NEW ADVENTURES:

DENOG10

RPKI

MARTIN HOFFMANN

NLNETLABS

ars TECHNICA SUBSCRIPTIONS SIGN IN

BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 9:00 PM

amazon.co

Amazon

Amazon lost control of a small number of its cloud services IP addresses for two
morning when hackers exploited a known Internet-protocol weakness that let th

BGP Hijacking Attacks Target US Payment Processors

rd Kovacs on August 07, 2018

re G+ Tweet Recommend 17 RSS

l payment processing companies in the United States were targeted recer
iacking attacks whose goal was to redirect users to malicious websites, Or
ed last week.

rder Gateway Protocol (BGP) controls the route of data across the Web. BGP
own as prefix or route hijacking, is carried out by taking over IP address grou
ing the routing tables that store the path to a network.

past months, Oracle, which gained deep visibility into Web traffic after acqui
, has observed several instances of malicious actors trying to force users to
es by targeting authoritative DNS servers in BGP hijacking attacks.

BGPMON Now part of OpenDNS

HOME BLOG ABOUT US PRODUCTS AND SERVICES CLIENT PORTAL

Turkey Hijacking IP addresses for popular Global DNS providers

Posted by Andree Toonk – March 29, 2014 – Hijack, News and Updates – 26 Comments

At BGPmon we see numerous BGP hijacks every single day, some are interesting because of the size and scale of the hijack or as we've seen today because of the targeted hijacked prefixes. It all started last weekend when the Turkish president ordered the censorship of twitter.com. This
lock of twitter by returning false twitter IP addresses by Turk Telekom DNS
sers in Turkey discovered that changing DNS providers to Google DNS or
good method of bypassing the censorship. But as of around 9am UTC today
29) this changed when Turk Telekom started to hijack the IP address for
open DNS providers such as Google's 8.8.8.8, OpenDNS' 208.67.222.222 and

Blog

VANTAGEPOINT
IN: RESEARCH

Shutting down the BGP Hijack Factory

Jul 10, 2018 // Doug Madory

ed with a lengthy email to the NANOG mailing list on 25 June
ndependent security researcher Ronald Guilmette detailed the
ious routing activities of a company called Bitcanal, whom he
d to as a "Hijack Factory." In his post, Ronald detailed some of
rtuguese company's most recent BGP hijacks and asked the
on: why Bitcanal's transit providers continue to carry its BGP
d routes on to the global internet?

mail kicked off a discussion that led to a concerted effort to kick
d actor, who has hijacked with impunity for many years, off the
et.

December 18, 2017 By Pierluigi Paganini

Traffic for Google, Apple, Facebook, Microsoft and other tech giants routed through Russia, experts believe it was an intentional BGP Hijacking.

Last week a suspicious event routed traffic for major tech companies (i.e. Google, Facebook, Apple, and Microsoft) through a previously unknown Russian Internet provider. The event occurred on Wednesday, researchers who investigated it believe the traffic was intentionally hijacked.

The incident involved the Internet's Border Gateway Protocol that is used to route traffic among Internet backbones, ISPs, and other large networks.

BGP BGPmon.net

c|net

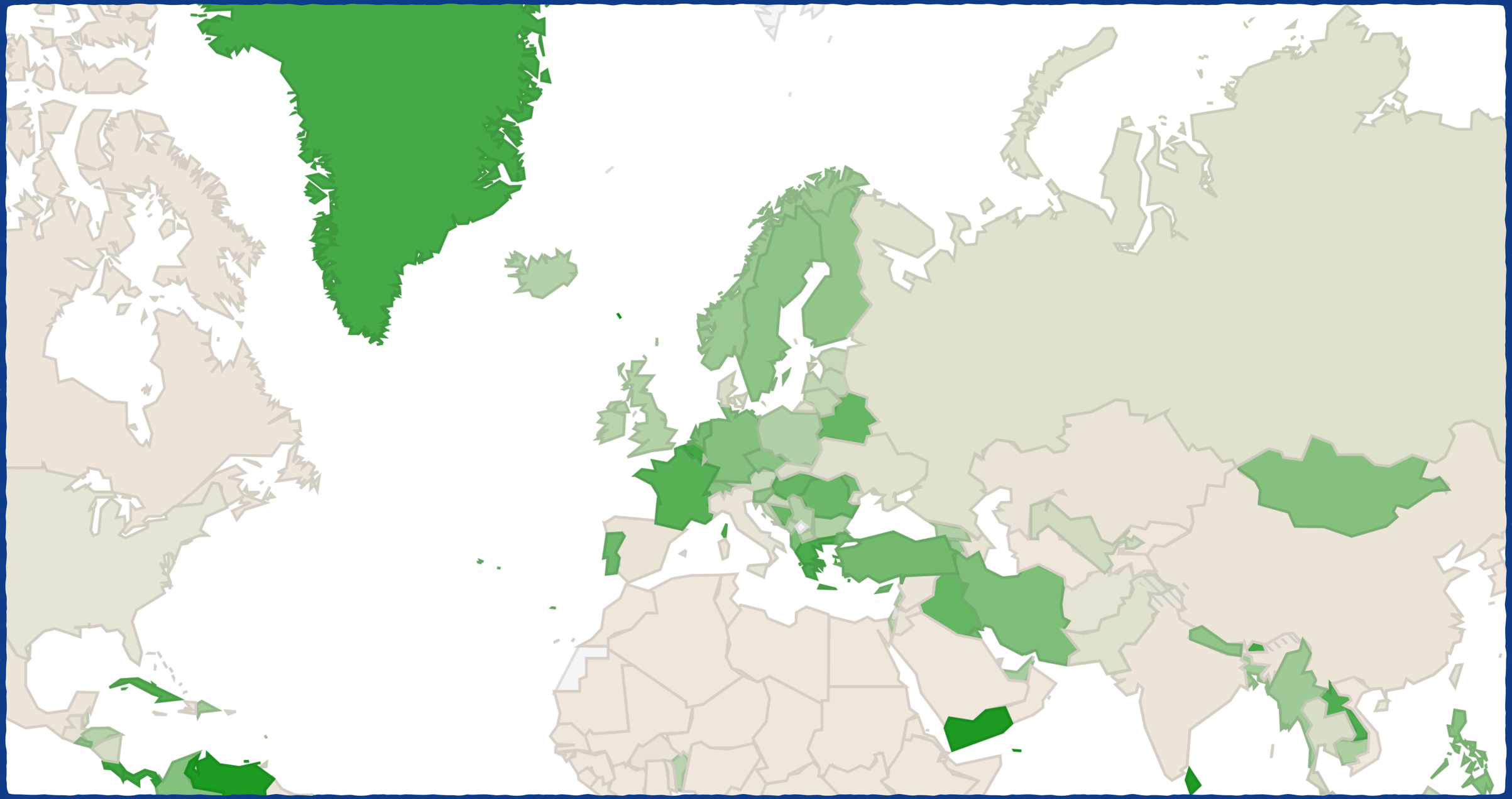
3

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

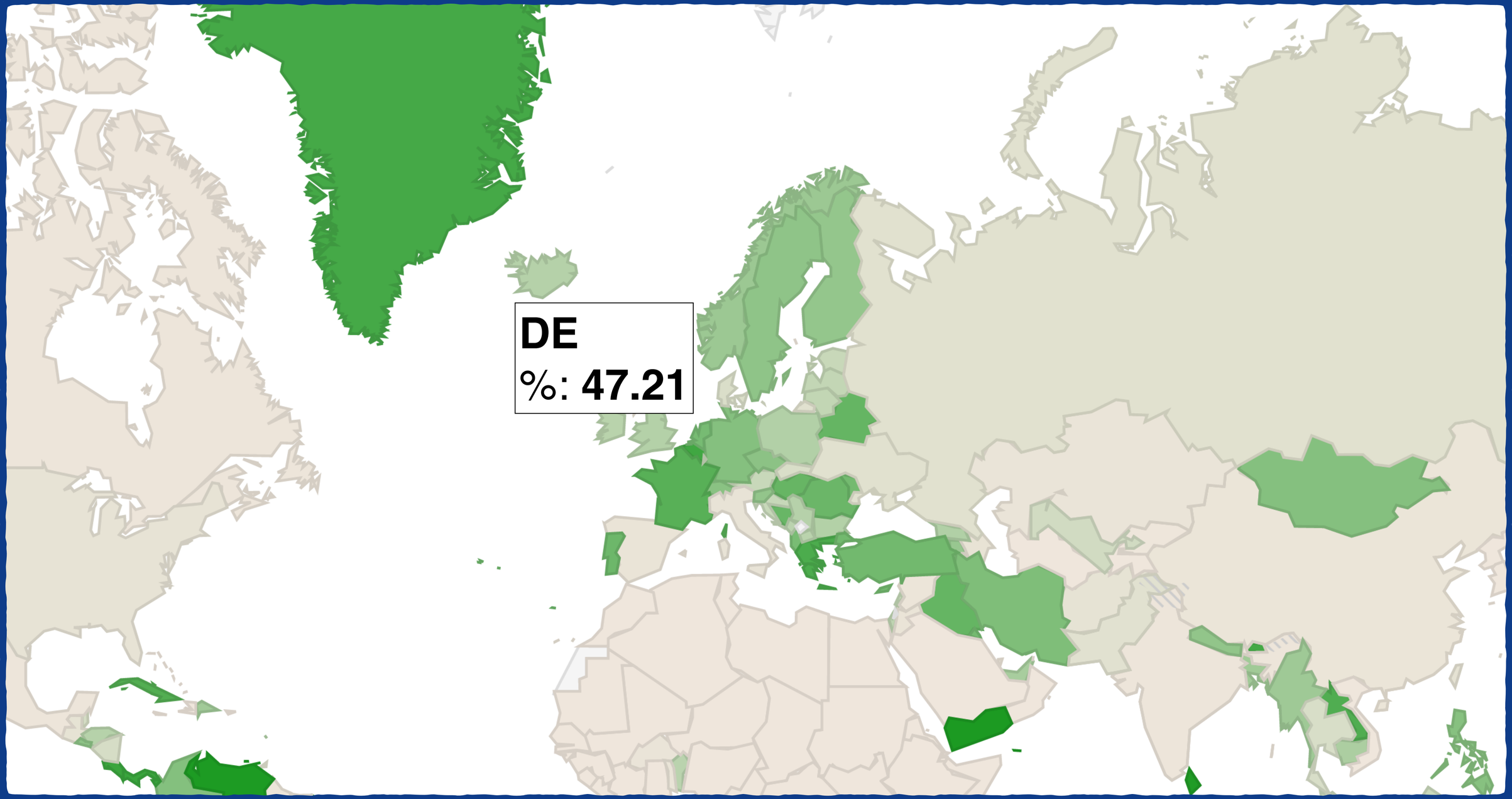
YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.

by **Declan McCullagh**

Updated: February 25, 2008 4:28 PM PST



https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html



https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) | Website

Search IP Address and ASN

Manage IPs and ASNs | Analyse | Participate | Get Support | Publications | About Us

You are here: Home > Manage IPs and ASNs > LIR Portal

You are editing: Stichting NLnet Labs

- My LIR
- Resources
  - My Resources
  - Request Resources
  - Request Transfer
  - IPv4 Transfer Listing Service
  - RPKI Dashboard
- RIPE Database

RPKI Dashboard

2 CERTIFIED RESOURCES | ALERTS ARE SENT TO 1 ADDRESS

2 BGP Announcements

2 Valid | 0 Invalid | 0 Unknown

2 ROAs

2 OK | 0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

Search...

Discard Changes | Delete ROAs | Causing Problems | Not Causing Problems | + New ROA

AS number	Prefix	Most specific length allowed	Affects
AS Number	Prefix	Max length	
AS199664	2a04:b900::/29	29	1
AS199664	185.49.140.0/22	22	1

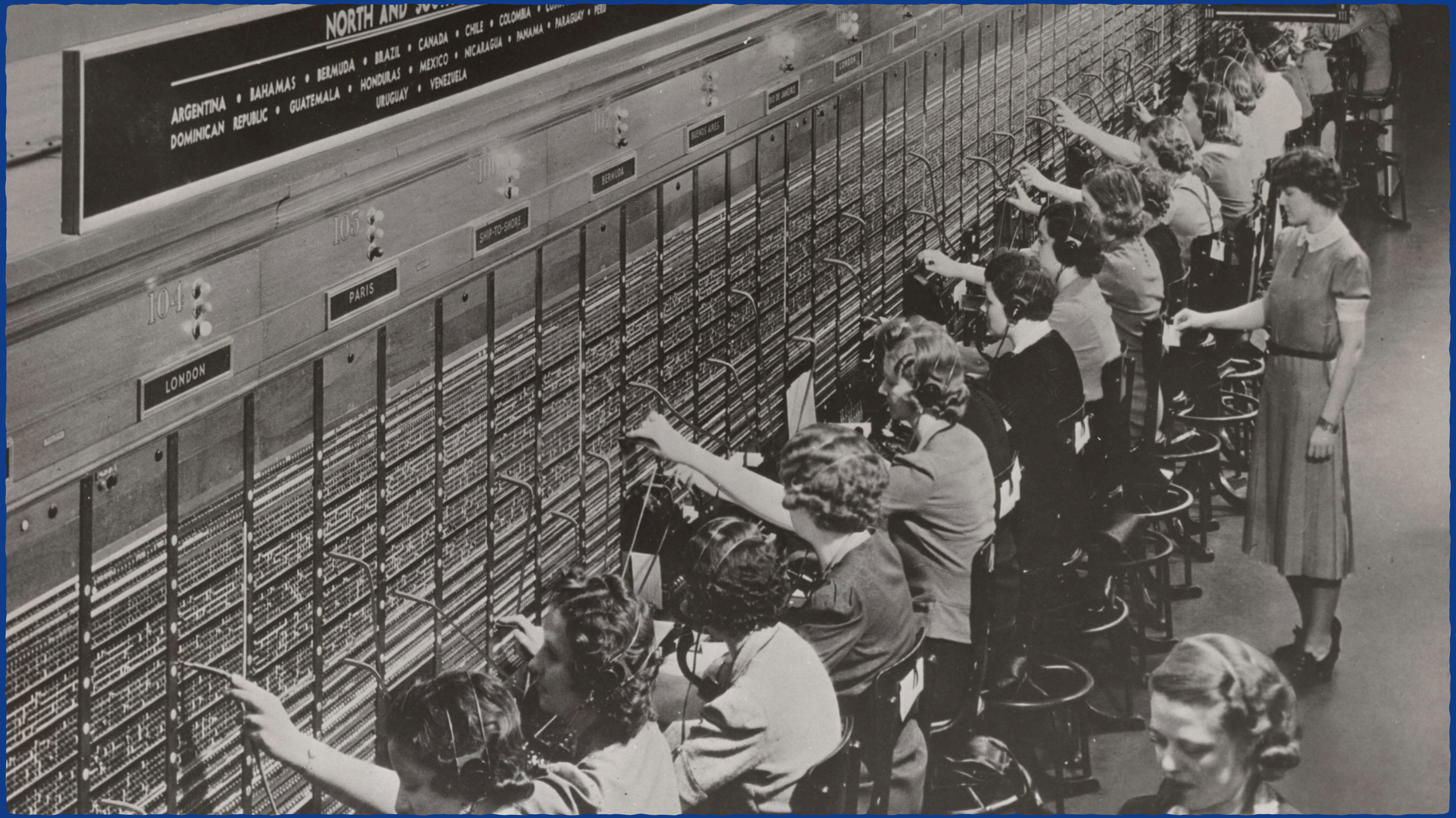
Show 25 of 2 items

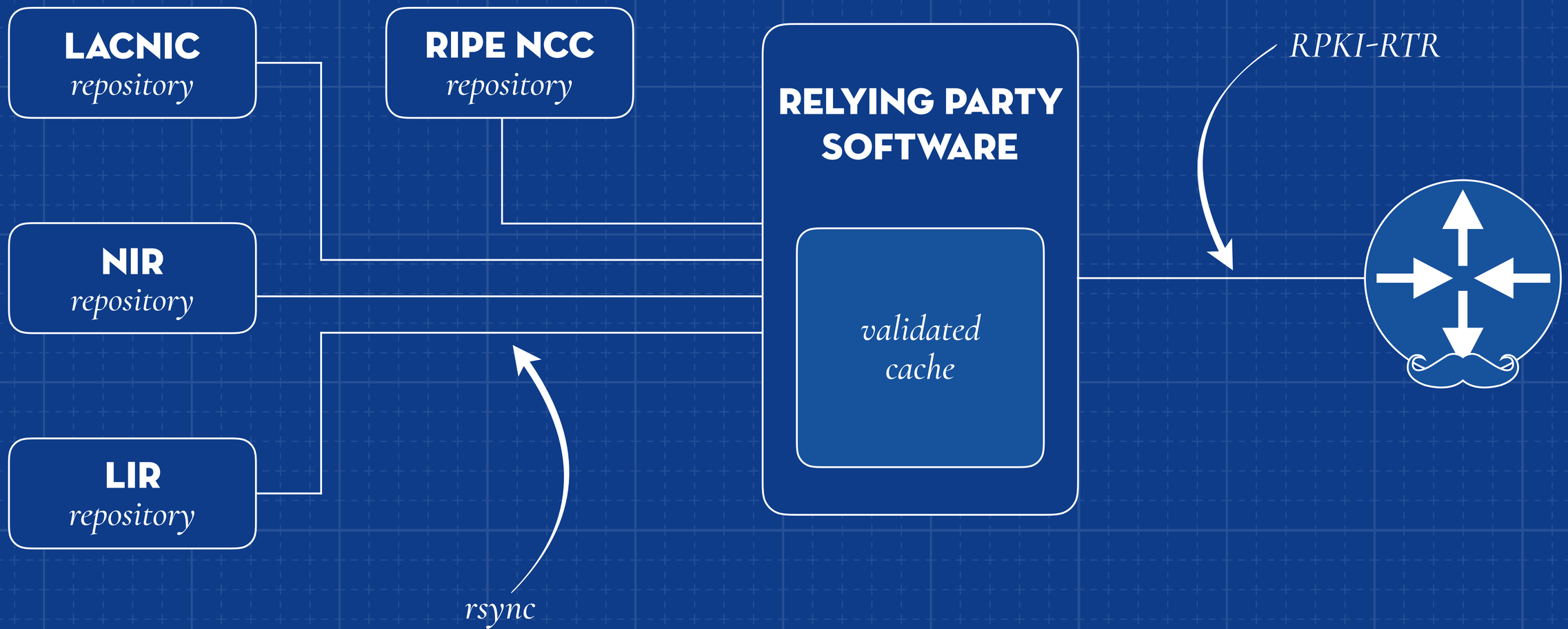
CERTIFICATE AUTHORITY

PUBLICATION SERVER

Photo by Shane McLendon on Unsplash

https://nlnetlabs.nl/projects/rpki/project-plan/


NORTH AND
ARGENTINA • BAHAMAS • BERMUDA • BRAZIL • CANADA • CHILE • COLOMBIA •
DOMINICAN REPUBLIC • GUATEMALA • HONDURAS • MEXICO • NICARAGUA • PANAMA • PARAGUAY •
URUGUAY • VENEZUELA
LONDON
PARIS
SHIP-TO-SHORE
BERMUDA
BUENOS AIRES
RIO DE JANEIRO
LONDON
104
105


LACNIC
repository
RIPE NCC
repository
NIR
repository
LIR
repository
RELYING PARTY
SOFTWARE
validated
cache
RPKI-RTR
rsync


ROUTINATOR

```
$ apt-get install rsync build-essential
$ curl https://sh.rustup.rs -sSf | sh
$ source ~/.cargo/env
$ cargo install routinator
$ _
```

```
$ apt-get install rsync build-essential
$ curl https://sh.rustup.rs -sSf | sh
$ source ~/.cargo/env
$ cargo install routinator
$ routinator_
```

```
$ cargo install routinator
$ routinator
MISSING TRUST ANCHOR LOCATOR

The trust anchor locator (TAL) in file

   /home/m/.rpki-cache/tals/arin.tal

has not been installed. Please go to

   https://www.arin.net/resources/rpki/tal.html

and download the TAL in RFC 7730 format. Place the downloaded file at

   /home/m/.rpki-cache/tals/arin.tal

Routinator will refuse to run until you have done that.
$_
```

```
$ routinator -f csv
ASN,IP Prefix,Max Length
AS38719,27.111.92.0/22,22
AS8551,79.178.43.0/24,24
AS56630,2a03:f80:359::/48,48
AS43131,185.236.11.0/24,24
AS64520,2001:13f8:9000::/44,44
^C
```

```
$ routinator -f json
{
  "roas": [
    { "asn": "AS196921", "prefix": "94.187.192.0/19", "maxLength": 21 },
    { "asn": "AS43754", "prefix": "37.156.232.0/21", "maxLength": 21 },
    { "asn": "AS64093", "prefix": "103.252.83.0/24", "maxLength": 24 },
^C
```

```
$ routinator -f rpsl

route: 195.176.0.0/17
origin: AS559
descr: RPKI attestation
mnt-by: NA
created: 2018-11-20T14:31:36.791062+00:00
last-modified: 2018-11-20T14:31:36.791062+00:00
source: NA

^C
```

```
$ routinator -r -l [2001:0DB8::13]:3323 -v
Starting RTR listener…
```

```
$ find ~/.rpki-cache/repository -type f | wc -l
42636
$ du -sh ~/.rpki-cache/repository
241M
$ _
```

```
$ find ~/.rpki-cache/repository -type f | wc -l
42636
$ du -sh ~/.rpki-cache/repository
241M
$ routinator -r &
[1] 12182
$ pmap 12182 | grep total
 total            62168K
$ _
```

```
$ find ~/.rpki-cache/repository -type f | wc -l
42636
$ du -sh ~/.rpki-cache/repository
241M
$ routinator -r &
[1] 12182
$ pmap 12182 | grep total
 total            62168K
$ time routinator -n

real    0m5.881s
user    0m7.224s
sys     0m0.276s
$ _
```


pi@raspberrypi:~ $ time ./routinator -nf none
real 4m58.126s
user 4m43.880s
sys 0m6.080s
pi@raspberrypi:~ $

RPKI

MAILING LIST

https://nlnetlabs.nl/mailman/listinfo/rpki

FAQ

https://nlnetlabs.nl/projects/rpki/faq/

https://github.com/nlnetlabs/rpki-faq

https://github.com/nlnetlabs/routinator

@ rpki-team@nlnetlabs.nl

@routinator3000

NLNETLABS