUTEVIEWS-PY

Setup Your Own BGP Monitoring

USING ROUTEVIEWS-PY

- Cheap ($5/month) VPS, spare machine will work fine
- Download routeviews-py from GitHub
- Select ASNs
- Add to crontab:

```
0 0,2,4,6,8,10,12,14,16,18,20,22 * * * /home/routeviews-py.py -a 29386 > /dev/null 2>&1
```

Setup Your Own BGP Monitoring

USING ROUTEVIEWS-PY

- Detect & report censorship
- Visualize data (Highcharts, etc.)
- Push updates to various locations:
  - Twitter
  - Mailing list

What's Next?

BUDGET BGP MONITORING

- Detect BGP hijacking?
- Response to BGP censorship?
  - Modem bank

Contact Us

@BISHOPFOX

FACEBOOK.COM/BISHOPFOXCONSULTING

LINKEDIN.COM/COMPANY/BISHOP-FOX

GOOGLE.COM/+BISHOPFOX

BISHOP FOX®

Thank You – Questions?

- https://github.com/tprime-/routeviews-py
- zjulian@bishopfox.com
- @tprime_

BISHOP FOX