BGP Hijacking Detection

Open-source Intelligence and Comand line based Approach

Joon Kim@24.10.24

Agenda

- Intro to Speaker
- BGP Hijacking Case Study
- Command-line-based Analysis 101
- State-Sponsored BGP Hijacking Detection

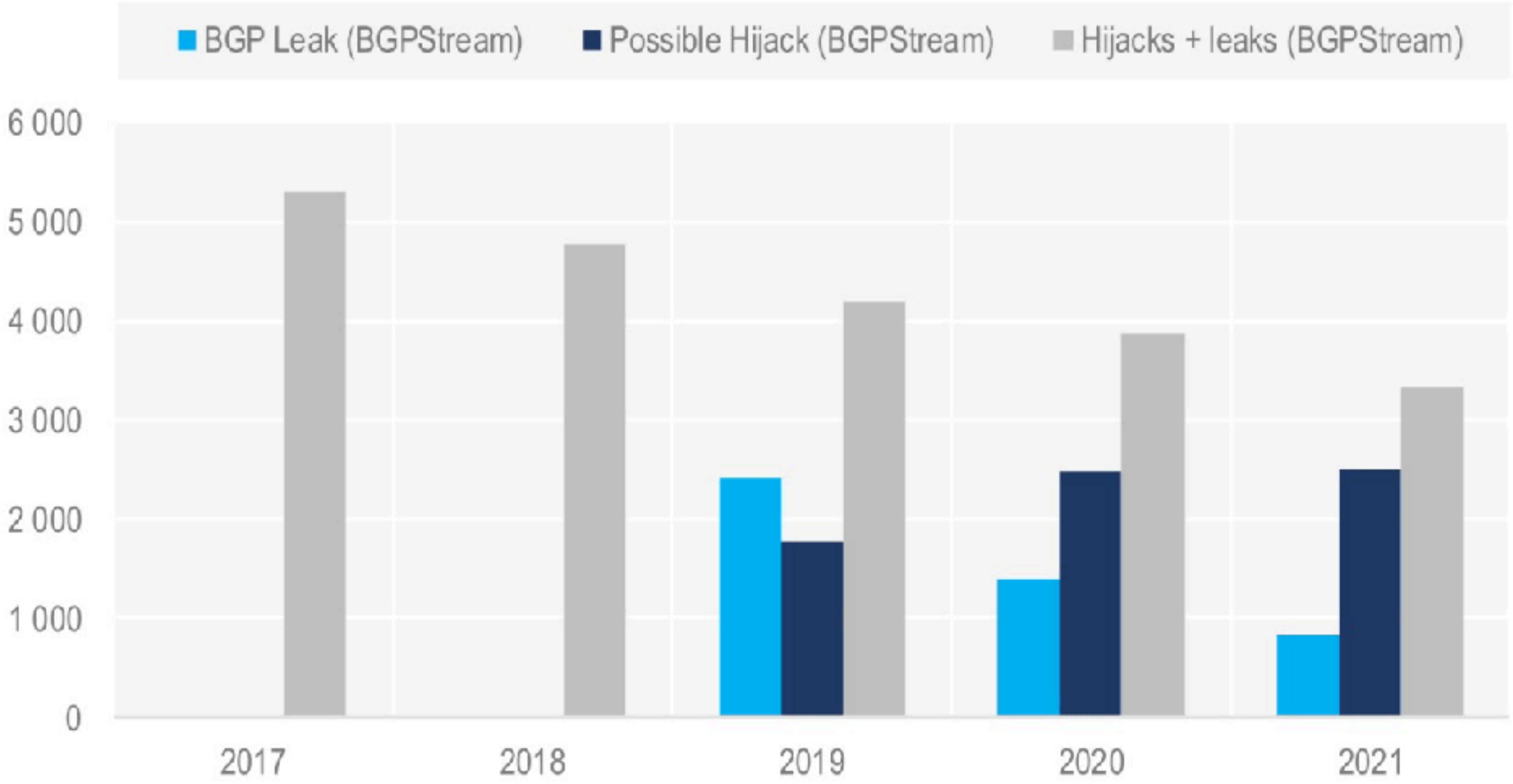
About Speaker

Joon Kim

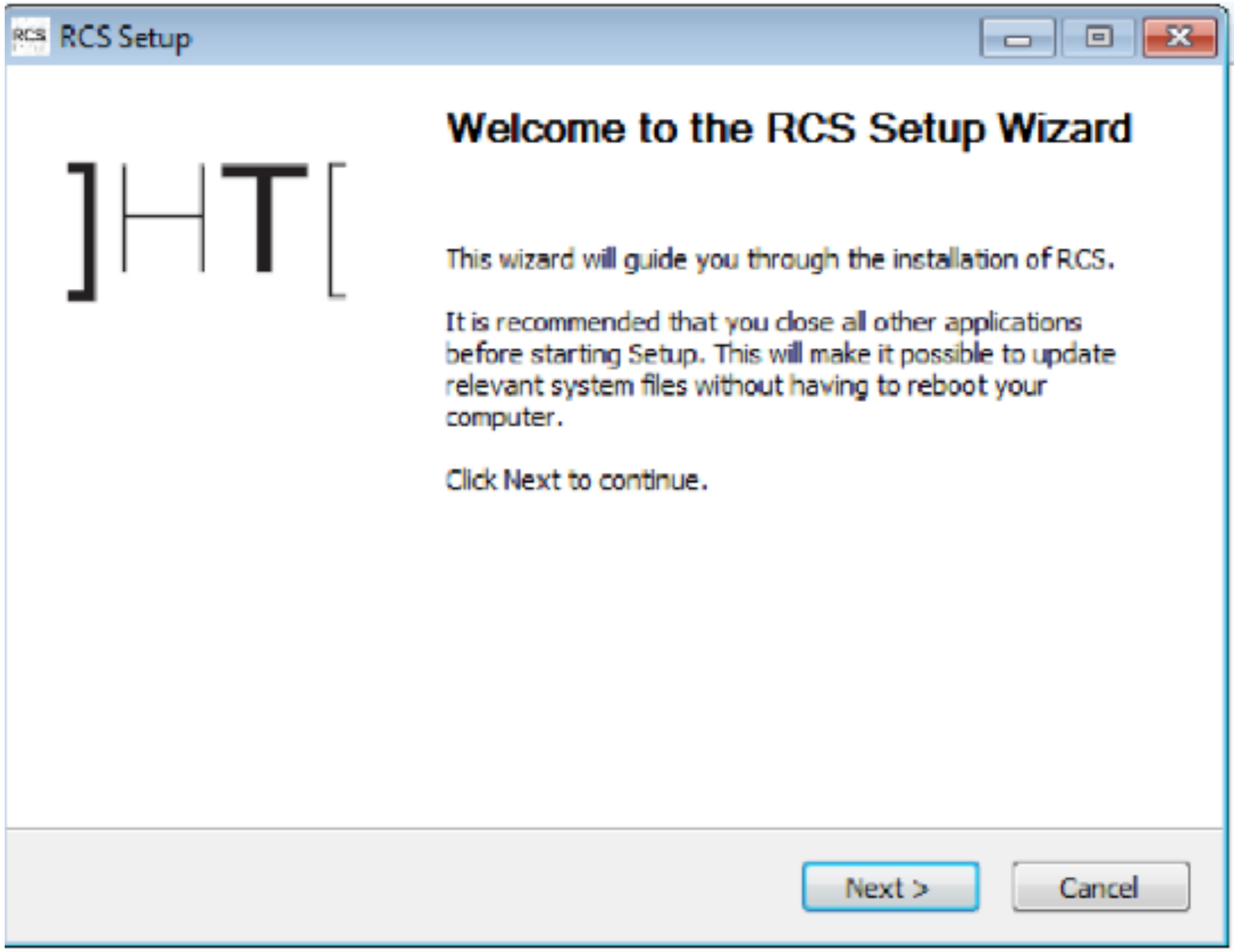
- CEO & Founder Naru Security Inc.
- Member of National Cyber Security Center
- National Police Cyber Threat Expert Group
- National Joint Cyber **Incident Response** Team
- Adjunct Prof. Sungkyunkwan University
- Ex. Advisor, Korean Cyber Operation Command
- Ex. Korean Information Security Agency
- University of Alberta CA, Computer Engineering
- 2021 Army Chief of Staff Cybersecurity Award
- 2019 Ministry of Trade Minister's Award
- 2018 Chief of National Police Agency Award
- 2008 FIRST Security Best Practice Award

Case Study

BGP Hijacking Stats by OECD



2013 State Sponsored BGP Hijacking



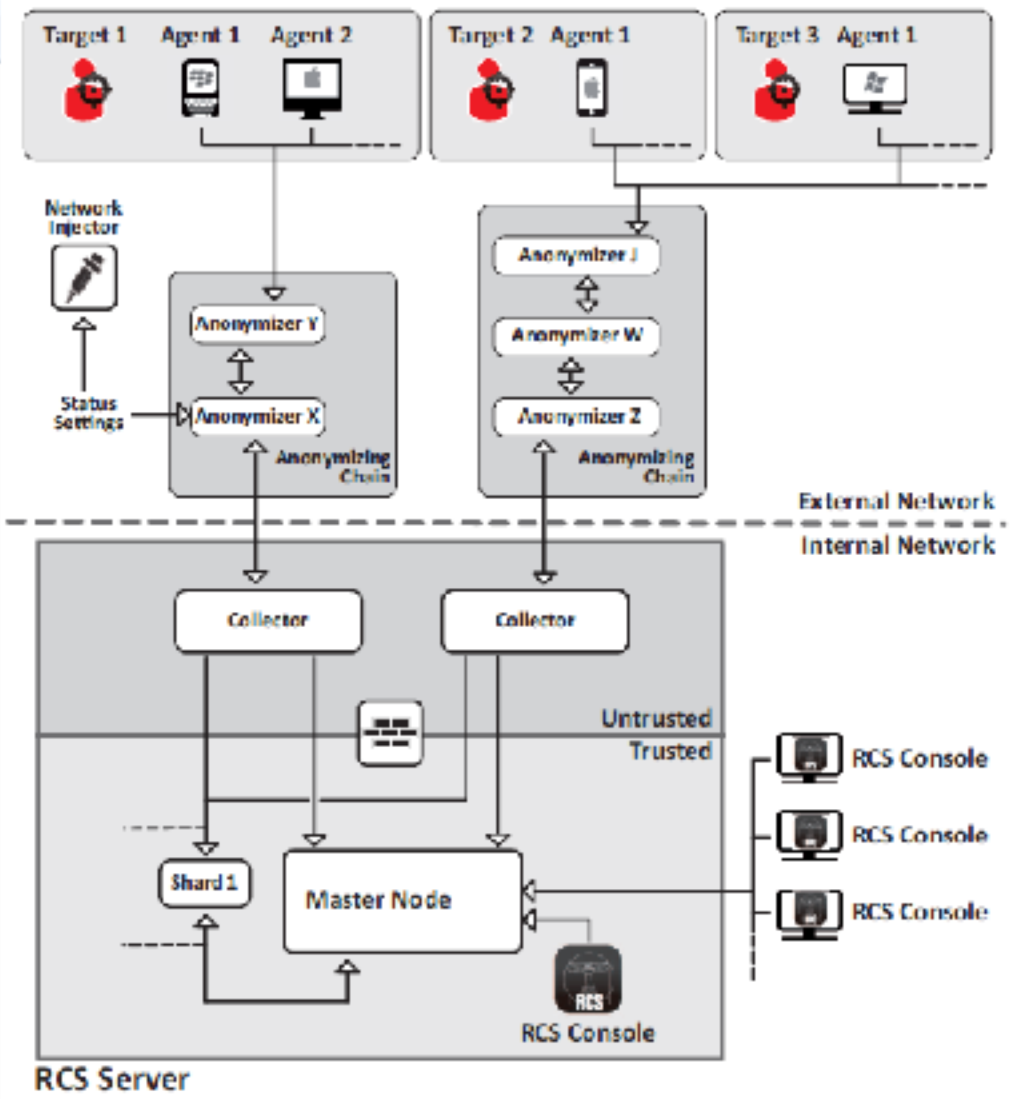
RCS Setup

Welcome to the RCS Setup Wizard

This wizard will guide you through the installation of RCS.

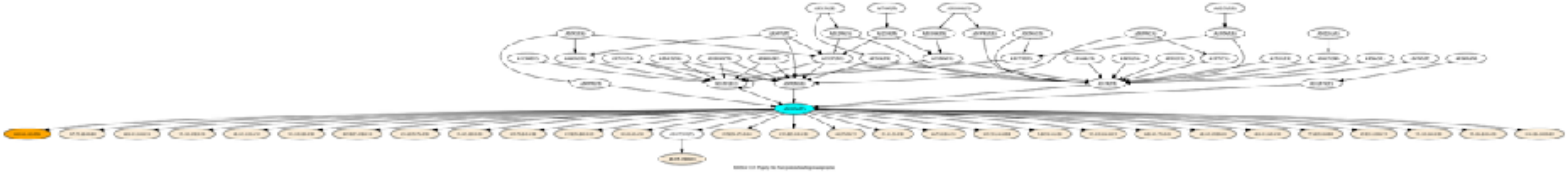
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

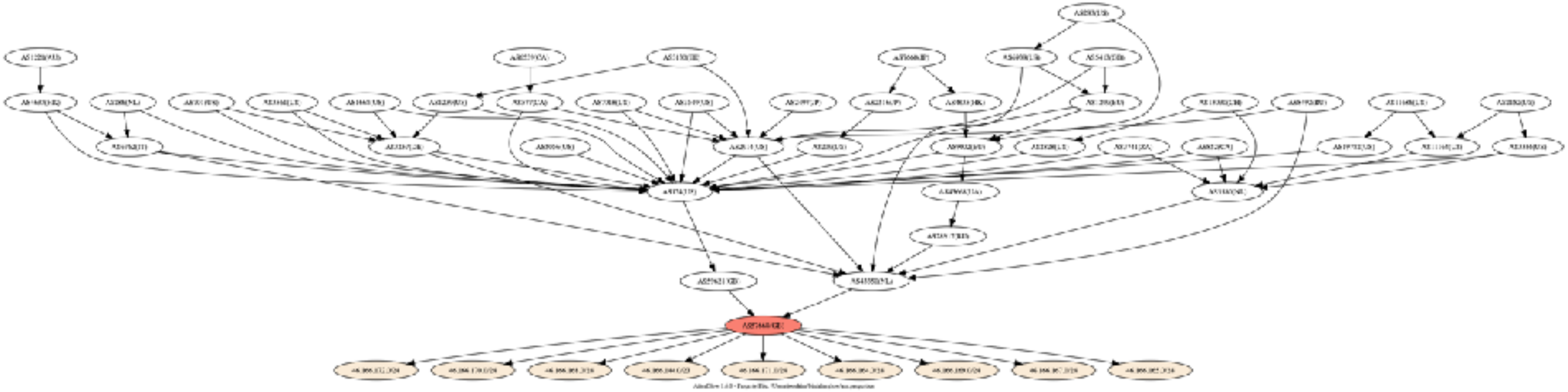
Click Next to continue.



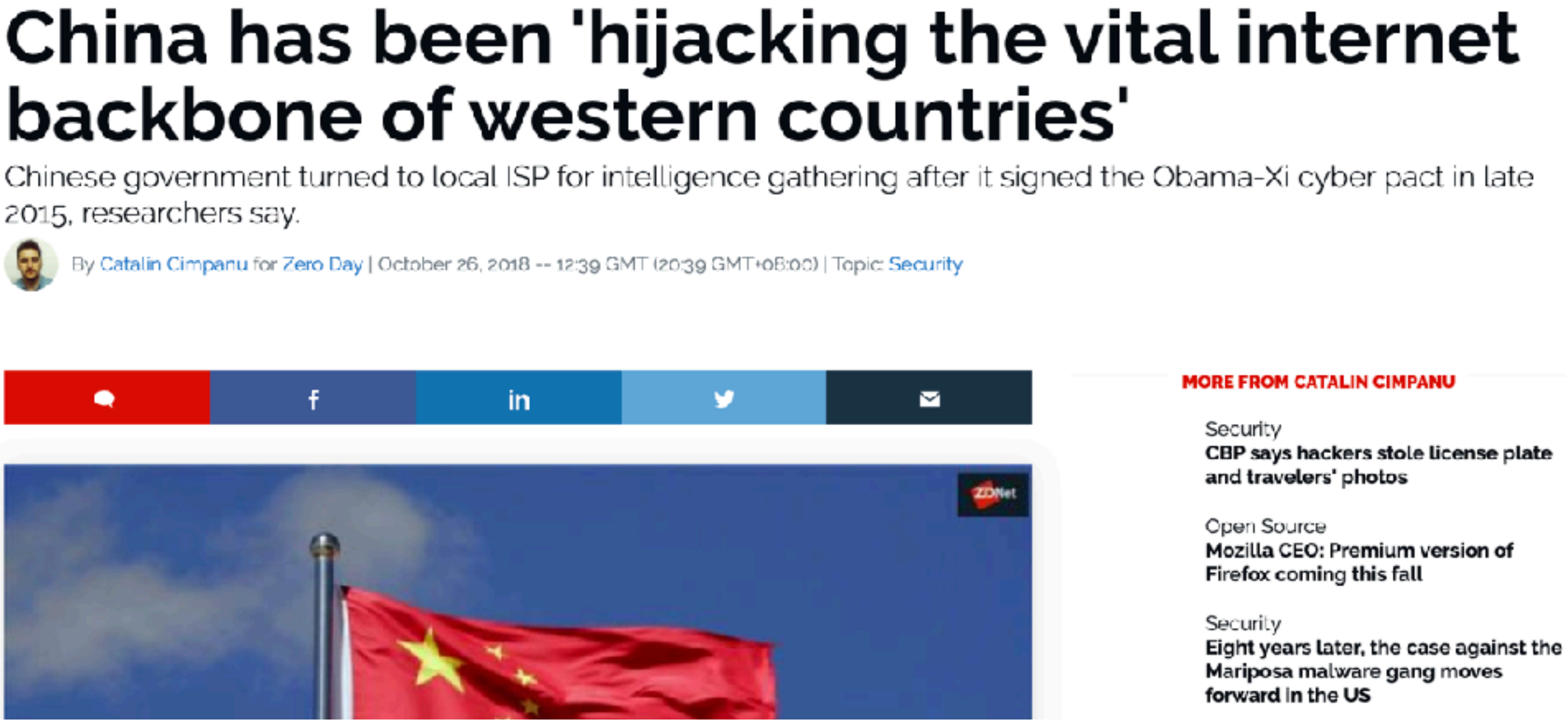
The Italian hacking group "Hacking Team" was involved in a state-sponsored BGP hijacking incident. They collaborated with the Italian Special Operations Group to manipulate the Border Gateway Protocol (BGP) and divert internet traffic.

BGP Hijacking Before and After





2016 BGP MITM by China



China has been 'hijacking the vital internet backbone of western countries'

Chinese government turned to local ISP for intelligence gathering after it signed the Obama-Xi cyber pact in late 2015, researchers say.

By Catalin Cimpanu for Zero Day | October 26, 2018 -- 12:39 GMT (20:39 GMT+08:00) | Topic: Security

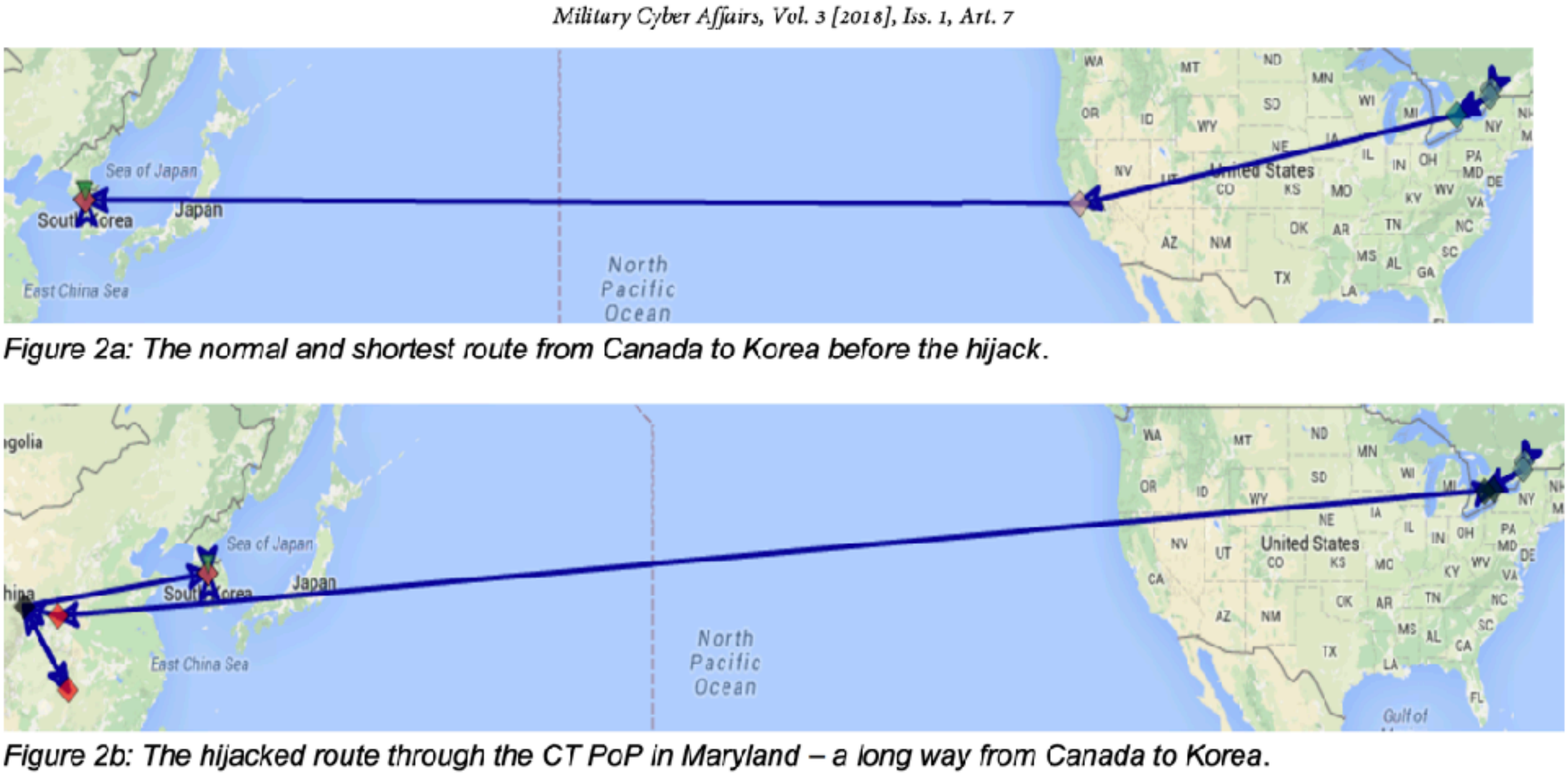
MORE FROM CATALIN CIMPANU

Security
CBP says hackers stole license plate and travelers' photos

Open Source
Mozilla CEO: Premium version of Firefox coming this fall

Security
Eight years later, the case against the Mariposa malware gang moves forward in the US

TRACEROUTE Based Apparoch

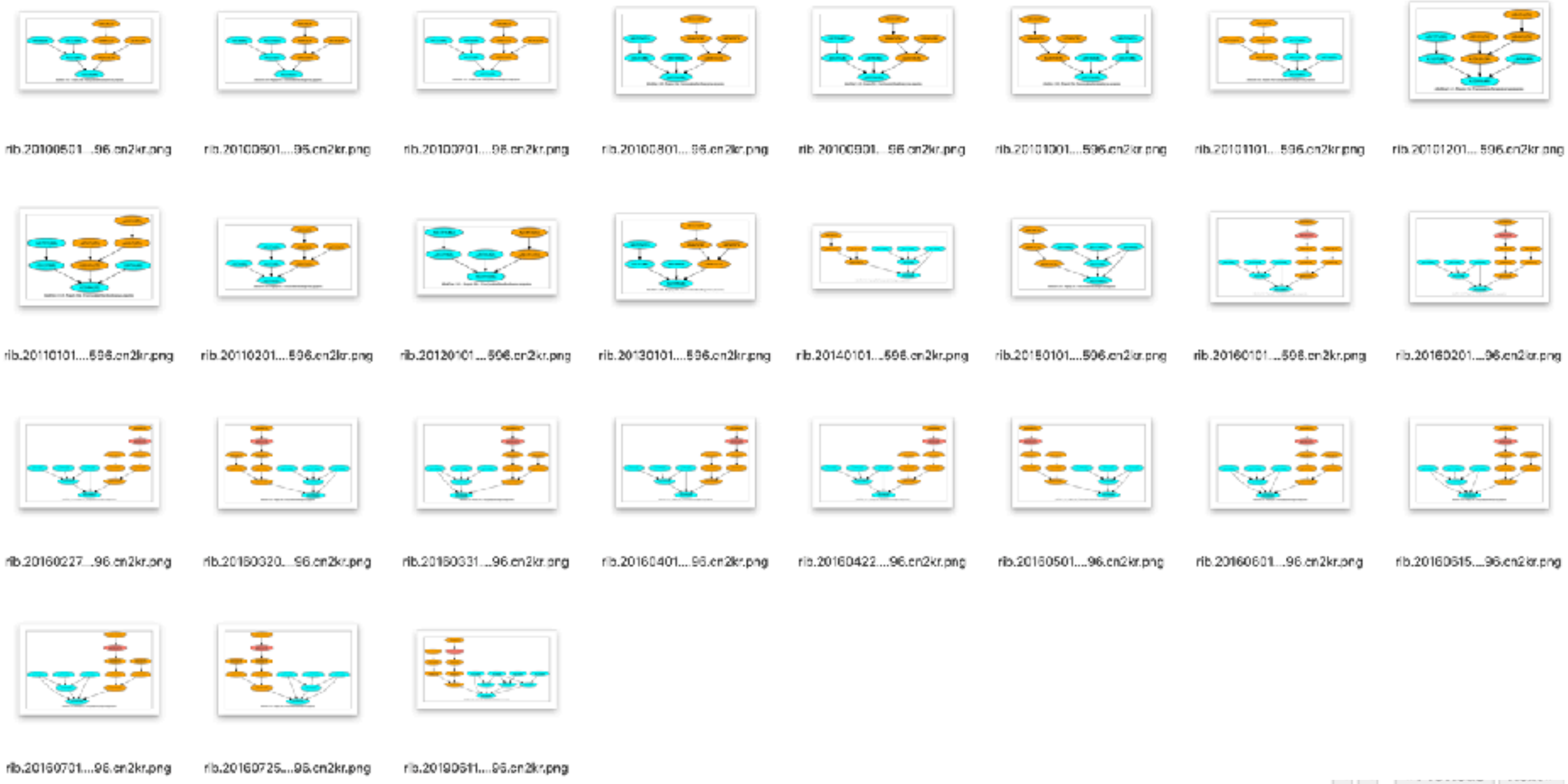


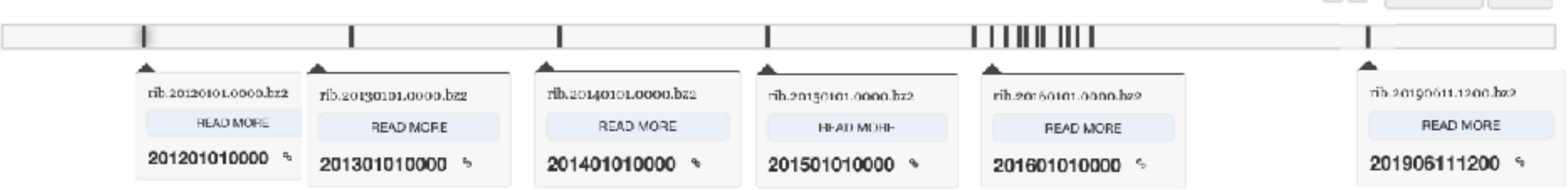
Military Cyber Affairs, Vol. 3 [2018], Iss. 1, Art. 7

Figure 2a: The normal and shortest route from Canada to Korea before the hijack.

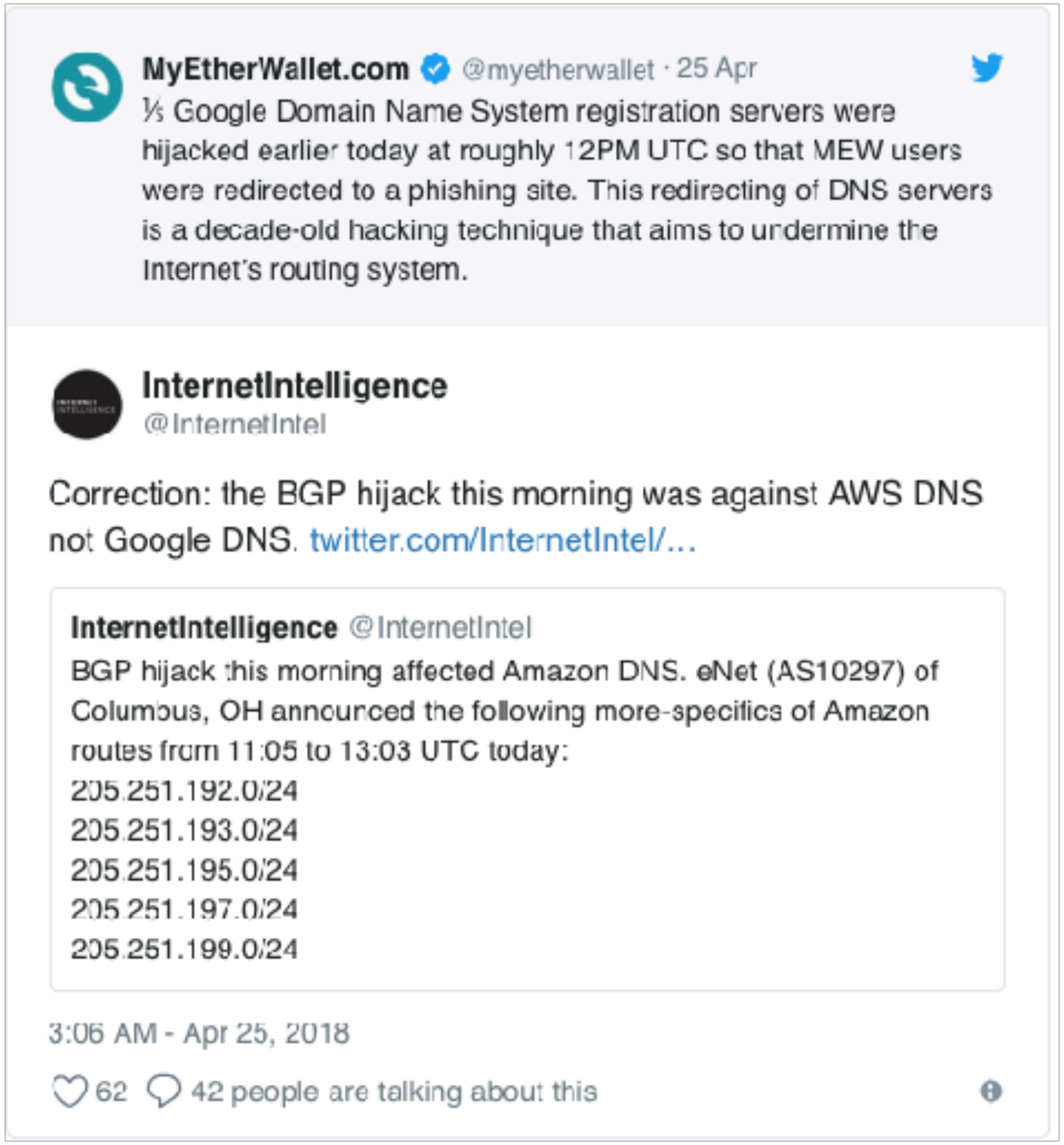
Figure 2b: The hijacked route through the CT PoP in Maryland – a long way from Canada to Korea.

Internet Routing Table based Approach


rib.20100501...96.cn2kr.png
rib.20100601....95.cn2kr.png
rib.20100701....96.cn2kr.png
rib.20100801....96.cn2kr.png
rib.20100901....96.cn2kr.png
rib.20101001....596.cn2kr.png
rib.20101101....596.cn2kr.png
rib.20101201....596.cn2kr.png
rib.20110101....596.cn2kr.png
rib.20110201....596.cn2kr.png
rib.20120101....506.cn2kr.png
rib.20130101....596.cn2kr.png
rib.20140101....596.cn2kr.png
rib.20150101....506.cn2kr.png
rib.20160101....596.cn2kr.png
rib.20160201....96.cn2kr.png
rib.20160227...96.cn2kr.png
rib.20160320....96.cn2kr.png
rib.20160331....96.cn2kr.png
rib.20160401....96.cn2kr.png
rib.20160422....96.cn2kr.png
rib.20160501....96.cn2kr.png
rib.20160601....96.cn2kr.png
rib.20160615....96.cn2kr.png
rib.20160701....96.cn2kr.png
rib.20160725....96.cn2kr.png
rib.20190611....96.cn2kr.png



2018 Amazon DNS BGP Hijacking



MyEtherWallet.com @myetherwallet · 25 Apr

⅓ Google Domain Name System registration servers were hijacked earlier today at roughly 12PM UTC so that MEW users were redirected to a phishing site. This redirecting of DNS servers is a decade-old hacking technique that aims to undermine the Internet's routing system.

InternetIntelligence
@InternetIntel

Correction: the BGP hijack this morning was against AWS DNS not Google DNS. twitter.com/InternetIntel/...

InternetIntelligence @InternetIntel
BGP hijack this morning affected Amazon DNS. eNet (AS10297) of Columbus, OH announced the following more-specifics of Amazon routes from 11:05 to 13:03 UTC today:
205.251.192.0/24
205.251.193.0/24
205.251.195.0/24
205.251.197.0/24
205.251.199.0/24

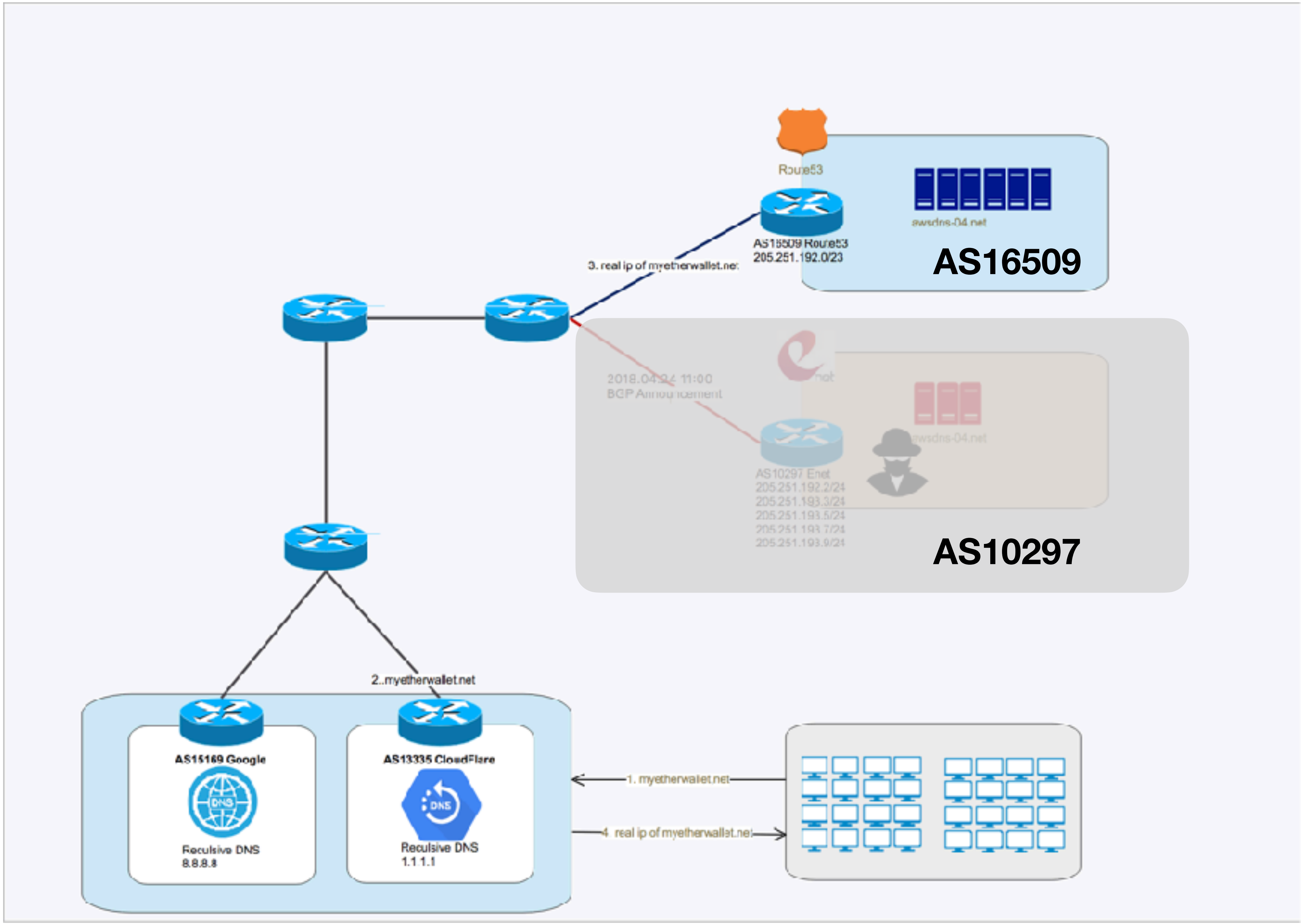
3:06 AM - Apr 25, 2018

♡ 62 42 people are talking about this

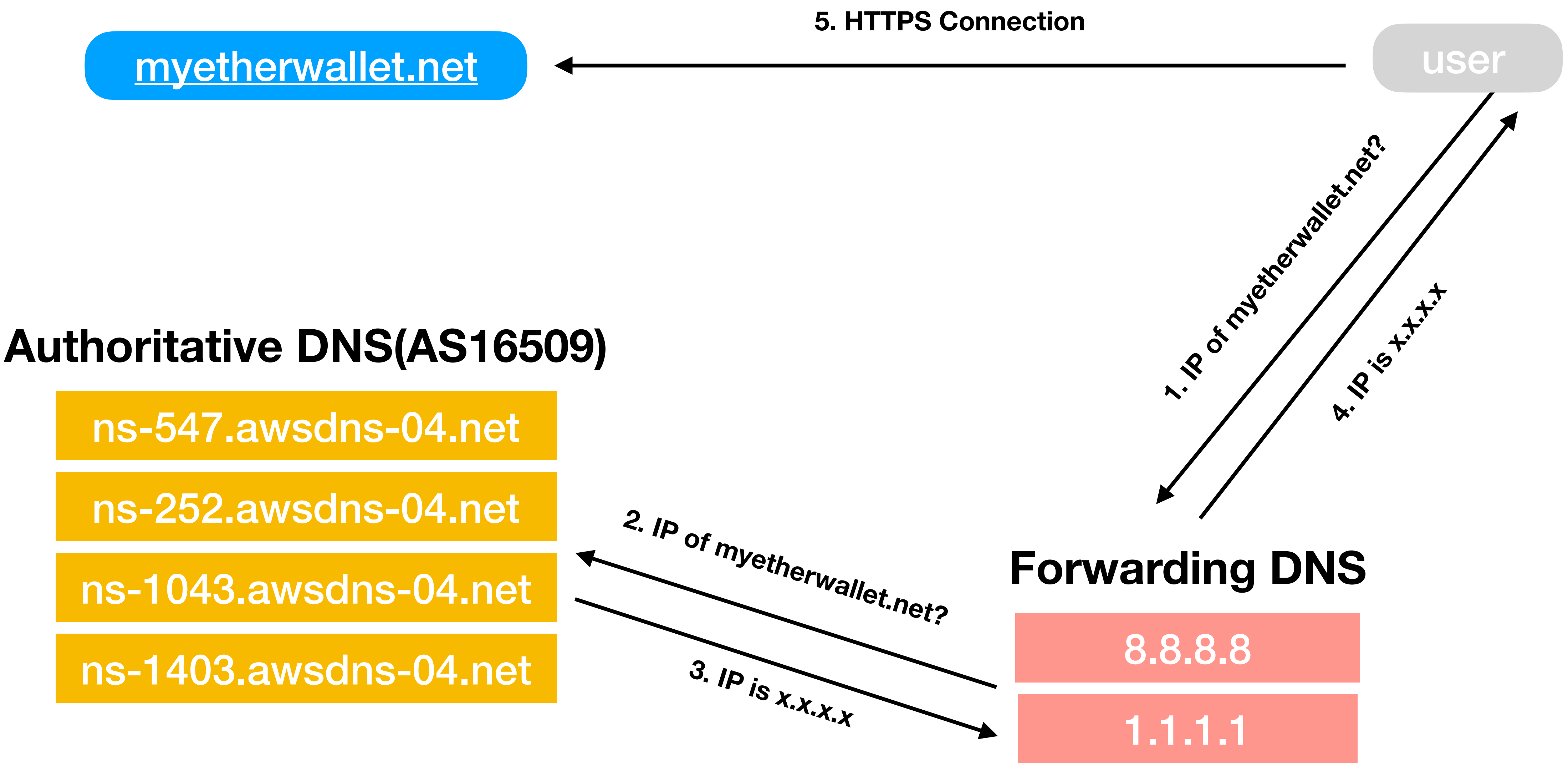
- myetherwallet.com reports AWD DNS Hijacking on the same day On 24th April, 2018 Amazon /24 x 4 Networks are BGP Hijacked
- eNet(AS 10297) of Columbus, OH announced more specific of Amazon Route from 11:05 to 13:03 UTC
- 205.251.192.0/24, 205.251.193.0/24, 205.251.195.0/24, 205.251.197.0/24, 205.251.199.0/24

Reference : https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/

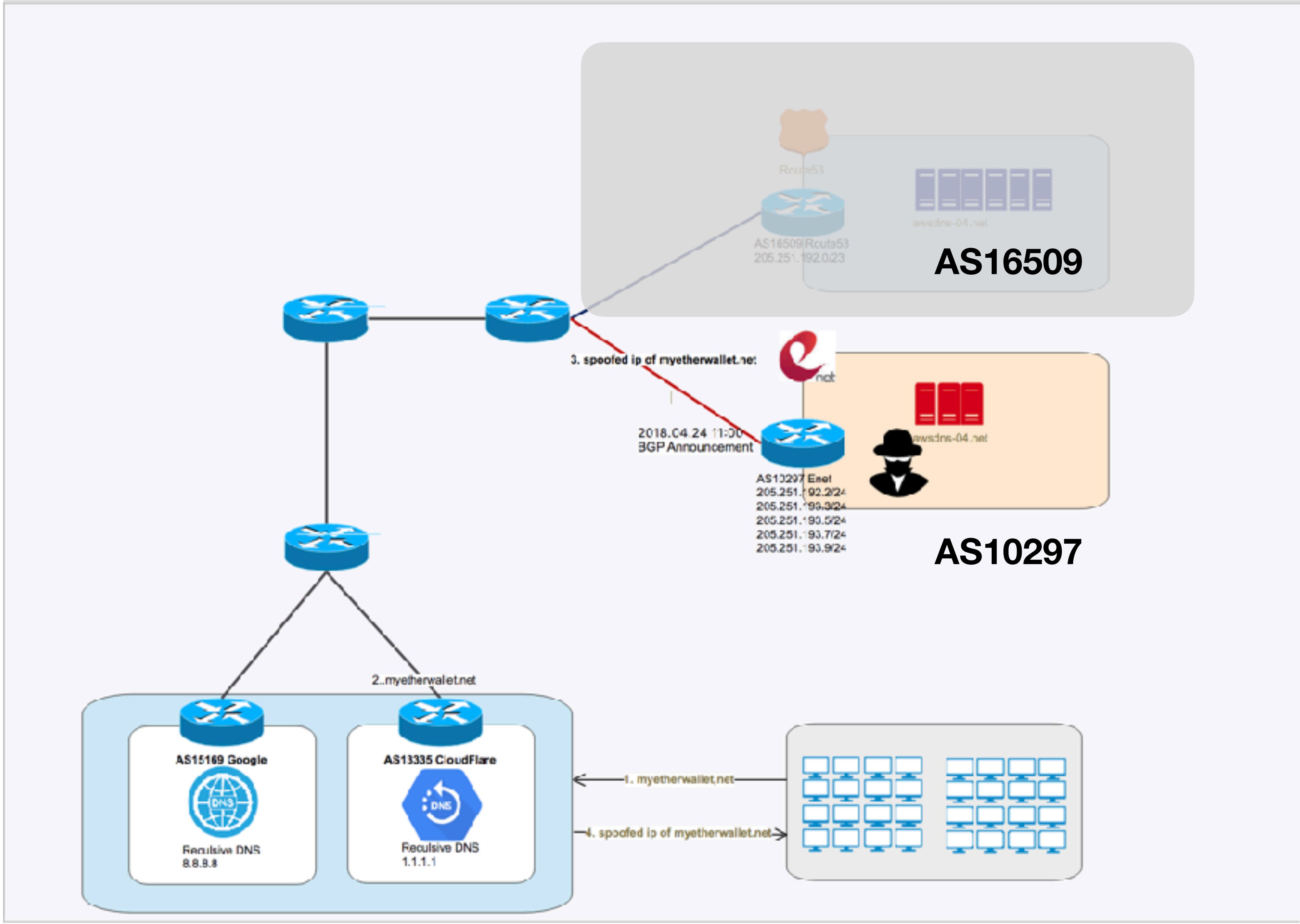
Hijacked Operation(BEFORE)



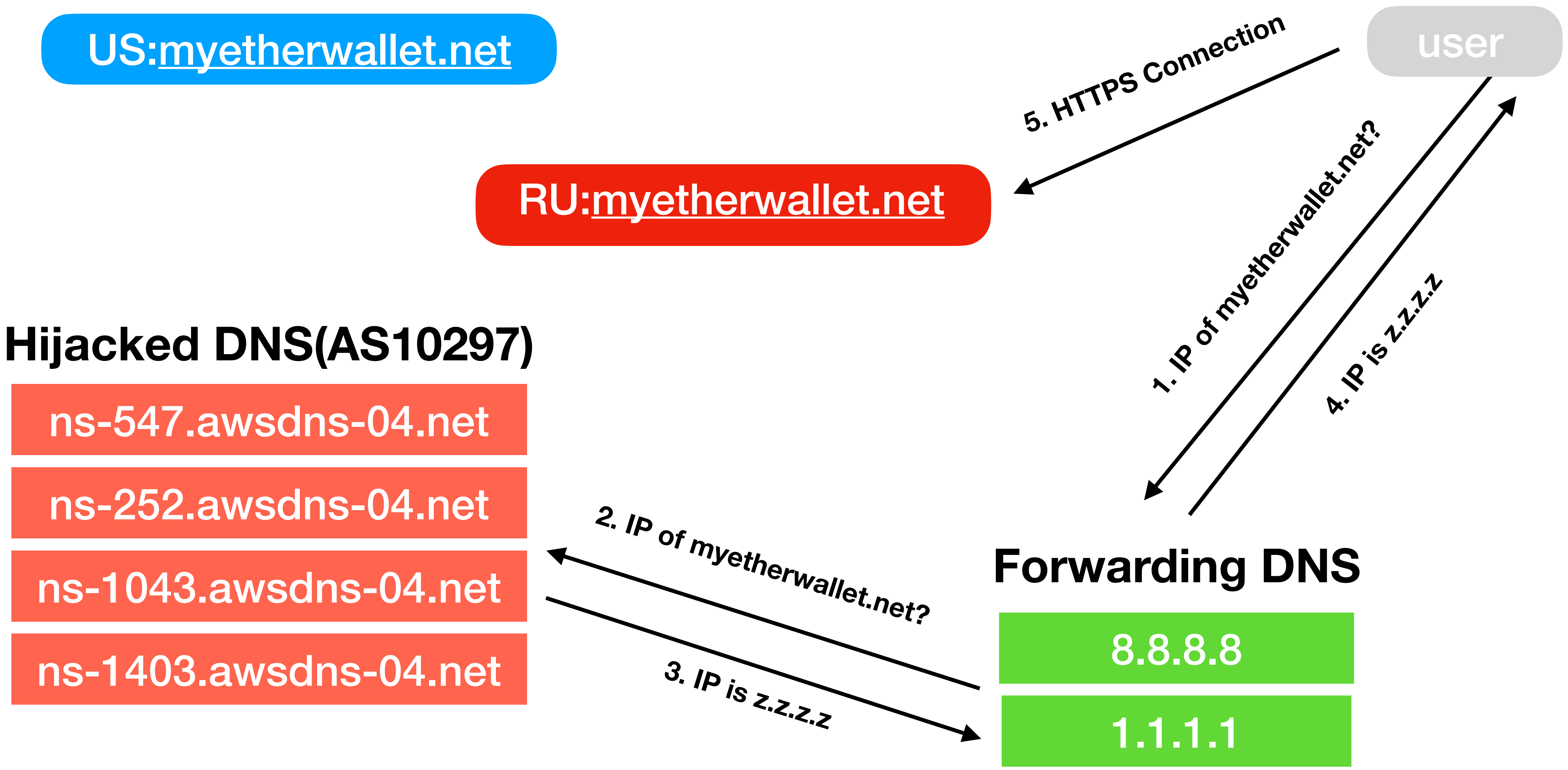
Normal Operation(DNS Layer)



Hijacked Operation(BEFORE)



Hijacked Operation(DNS Layer)



US:myetherwallet.net

user

5. HTTPS Connection

RU:myetherwallet.net

1. IP of myetherwallet.net?

4. IP is z.z.z.z

Hijacked DNS(AS10297)

ns-547.awsdns-04.net

ns-252.awsdns-04.net

ns-1043.awsdns-04.net

ns-1403.awsdns-04.net

2. IP of myetherwallet.net?

3. IP is z.z.z.z

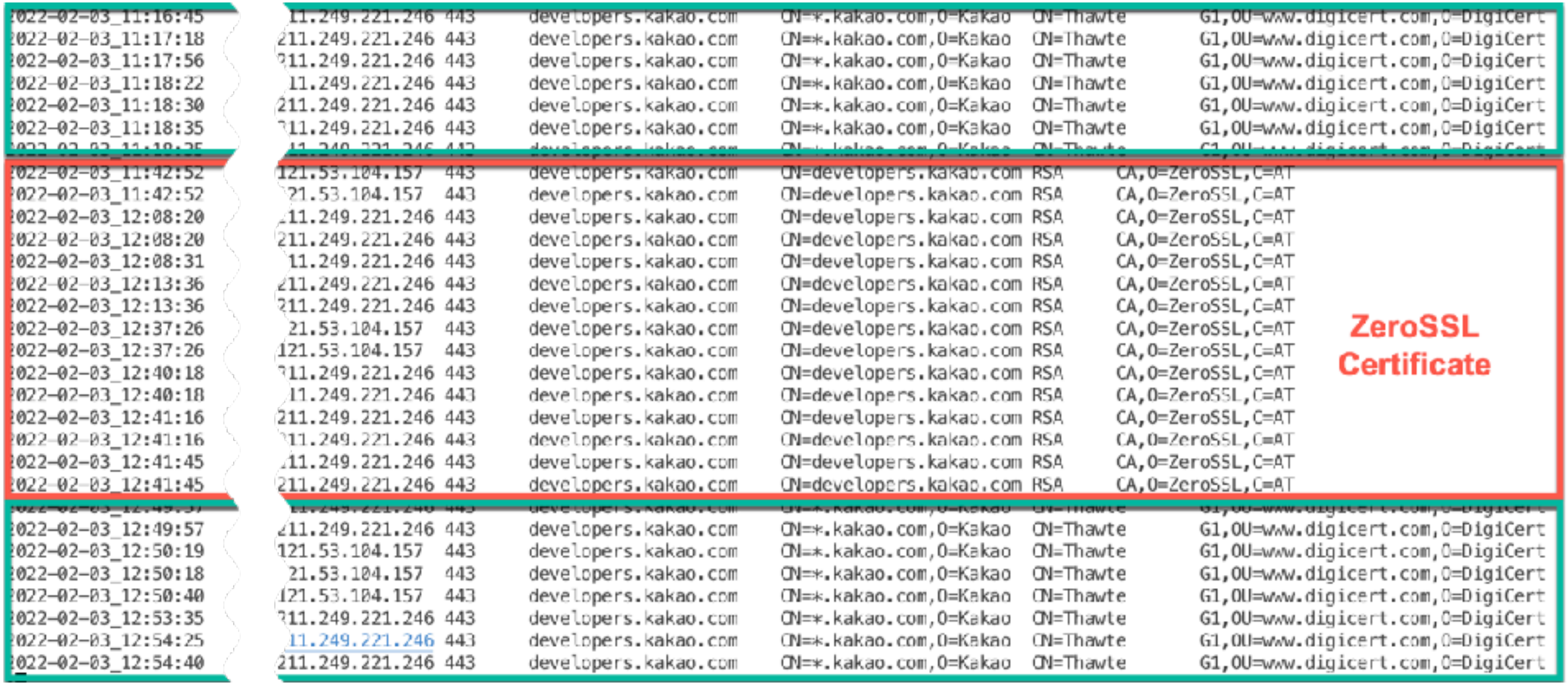
Forwarding DNS

8.8.8.8

1.1.1.1

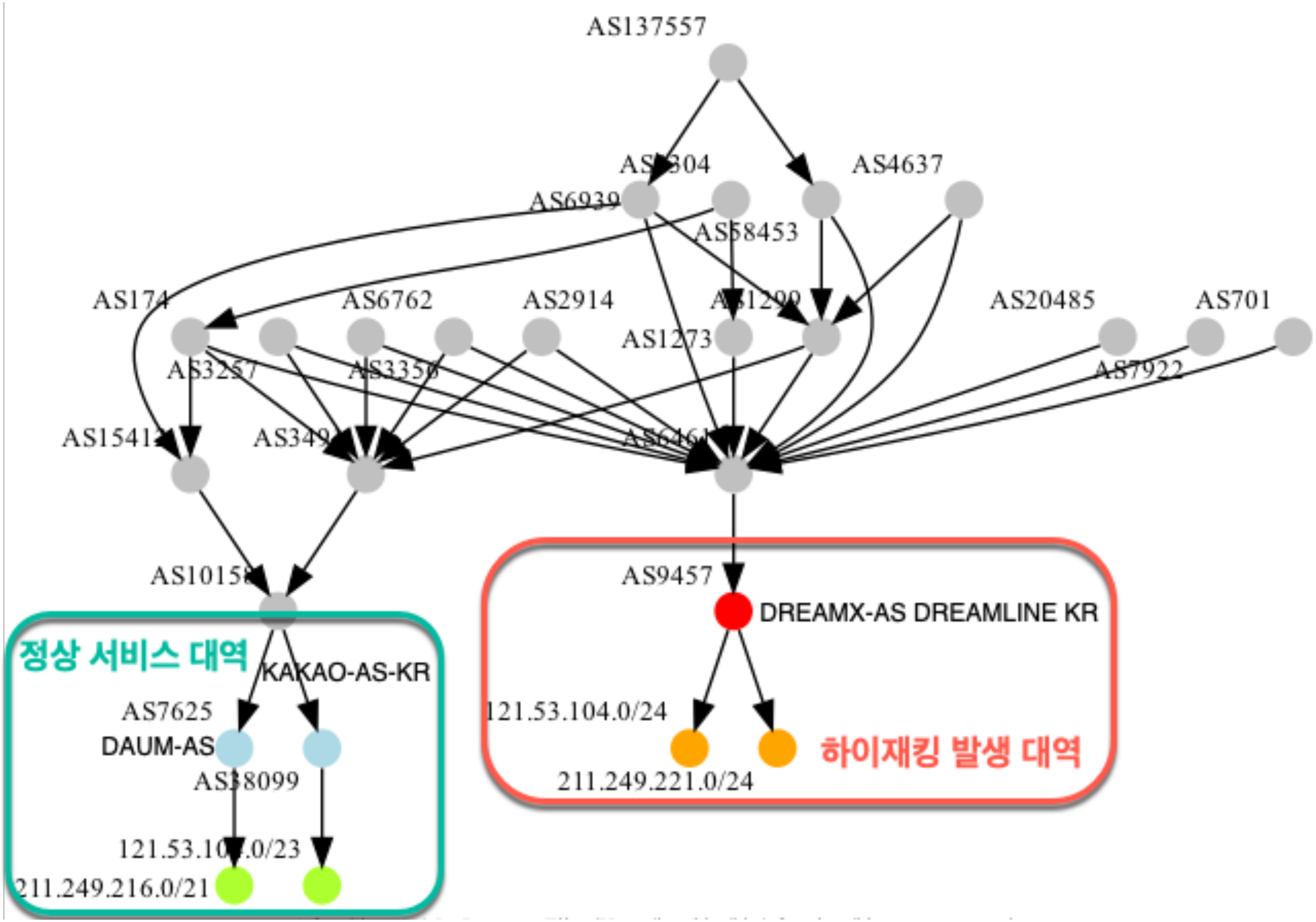
Activation of ZeroSSL Certificate

developers.kakao.com SSL Certificate



```
2022-02-03_11:16:45   11.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:17:18  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:17:56  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:18:22   11.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:18:30  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:18:35  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:18:35   11.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_11:42:52  121.53.104.157  443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_11:42:52   21.53.104.157  443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:08:20   11.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:08:20  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:08:31   11.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:13:36  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:13:36  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:37:26   21.53.104.157  443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:37:26  121.53.104.157  443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:40:18  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:40:18   11.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:41:16  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:41:16  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:41:45   11.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:41:45  211.249.221.246 443   developers.kakao.com   CN=developers.kakao.com RSA   CA,O=ZeroSSL,C=AT
2022-02-03_12:49:57   11.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:49:57  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:50:19  121.53.104.157  443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:50:18   21.53.104.157  443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:50:40  121.53.104.157  443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:53:35  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:54:25   11.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
2022-02-03_12:54:40  211.249.221.246 443   developers.kakao.com   CN=*.kakao.com,O=Kakao  CN=Thawte       G1,OU=www.digicert.com,O=DigiCert
```

Incident Analysis



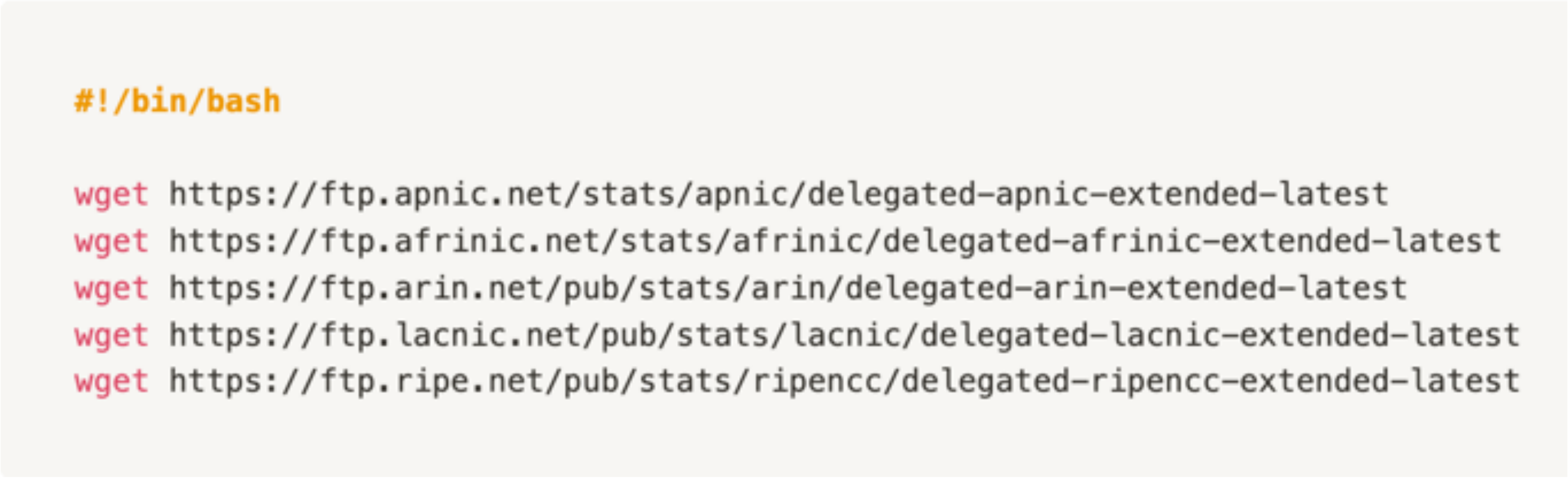
Warming Up

Basic Skills

1. Handling RIR Database

Command to learn: wget

Retrieve the most current Internet address allocation data from each Regional Internet Registry.

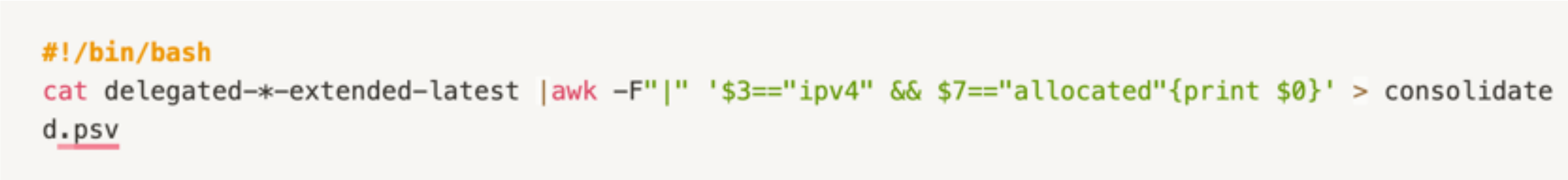


```
#!/bin/bash

wget https://ftp.apnic.net/stats/apnic/delegated-apnic-extended-latest
wget https://ftp.afrinic.net/stats/afrinic/delegated-afrinic-extended-latest
wget https://ftp.arin.net/pub/stats/arin/delegated-arin-extended-latest
wget https://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-latest
wget https://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-extended-latest
```

Basic Skills

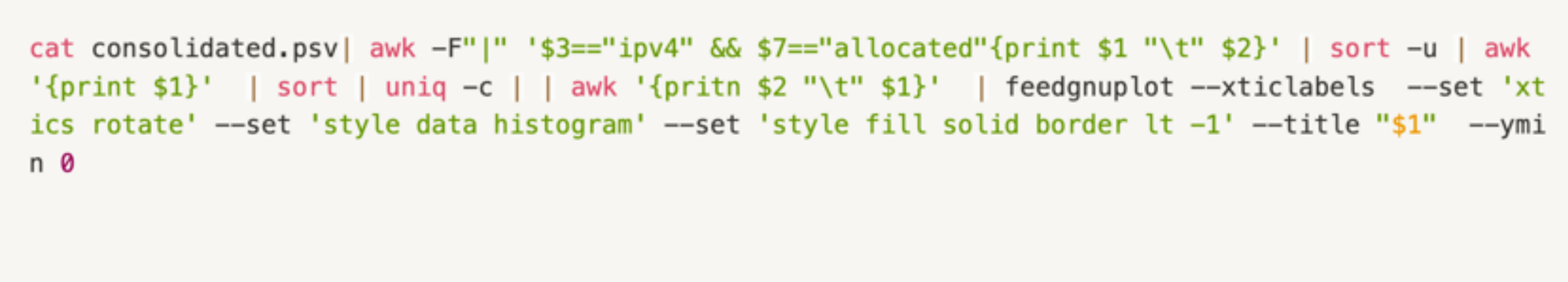
Handling RIR Database

Consolidate all allocated ipv4 record from the downloaded RIR data into a single file.



```
#!/bin/bash
cat delegated-*-extended-latest |awk -F"|" '$3=="ipv4" && $7=="allocated"{print $0}' > consolidate
d.psv
```

Illustrate the distribution of Countries of which IPv4 addresses allocated with respect to Regional Internet Registries.

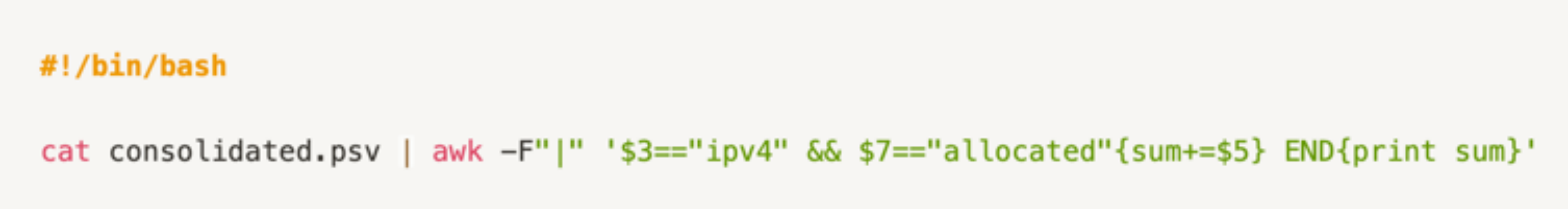


```
cat consolidated.psv| awk -F"|" '$3=="ipv4" && $7=="allocated"{print $1 "\t" $2}' | sort -u | awk
'{print $1}'  | sort | uniq -c | | awk '{pritn $2 "\t" $1}'  | feedgnuplot --xticlabels  --set 'xt
ics rotate' --set 'style data histogram' --set 'style fill solid border lt -1' --title "$1"  --ymi
n 0
```

Basic Skills

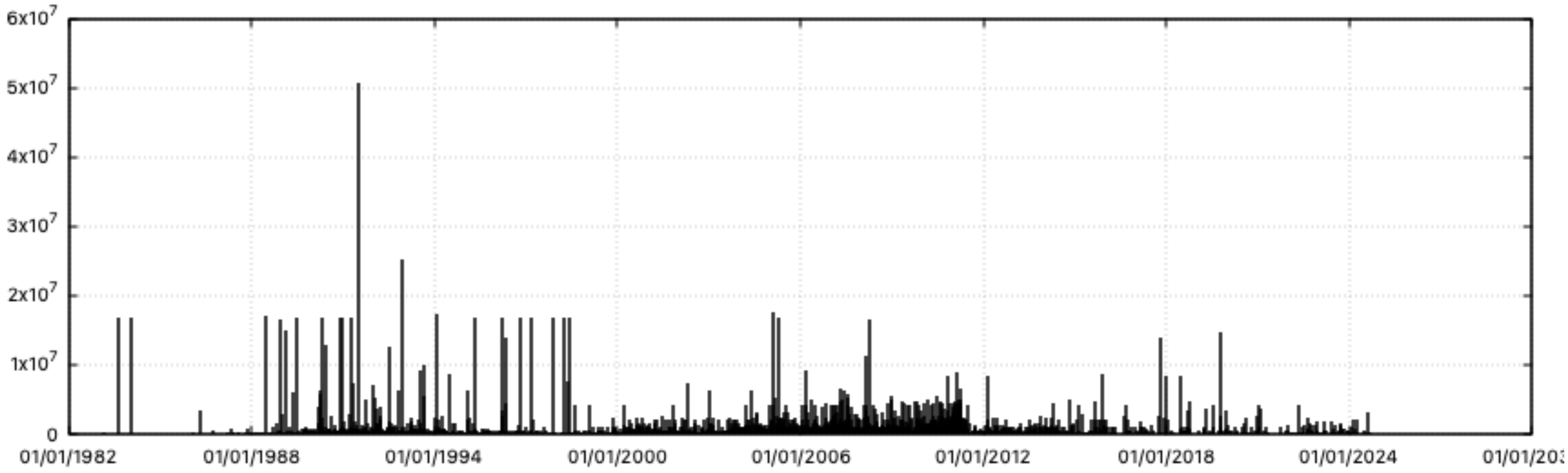
Handling RIR Database

As of today, how many IPv4 addresses have been allocated in total on the day?



```
#!/bin/bash

cat consolidated.psv | awk -F"|" '$3=="ipv4" && $7=="allocated"{sum+=$5} END{print sum}'
```

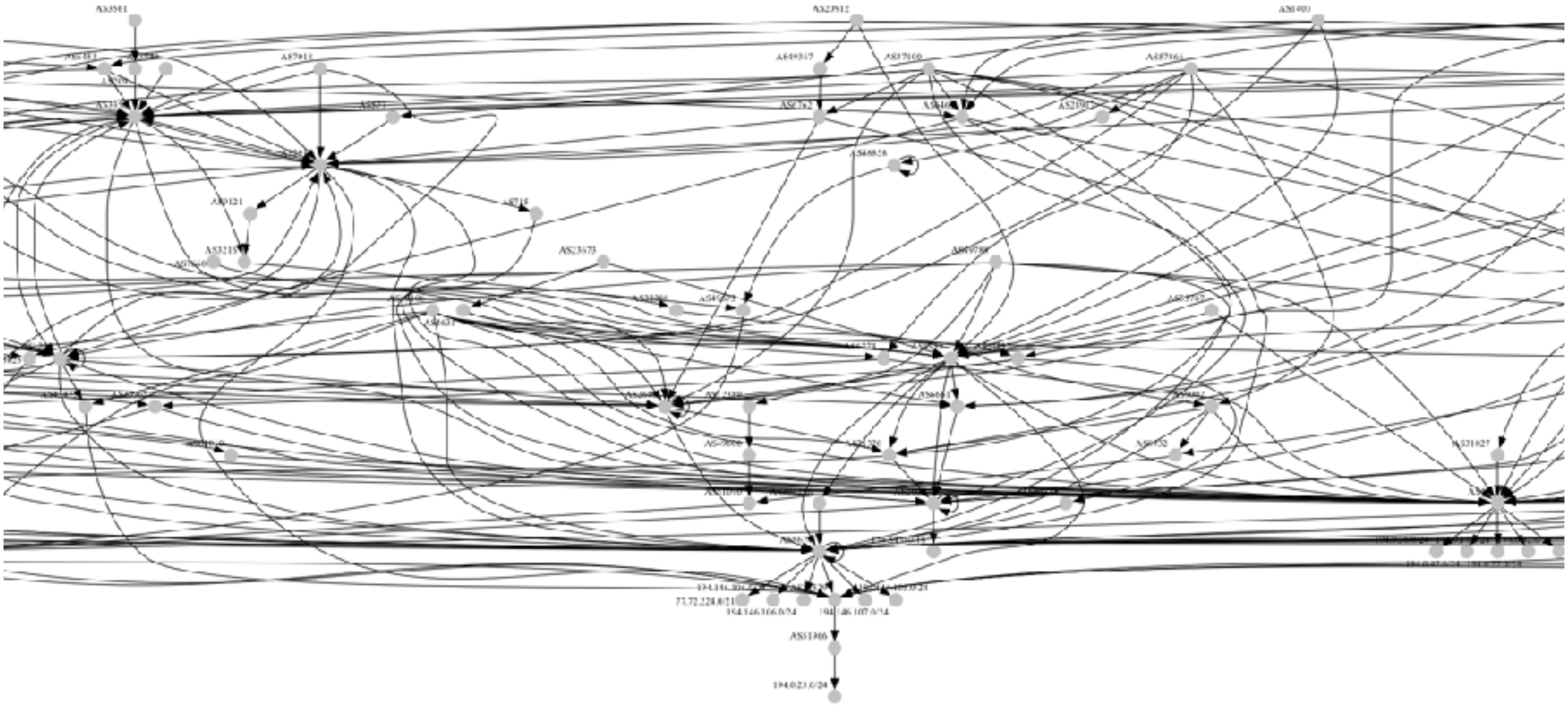
Visualize Yearly IP allocation trends



Basic Skills

2. The Internet Route Visualization

Visualize the Internet ROUTE to Luxembourg DNS



What else you can do with Command-Line Analysis

- DDoS Detection and Analysis
- Webshell Detection
- SQL Injection Analysis
- Compromised Assets Detection
- Attacker Infra Tracking
- Command and Control Detection
- RAT Backdoor Detection
- Data Exfiltration Detection
- State-Sponsored Cyber Adversaries Tracking

Basic Skills

codepresso.io

code.presso

Only for Today's Attendees!

Upon Registration,
Get FREE Access to Our
Cybersecurity Training!

BGP Hijacking Detection

State-Sponsored BGP Hijacking

Incident Description

In **Aug 2013**, the Italian surveillance software company Hacking Team was involved in a significant incident of BGP (Border Gateway Protocol)

It is hijacking against the subnet of **46.166.163.0/24** from the notorious Bulletproof-hosting provider Santrex. BGP hijacking involves manipulating internet routing tables to misdirect traffic intended for a specific IP range to an unexpected destination. This can intercept data, reroute traffic for surveillance, or disrupt services.

In this case, it was reported that the Hacking Team used BGP hijacking to redirect traffic for their purposes, likely as part of their cyber surveillance and intelligence-gathering activities.

State-Sponsored BGP Hijacking

Who Owns the prefix 46.166.163.0/24

```
whois -h whois.cymru.com “ 46.166.163.0 ”
```

```
16125|46.166.163.0|46.166.160.0/21|LT|ripencc|2010-12-16|CHERRYSERVERS1-AS, LT
```

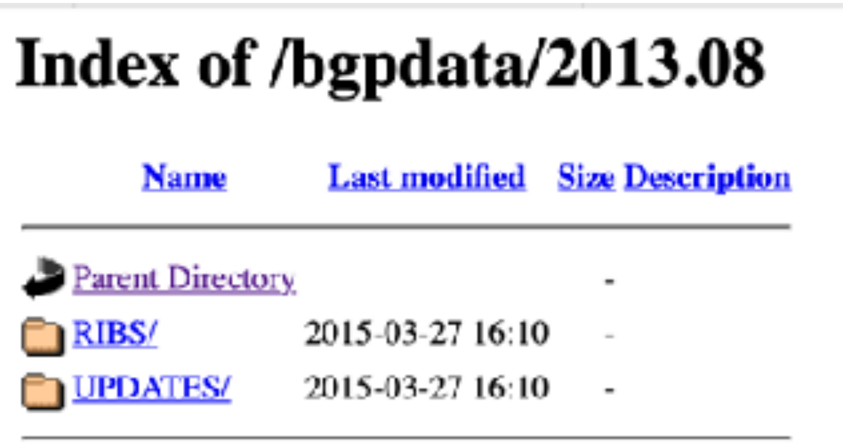
```
wget https://ftp.ripe.net/pub/stats/ripencc/2013/delegated-ripencc-20130801.bz2
```

```
bzcat delegated-ripencc-20130801.bz2 | awk -F"|" '$4~/^46.166/{print $0}'
```

- As the hijacked prefix was 46.166.163.0/24, we should look up prefixes with the preceding 46.166 from the bz2file
- Three allocated IP blocks satisfy the condition.
- As 16,384 is 2 to the power of 14, 32-14 is the subnet mask, and which is 18
- Prefix of the network address is 46.166.128.0/18
- The ipv4 record that satisfies the condition has been allocated to GB since 20101216

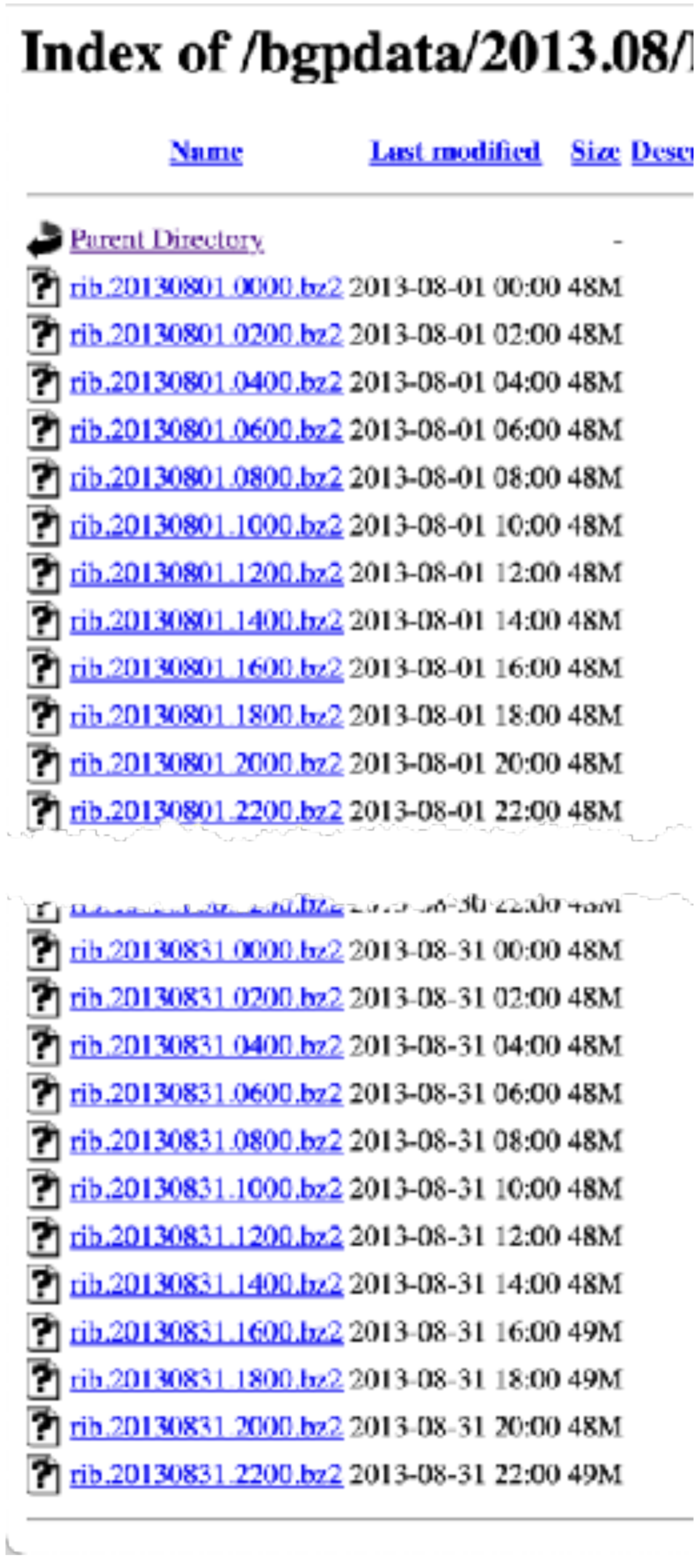
State-Sponsored BGP Hijacking

University of Oregon Route View Archive Project



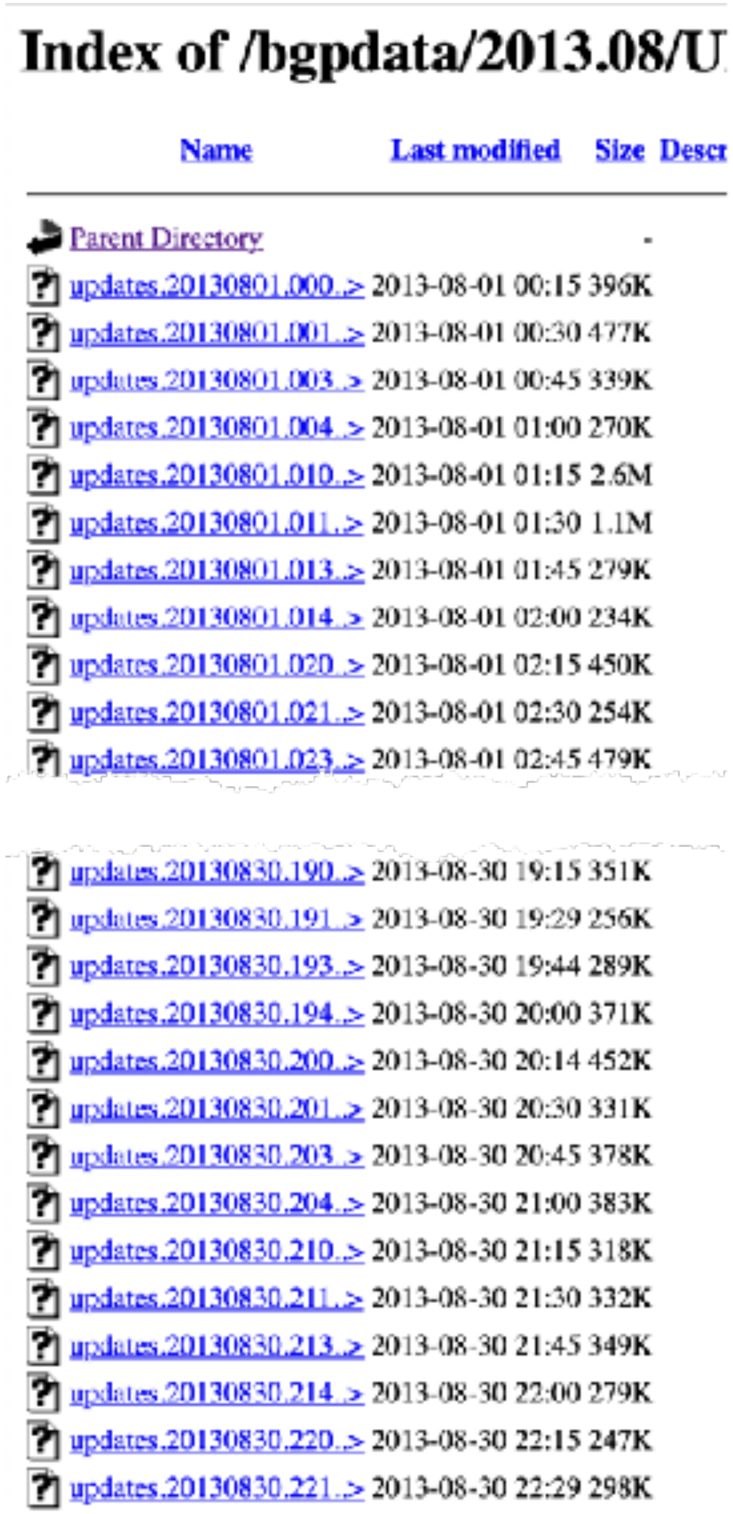
Index of /bgpdata/2013.08

Name	Last modified	Size	Description
Parent Directory		-	
RIBS/	2015-03-27 16:10	-	
UPDATES/	2015-03-27 16:10	-	



Index of /bgpdata/2013.08/

Name	Last modified	Size	Desc
Parent Directory		-	
rib.20130801.0000.bz2	2013-08-01 00:00	48M	
rib.20130801.0200.bz2	2013-08-01 02:00	48M	
rib.20130801.0400.bz2	2013-08-01 04:00	48M	
rib.20130801.0600.bz2	2013-08-01 06:00	48M	
rib.20130801.0800.bz2	2013-08-01 08:00	48M	
rib.20130801.1000.bz2	2013-08-01 10:00	48M	
rib.20130801.1200.bz2	2013-08-01 12:00	48M	
rib.20130801.1400.bz2	2013-08-01 14:00	48M	
rib.20130801.1600.bz2	2013-08-01 16:00	48M	
rib.20130801.1800.bz2	2013-08-01 18:00	48M	
rib.20130801.2000.bz2	2013-08-01 20:00	48M	
rib.20130801.2200.bz2	2013-08-01 22:00	48M	
[illegible].bz2	[illegible]-30 22:00	48M	
rib.20130831.0000.bz2	2013-08-31 00:00	48M	
rib.20130831.0200.bz2	2013-08-31 02:00	48M	
rib.20130831.0400.bz2	2013-08-31 04:00	48M	
rib.20130831.0600.bz2	2013-08-31 06:00	48M	
rib.20130831.0800.bz2	2013-08-31 08:00	48M	
rib.20130831.1000.bz2	2013-08-31 10:00	48M	
rib.20130831.1200.bz2	2013-08-31 12:00	48M	
rib.20130831.1400.bz2	2013-08-31 14:00	48M	
rib.20130831.1600.bz2	2013-08-31 16:00	49M	
rib.20130831.1800.bz2	2013-08-31 18:00	49M	
rib.20130831.2000.bz2	2013-08-31 20:00	48M	
rib.20130831.2200.bz2	2013-08-31 22:00	49M	



Index of /bgpdata/2013.08/U

Name	Last modified	Size	Descr
Parent Directory		-	
updates.20130801.000..>	2013-08-01 00:15	396K	
updates.20130801.001..>	2013-08-01 00:30	477K	
updates.20130801.003..>	2013-08-01 00:45	339K	
updates.20130801.004..>	2013-08-01 01:00	270K	
updates.20130801.010..>	2013-08-01 01:15	2.6M	
updates.20130801.011..>	2013-08-01 01:30	1.1M	
updates.20130801.013..>	2013-08-01 01:45	279K	
updates.20130801.014..>	2013-08-01 02:00	234K	
updates.20130801.020..>	2013-08-01 02:15	450K	
updates.20130801.021..>	2013-08-01 02:30	254K	
updates.20130801.023..>	2013-08-01 02:45	479K	
updates.20130830.190..>	2013-08-30 19:15	351K	
updates.20130830.191..>	2013-08-30 19:29	256K	
updates.20130830.193..>	2013-08-30 19:44	289K	
updates.20130830.194..>	2013-08-30 20:00	371K	
updates.20130830.200..>	2013-08-30 20:14	452K	
updates.20130830.201..>	2013-08-30 20:30	331K	
updates.20130830.203..>	2013-08-30 20:45	378K	
updates.20130830.204..>	2013-08-30 21:00	383K	
updates.20130830.210..>	2013-08-30 21:15	318K	
updates.20130830.211..>	2013-08-30 21:30	332K	
updates.20130830.213..>	2013-08-30 21:45	349K	
updates.20130830.214..>	2013-08-30 22:00	279K	
updates.20130830.220..>	2013-08-30 22:15	247K	
updates.20130830.221..>	2013-08-30 22:29	298K	

State-Sponsored BGP Hijacking

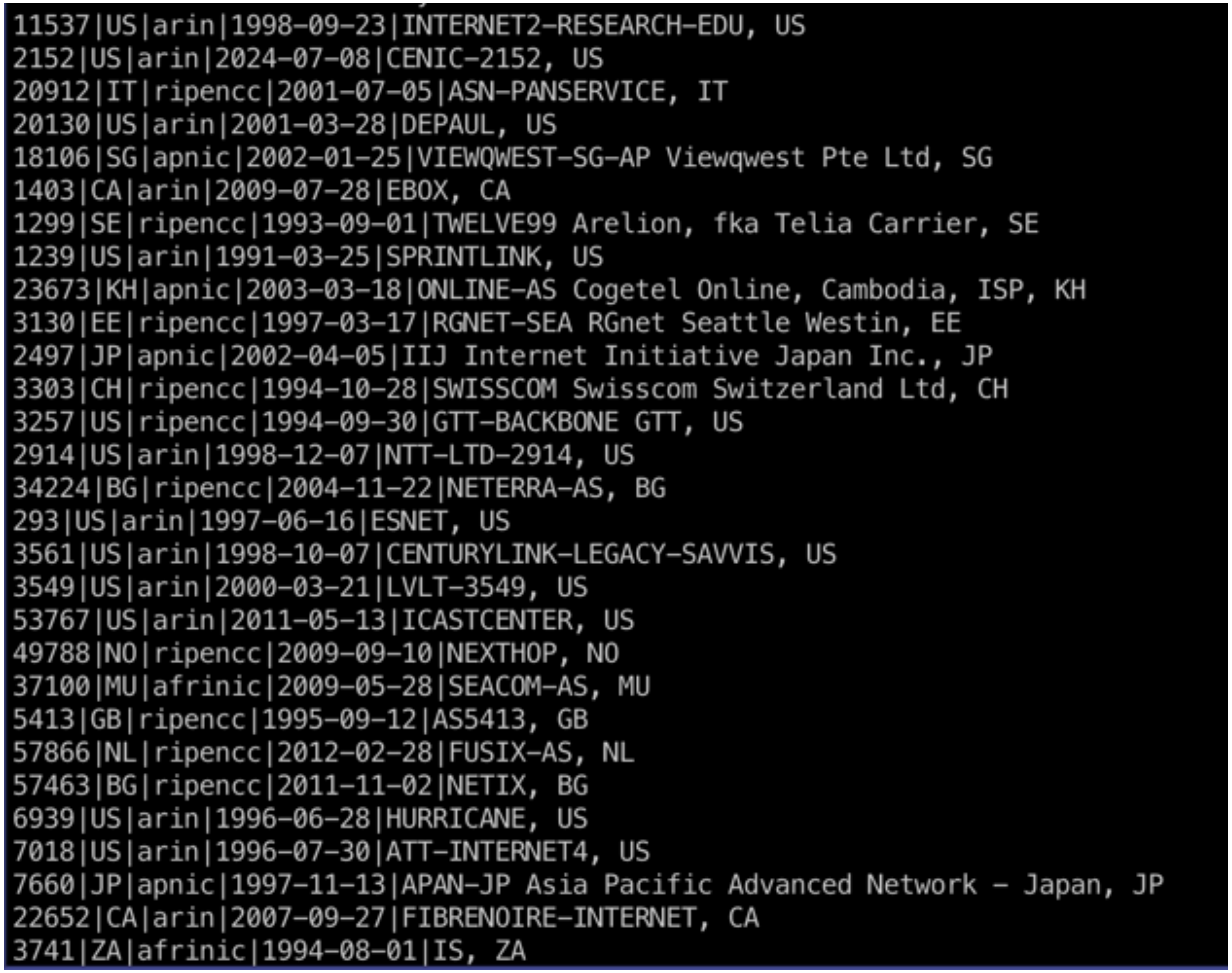
https://archive.routeviews.org/bgpdata/2013.08/UPDATES/

- updates.20130701.0115.bz2
- updates.20130703.0400.bz2
- updates.20130703.0645.bz2
- updates.20130703.0700.bz2
- updates.20130703.0830.bz2
- updates.20130816.0930.bz2
- updates.20130821.0300.bz2
- updates.20130821.0400.bz2
- updates.20130822.0730.bz2
- updates.20130822.1330.bz2

State-Sponsored BGP Hijacking

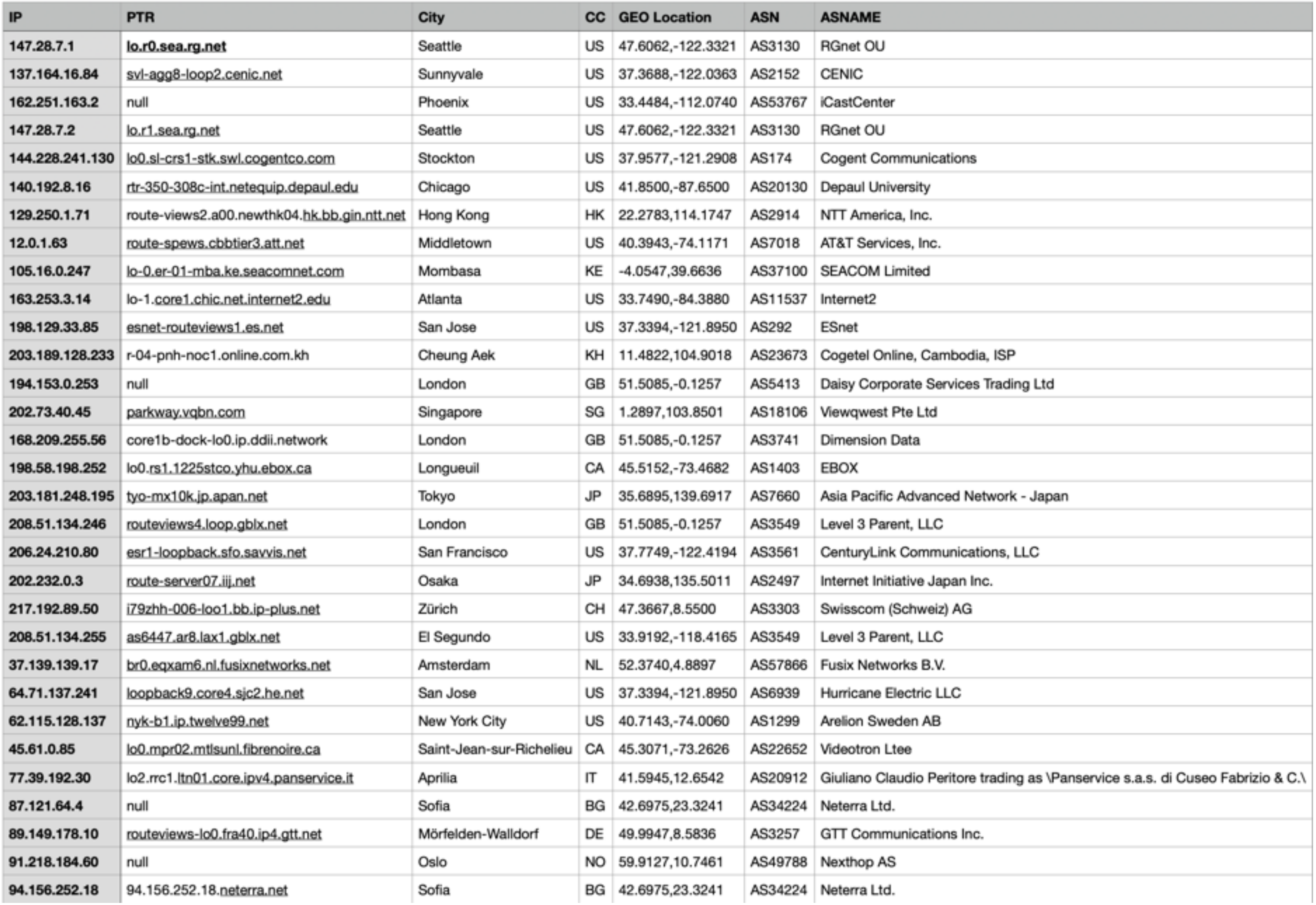
University of Oregon Route View Archive Project

- ASN having BGP Sensors (270,006,254 Lines)



```
11537|US|arin|1998-09-23|INTERNET2-RESEARCH-EDU, US
2152|US|arin|2024-07-08|CENIC-2152, US
20912|IT|ripencc|2001-07-05|ASN-PANSERVICE, IT
20130|US|arin|2001-03-28|DEPAUL, US
18106|SG|apnic|2002-01-25|VIEWQWEST-SG-AP Viewqwest Pte Ltd, SG
1403|CA|arin|2009-07-28|EBOX, CA
1299|SE|ripencc|1993-09-01|TWELVE99 Arelion, fka Telia Carrier, SE
1239|US|arin|1991-03-25|SPRINTLINK, US
23673|KH|apnic|2003-03-18|ONLINE-AS Cogetel Online, Cambodia, ISP, KH
3130|EE|ripencc|1997-03-17|RGNET-SEA RGnet Seattle Westin, EE
2497|JP|apnic|2002-04-05|IIJ Internet Initiative Japan Inc., JP
3303|CH|ripencc|1994-10-28|SWISSCOM Swisscom Switzerland Ltd, CH
3257|US|ripencc|1994-09-30|GTT-BACKBONE GTT, US
2914|US|arin|1998-12-07|NTT-LTD-2914, US
34224|BG|ripencc|2004-11-22|NETERRA-AS, BG
293|US|arin|1997-06-16|ESNET, US
3561|US|arin|1998-10-07|CENTURYLINK-LEGACY-SAVVIS, US
3549|US|arin|2000-03-21|LVLT-3549, US
53767|US|arin|2011-05-13|ICASTCENTER, US
49788|NO|ripencc|2009-09-10|NEXTHOP, NO
37100|MU|afrinic|2009-05-28|SEACOM-AS, MU
5413|GB|ripencc|1995-09-12|AS5413, GB
57866|NL|ripencc|2012-02-28|FUSIX-AS, NL
57463|BG|ripencc|2011-11-02|NETIX, BG
6939|US|arin|1996-06-28|HURRICANE, US
7018|US|arin|1996-07-30|ATT-INTERNET4, US
7660|JP|apnic|1997-11-13|APAN-JP Asia Pacific Advanced Network - Japan, JP
22652|CA|arin|2007-09-27|FIBRENOIRE-INTERNET, CA
3741|ZA|afrinic|1994-08-01|IS, ZA
```

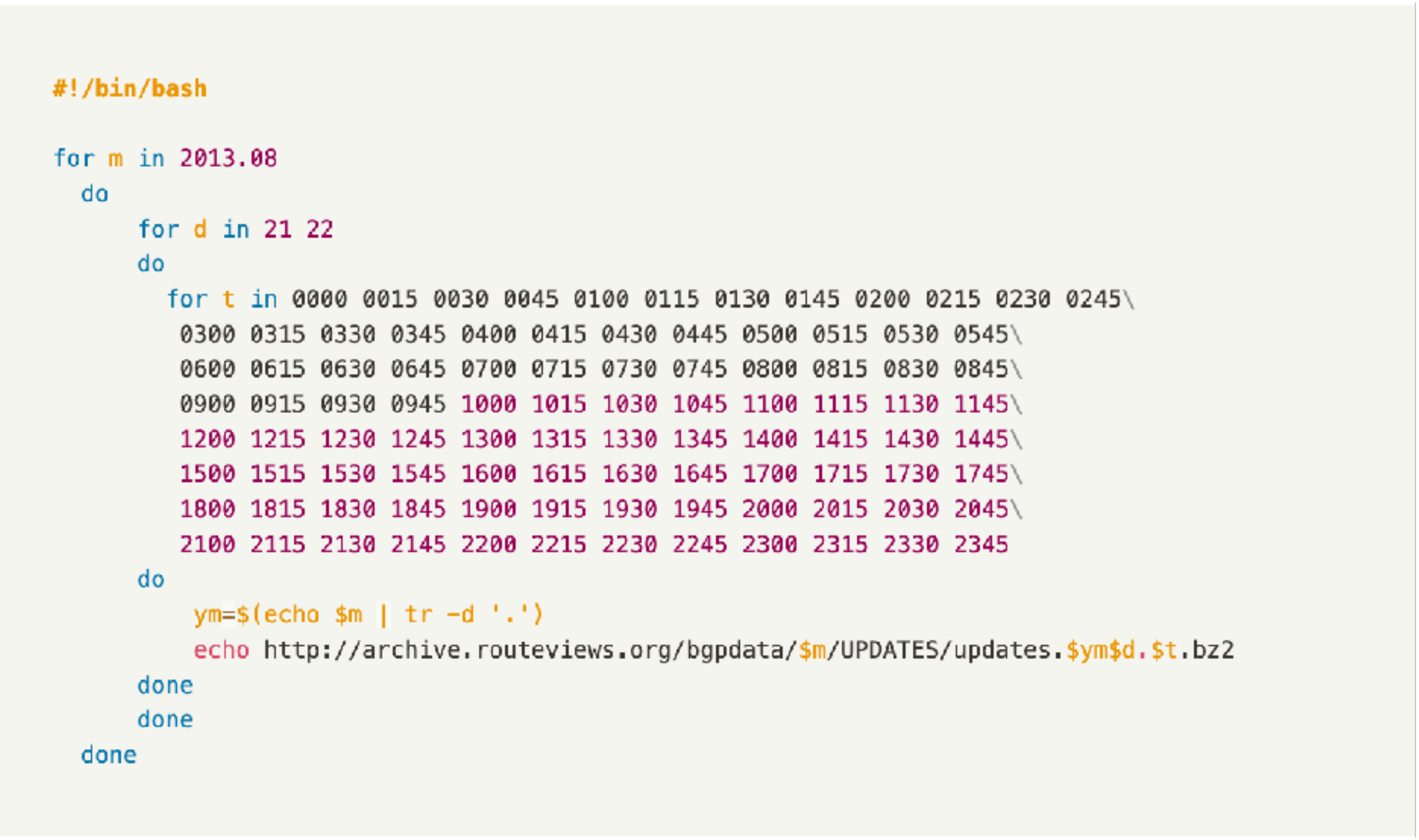
State-Sponsored BGP Hijacking



IP	PTR	City	CC	GEO Location	ASN	ASNAME
147.28.7.1	lo.r0.sea.rg.net	Seattle	US	47.6062,-122.3321	AS3130	RGnet OU
137.164.16.84	svl-agg8-loop2.cenic.net	Sunnyvale	US	37.3688,-122.0363	AS2152	CENIC
162.251.163.2	null	Phoenix	US	33.4484,-112.0740	AS53767	iCastCenter
147.28.7.2	lo.r1.sea.rg.net	Seattle	US	47.6062,-122.3321	AS3130	RGnet OU
144.228.241.130	lo0.sl-crs1-stk.swl.cogentco.com	Stockton	US	37.9577,-121.2908	AS174	Cogent Communications
140.192.8.16	rtr-350-308c-int.netequip.depaul.edu	Chicago	US	41.8500,-87.6500	AS20130	Depaul University
129.250.1.71	route-views2.a00.newthk04.hk.bb.gin.ntt.net	Hong Kong	HK	22.2783,114.1747	AS2914	NTT America, Inc.
12.0.1.63	route-spews.cbbtier3.att.net	Middletown	US	40.3943,-74.1171	AS7018	AT&T Services, Inc.
105.16.0.247	lo-0.er-01-mba.ke.seacomnet.com	Mombasa	KE	-4.0547,39.6636	AS37100	SEACOM Limited
163.253.3.14	lo-1.core1.chic.net.internet2.edu	Atlanta	US	33.7490,-84.3880	AS11537	Internet2
198.129.33.85	esnet-routeviews1.es.net	San Jose	US	37.3394,-121.8950	AS292	ESnet
203.189.128.233	r-04-pnh-noc1.online.com.kh	Cheung Aek	KH	11.4822,104.9018	AS23673	Cogetel Online, Cambodia, ISP
194.153.0.253	null	London	GB	51.5085,-0.1257	AS5413	Daisy Corporate Services Trading Ltd
202.73.40.45	parkway.vqbn.com	Singapore	SG	1.2897,103.8501	AS18106	Viewqwest Pte Ltd
168.209.255.56	core1b-dock-lo0.ip.ddii.network	London	GB	51.5085,-0.1257	AS3741	Dimension Data
198.58.198.252	lo0.rs1.1225stco.yhu.ebox.ca	Longueuil	CA	45.5152,-73.4682	AS1403	EBOX
203.181.248.195	tyo-mx10k.jp.apan.net	Tokyo	JP	35.6895,139.6917	AS7660	Asia Pacific Advanced Network - Japan
208.51.134.246	routeviews4.loop.gblx.net	London	GB	51.5085,-0.1257	AS3549	Level 3 Parent, LLC
206.24.210.80	esr1-loopback.sfo.savvis.net	San Francisco	US	37.7749,-122.4194	AS3561	CenturyLink Communications, LLC
202.232.0.3	route-server07.iij.net	Osaka	JP	34.6938,135.5011	AS2497	Internet Initiative Japan Inc.
217.192.89.50	i79zhh-006-loo1.bb.ip-plus.net	Zürich	CH	47.3667,8.5500	AS3303	Swisscom (Schweiz) AG
208.51.134.255	as6447.ar8.lax1.gblx.net	El Segundo	US	33.9192,-118.4165	AS3549	Level 3 Parent, LLC
37.139.139.17	br0.eqxam6.nl.fusixnetworks.net	Amsterdam	NL	52.3740,4.8897	AS57866	Fusix Networks B.V.
64.71.137.241	loopback9.core4.sjc2.he.net	San Jose	US	37.3394,-121.8950	AS6939	Hurricane Electric LLC
62.115.128.137	nyk-b1.ip.twelve99.net	New York City	US	40.7143,-74.0060	AS1299	Arelion Sweden AB
45.61.0.85	lo0.mpr02.mtlsunl.fibrenoire.ca	Saint-Jean-sur-Richelieu	CA	45.3071,-73.2626	AS22652	Videotron Ltee
77.39.192.30	lo2.rrc1.ltn01.core.ipv4.panservice.it	Aprilia	IT	41.5945,12.6542	AS20912	Giuliano Claudio Peritore trading as \Panservice s.a.s. di Cuseo Fabrizio & C.\
87.121.64.4	null	Sofia	BG	42.6975,23.3241	AS34224	Neterra Ltd.
89.149.178.10	routeviews-lo0.fra40.ip4.gtt.net	Mörfelden-Walldorf	DE	49.9947,8.5836	AS3257	GTT Communications Inc.
91.218.184.60	null	Oslo	NO	59.9127,10.7461	AS49788	Nexthop AS
94.156.252.18	94.156.252.18.neterra.net	Sofia	BG	42.6975,23.3241	AS34224	Neterra Ltd.

State-Sponsored BGP Hijacking

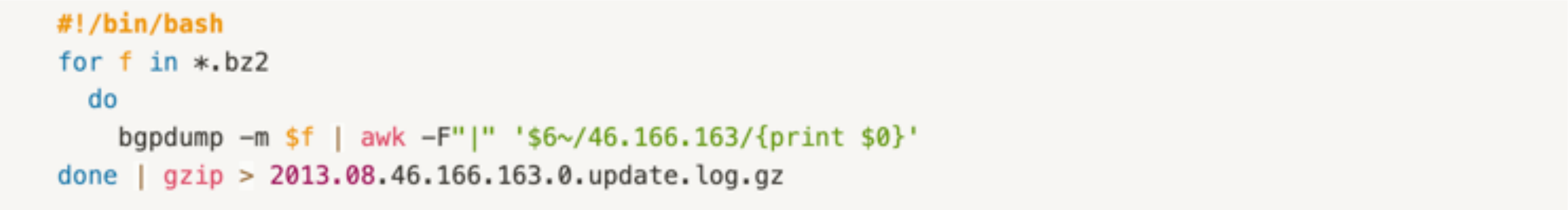
Retrieving BGP data



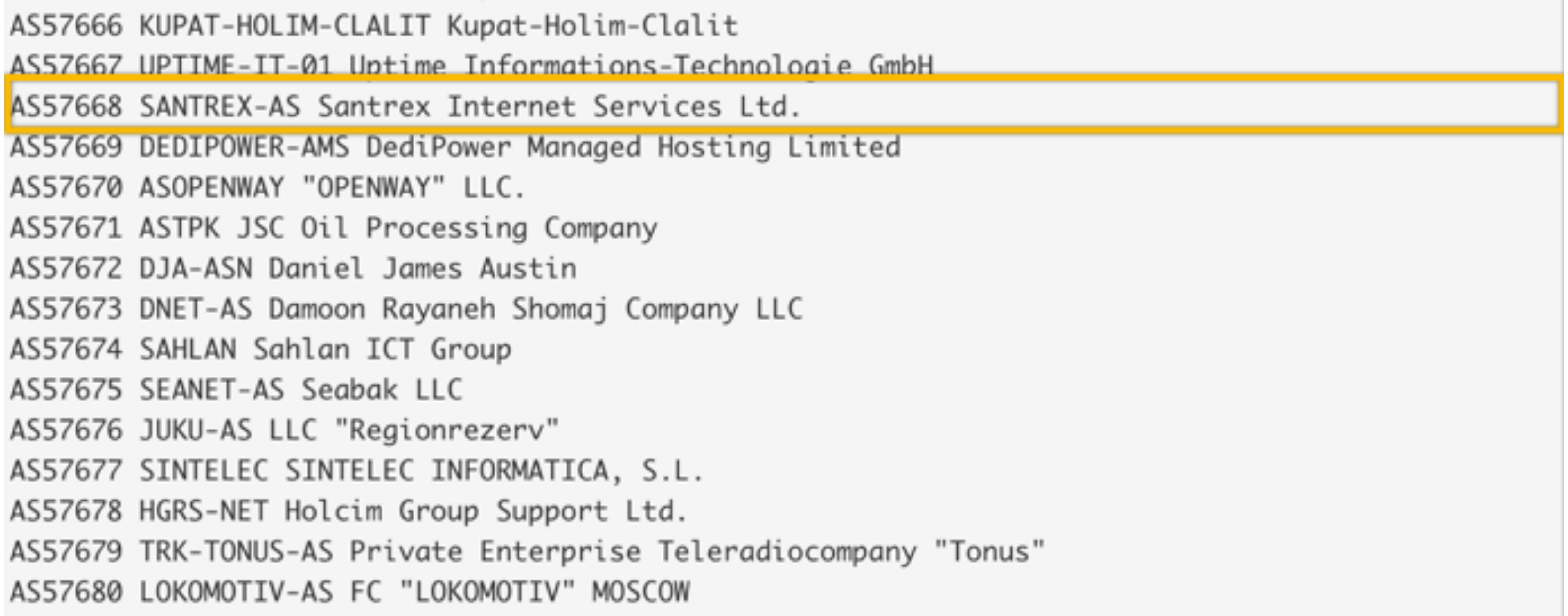
```
#!/bin/bash

for m in 2013.08
  do
      for d in 21 22
      do
        for t in 0000 0015 0030 0045 0100 0115 0130 0145 0200 0215 0230 0245\
         0300 0315 0330 0345 0400 0415 0430 0445 0500 0515 0530 0545\
         0600 0615 0630 0645 0700 0715 0730 0745 0800 0815 0830 0845\
         0900 0915 0930 0945 1000 1015 1030 1045 1100 1115 1130 1145\
         1200 1215 1230 1245 1300 1315 1330 1345 1400 1415 1430 1445\
         1500 1515 1530 1545 1600 1615 1630 1645 1700 1715 1730 1745\
         1800 1815 1830 1845 1900 1915 1930 1945 2000 2015 2030 2045\
         2100 2115 2130 2145 2200 2215 2230 2245 2300 2315 2330 2345
      do
          ym=$(echo $m | tr -d '.')
          echo http://archive.routeviews.org/bgpdata/$m/UPDATES/updates.$ym$d.$t.bz2
      done
      done
  done
```

State-Sponsored BGP Hijacking

Filter BGP announcing with 46.166.163.0/24



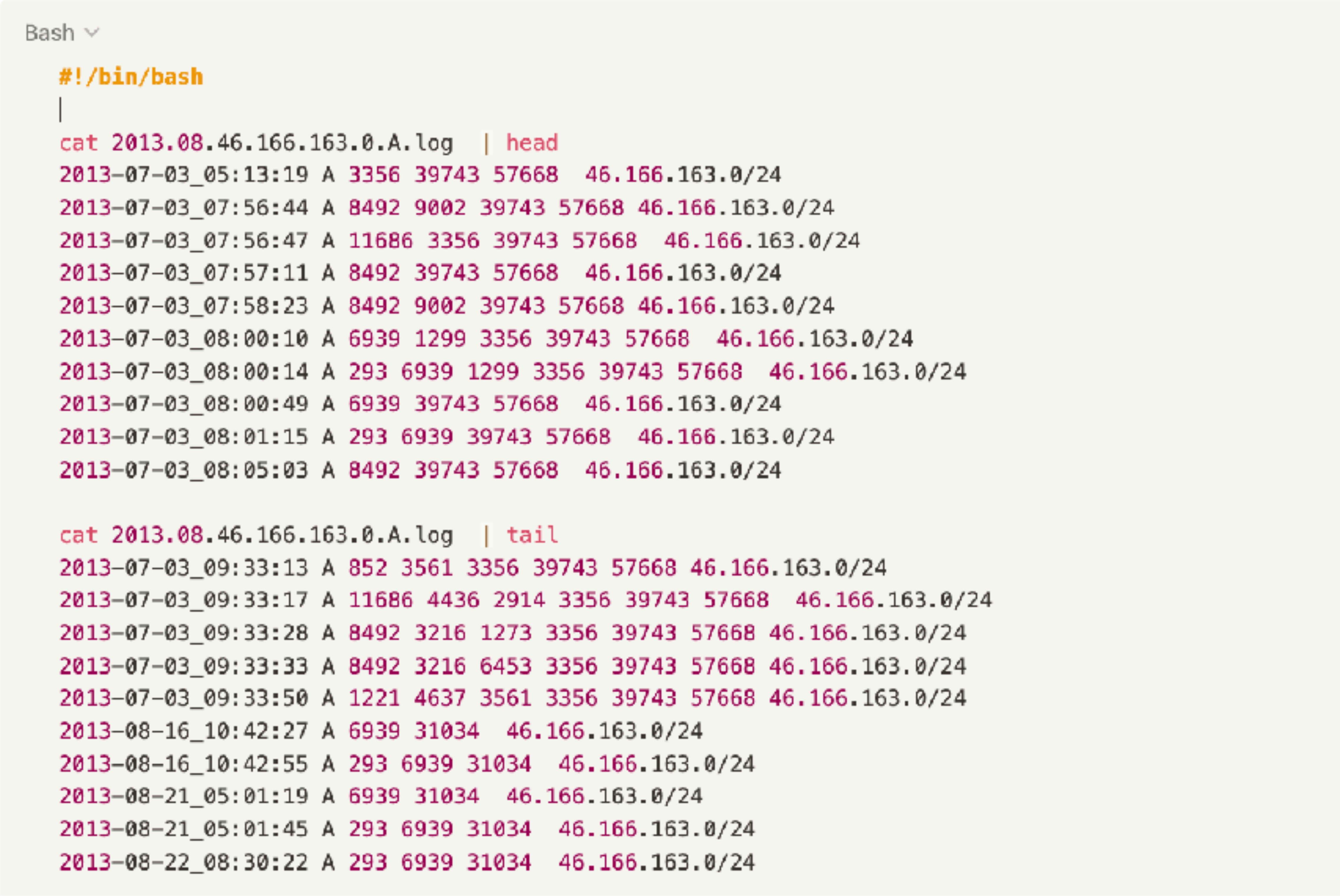
```
#!/bin/bash
for f in *.bz2
  do
    bgpdump -m $f | awk -F"|" '$6~/46.166.163/{print $0}'
done | gzip > 2013.08.46.166.163.0.update.log.gz
```



```
AS57666 KUPAT-HOLIM-CLALIT Kupat-Holim-Clalit
AS57667 UPTIME-IT-01 Uptime Informations-Technologie GmbH
AS57668 SANTREX-AS Santrex Internet Services Ltd.
AS57669 DEDIPOWER-AMS DediPower Managed Hosting Limited
AS57670 ASOPENWAY "OPENWAY" LLC.
AS57671 ASTPK JSC Oil Processing Company
AS57672 DJA-ASN Daniel James Austin
AS57673 DNET-AS Damoon Rayaneh Shomaj Company LLC
AS57674 SAHLAN Sahlan ICT Group
AS57675 SEANET-AS Seabak LLC
AS57676 JUKU-AS LLC "Regionrezerv"
AS57677 SINTELEC SINTELEC INFORMATICA, S.L.
AS57678 HGRS-NET Holcim Group Support Ltd.
AS57679 TRK-TONUS-AS Private Enterprise Teleradiocompany "Tonus"
AS57680 LOKOMOTIV-AS FC "LOKOMOTIV" MOSCOW
```

State-Sponsored BGP Hijacking

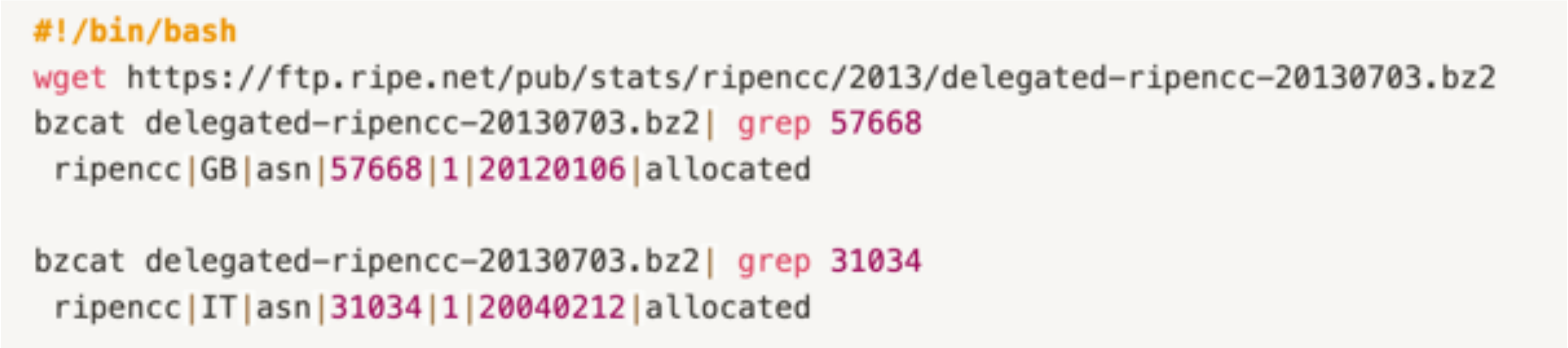
Identify BGP Hijacking Attempt



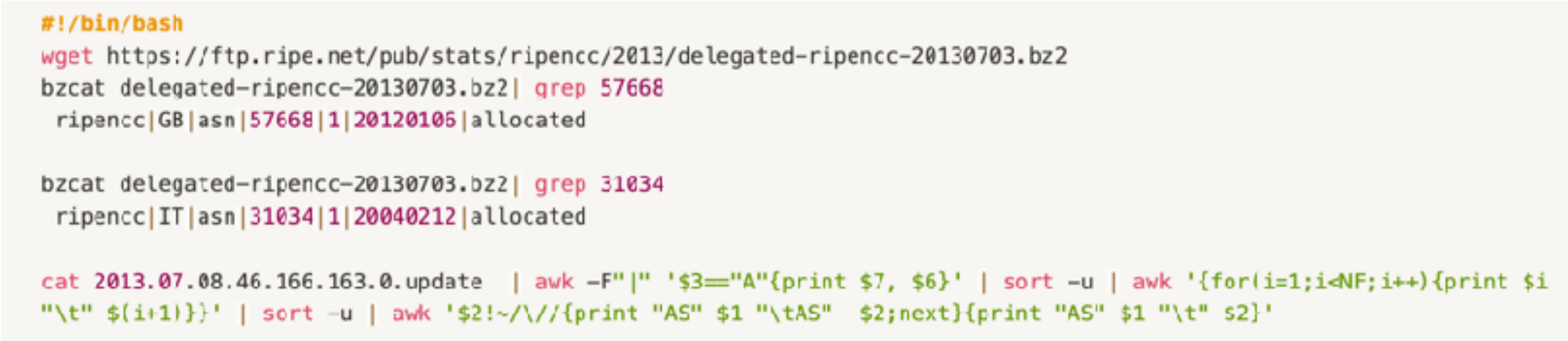
```bash
#!/bin/bash
|
cat 2013.08.46.166.163.0.A.log  | head
2013-07-03_05:13:19 A 3356 39743 57668  46.166.163.0/24
2013-07-03_07:56:44 A 8492 9002 39743 57668 46.166.163.0/24
2013-07-03_07:56:47 A 11686 3356 39743 57668  46.166.163.0/24
2013-07-03_07:57:11 A 8492 39743 57668  46.166.163.0/24
2013-07-03_07:58:23 A 8492 9002 39743 57668 46.166.163.0/24
2013-07-03_08:00:10 A 6939 1299 3356 39743 57668  46.166.163.0/24
2013-07-03_08:00:14 A 293 6939 1299 3356 39743 57668  46.166.163.0/24
2013-07-03_08:00:49 A 6939 39743 57668  46.166.163.0/24
2013-07-03_08:01:15 A 293 6939 39743 57668  46.166.163.0/24
2013-07-03_08:05:03 A 8492 39743 57668  46.166.163.0/24

cat 2013.08.46.166.163.0.A.log  | tail
2013-07-03_09:33:13 A 852 3561 3356 39743 57668 46.166.163.0/24
2013-07-03_09:33:17 A 11686 4436 2914 3356 39743 57668  46.166.163.0/24
2013-07-03_09:33:28 A 8492 3216 1273 3356 39743 57668 46.166.163.0/24
2013-07-03_09:33:33 A 8492 3216 6453 3356 39743 57668 46.166.163.0/24
2013-07-03_09:33:50 A 1221 4637 3561 3356 39743 57668 46.166.163.0/24
2013-08-16_10:42:27 A 6939 31034  46.166.163.0/24
2013-08-16_10:42:55 A 293 6939 31034  46.166.163.0/24
2013-08-21_05:01:19 A 6939 31034  46.166.163.0/24
2013-08-21_05:01:45 A 293 6939 31034  46.166.163.0/24
2013-08-22_08:30:22 A 293 6939 31034  46.166.163.0/24
```

State-Sponsored BGP Hijacking

Identify the Prefix Owner

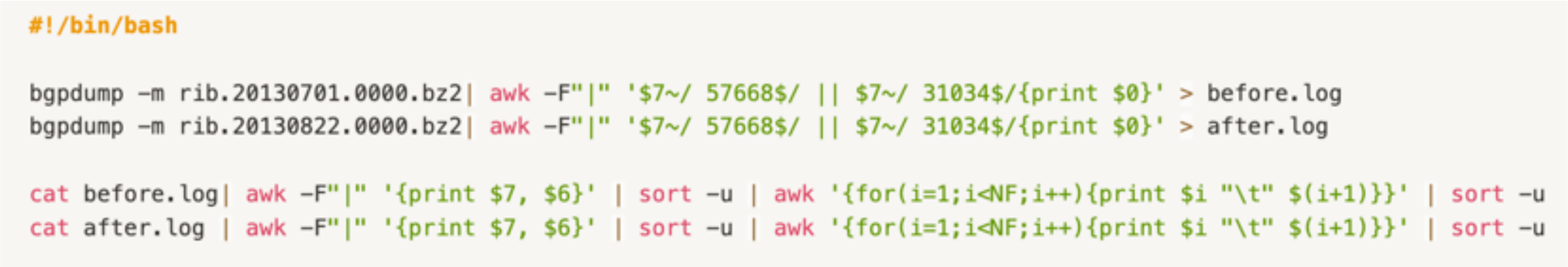


```
#!/bin/bash
wget https://ftp.ripe.net/pub/stats/ripencc/2013/delegated-ripencc-20130703.bz2
bzcat delegated-ripencc-20130703.bz2| grep 57668
 ripencc|GB|asn|57668|1|20120106|allocated

bzcat delegated-ripencc-20130703.bz2| grep 31034
 ripencc|IT|asn|31034|1|20040212|allocated
```



```
#!/bin/bash
wget https://ftp.ripe.net/pub/stats/ripencc/2013/delegated-ripencc-20130703.bz2
bzcat delegated-ripencc-20130703.bz2| grep 57668
 ripencc|GB|asn|57668|1|20120106|allocated

bzcat delegated-ripencc-20130703.bz2| grep 31034
 ripencc|IT|asn|31034|1|20040212|allocated
```

```
cat 2013.07.08.46.166.163.0.update  | awk -F"|" '$3=="A"{print $7, $6}' | sort -u | awk '{for(i=1;i<NF;i++){print $i
"\t" $(i+1)}}' | sort -u | awk '$2!~/\//{print "AS" $1 "\tAS"  $2;next}{print "AS" $1 "\t" $2}'
```

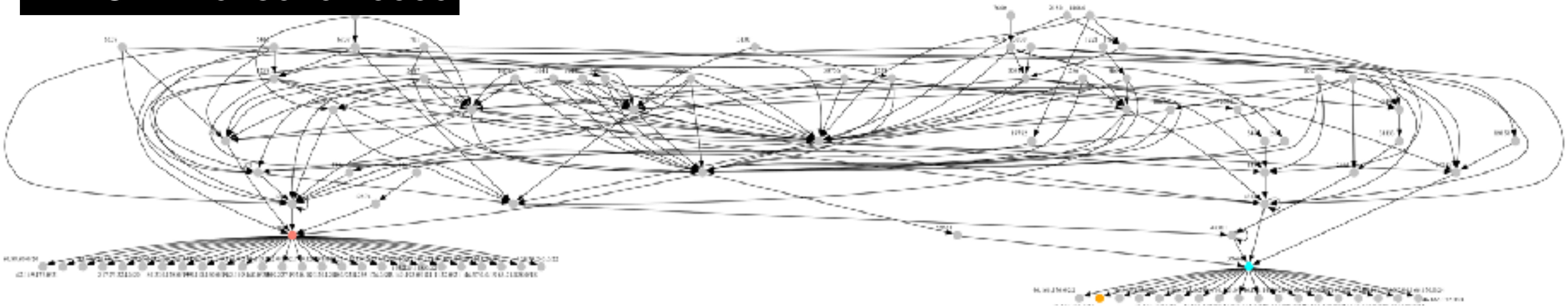


```
#!/bin/bash

bgpdump -m rib.20130701.0000.bz2| awk -F"|" '$7~/ 57668$/ || $7~/ 31034$/{print $0}' > before.log
bgpdump -m rib.20130822.0000.bz2| awk -F"|" '$7~/ 57668$/ || $7~/ 31034$/{print $0}' > after.log

cat before.log| awk -F"|" '{print $7, $6}' | sort -u | awk '{for(i=1;i<NF;i++){print $i "\t" $(i+1)}}' | sort -u
cat after.log | awk -F"|" '{print $7, $6}' | sort -u | awk '{for(i=1;i<NF;i++){print $i "\t" $(i+1)}}' | sort -u
```

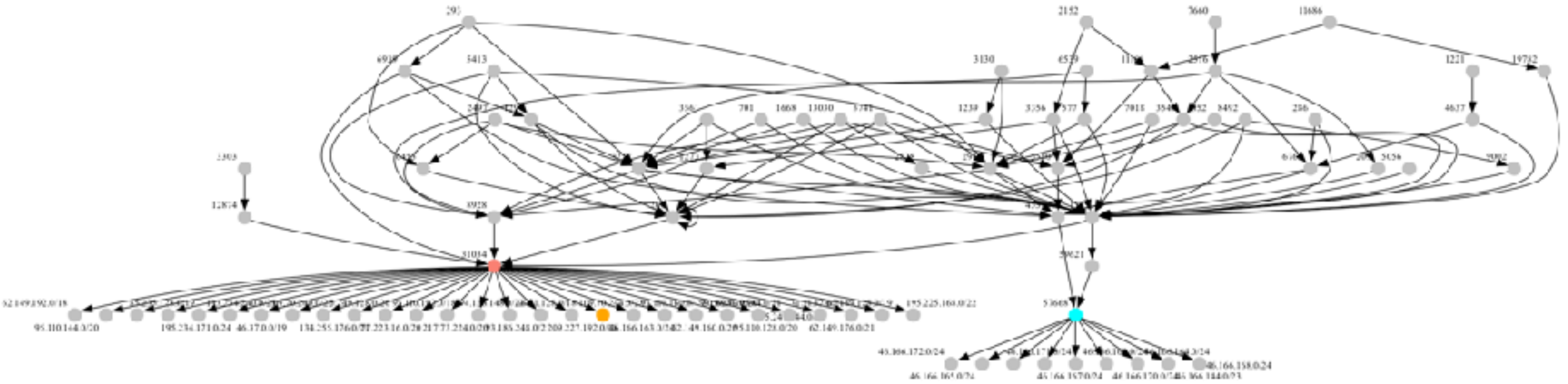
State-Sponsored BGP Hijacking

Visualization

BEFORE:20130701.0000



AFTER:20130822.0000


291
6939
3413
2152
5660
11686
3130
6539
1221
19712
2497
3356
701
1668
13030
3741
1239
3356
577
7018
3452
286
4637
3257
2914
3928
31034
58821
53608
52.149.192.0/18
95.110.164.0/20
195.234.171.0/24
46.170.0/19
134.255.176.0/20
62.149.176.0/21
195.225.160.0/22
46.166.172.0/24
46.166.158.0/24
46.166.165.0/24
46.166.157.0/24
46.166.184.0/23