CERT RCTS

BGP Hijacks

Carlos Friaças

November 2019

RCTS CERT

- Computer Incident Response Team for the Portuguese Research & Education Network
- Reactive and Proactive services for our constituency base
- Founding Member of the National CSIRT Network
  - www.redecsirt.pt
- Member of FIRST since 2011
  - www.first.org
- Certified by Trusted Introducer in 2015
  - Currently under Re-Certification
  - trusted-introducer.org

Rede Nacional CSIRT

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

«Hijacking»

- Technique used to avoid «attribution» or «identification»

- Using networks with records associated with other organisations
  - Whether active (higher chance of complaint) or inactive (closed).
  - Or from conflict zones…

What is the Goal?

- Diverting attribution (and law enforcement)
- Dumping toxic waste (snowshoe spamming operations)

Problematic Misconception

- The victim is only the address space owner
- But… huge potential impact on other networks that receive and accept hijacked prefixes
  - And send packets towards the hijacker
  - And allow packets from the hijacker (i.e. the route presence validates uRPF checks…)

BGP Hijacks, More or Less Accidental

c|net BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME GIFT GUIDE JOIN / SIGN IN

CULTURE

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 | FEBRUARY 25, 2008 4:28 PM PST

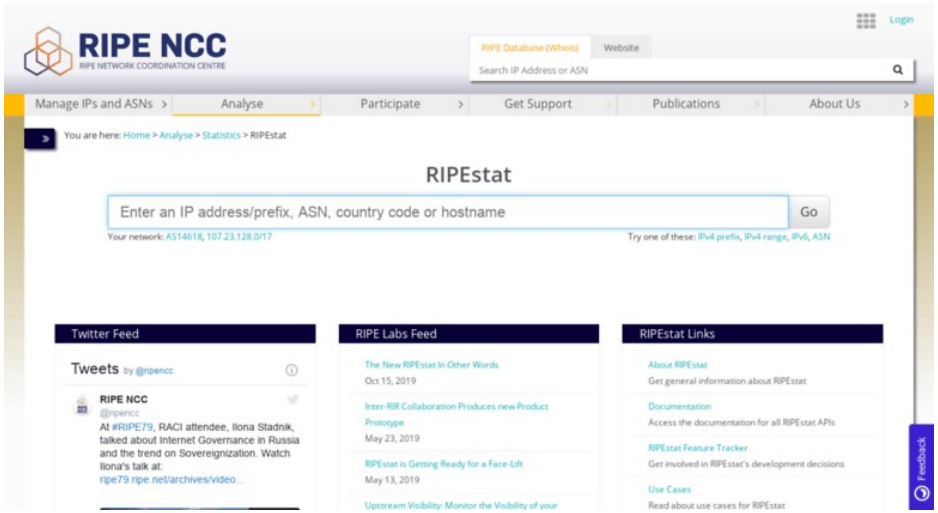
BGP Hijack – Goal: Eavesdropping?

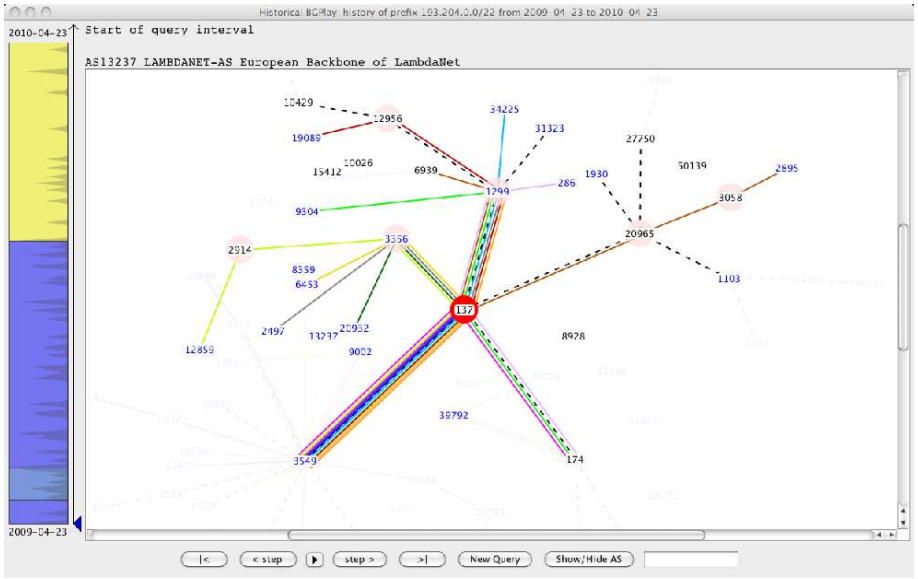
Traffic misdirection by AS4134

Tools: BGPmon

Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Outage		Yudhawira Khatulistiwa, PT (AS 45710)	2018-11-24 18:51:00	2018-11-24 18:54:00	More detail
Outage		Smithsonian Tropical Research Institute (AS 27922)	2018-11-24 18:37:00		More detail
BGP Leak		*Origin AS:* Orange Communication (The Sky Traders Ltd) (AS 134437) *Leaker AS:* Telecom Operator & Internet Service Provider as well (AS 17494)	2018-11-24 18:28:16		More detail
Outage		EDUARDO LIMA E SILVA NETTO - ME (AS 266566)	2018-11-24 18:17:00		More detail
Possible Hijack		*Expected Origin AS:* Gtech Sweden Interactive Ab (AS 48768) *Detected Origin AS:* Securitydam Ltd (AS 198949)	2018-11-24 16:38:00	2018-11-24 17:12:19	More detail
Outage		IMG BRASIL TELECOMUNICAÇÕES LTDA (AS 262447)	2018-11-24 16:37:00		More detail
Outage		ASOM-Net forening (AS 60111)	2018-11-24 14:11:00		More detail
Possible Hijack		*Expected Origin AS:* Akamai International B.V. (AS 20940) *Detected Origin AS:* Stowarzyszenie e-Poludnie (AS 50607)	2018-11-24 10:43:09	2018-11-24 10:46:28	More detail
Outage		Dnetworks Internet Services Pvt. Ltd. (AS 59161)	2018-11-24 10:41:00	2018-11-24 11:05:00	More detail

Tools: RIPEstat & BGPlay





Hijack Factory @Portugal

[redacted] hijack factory, courtesy of Cogent, GTT, and Level3

Ronald F. Guilmette rfg at tristatelogic.com
Tue Jun 26 04:49:15 UTC 2018

- Previous message (by thread): [redacted]entations RIPE 77
- Next message (by thread): [redacted] hijack factory, courtesy of Cogent, GTT, and Level3
- **Messages sorted by:** [date] [thread] [subject] [author]

Sometimes I see stuff that just makes me shake my head in disbelief.
Here is a good example:

https://bgp.he.net/[redacted]#_prefixes

I mean seriously, WTF?

As should be blatantly self-evident to pretty much everyone who has ever looked at any of the Internet's innumeriable prior incidents of very deliberately engineered IP [redacted] hijackings, all of the routes currently being announced by [redacted] Portugal) except for the ones in 213/8 are bloody o[redacted] (And to their credit, even Spamhaus has a couple of the U.S. legacy /16 blocks explicitly listed as such.)

That's [redacted]39 deliberately hijacked routes, at least going by the data visible on bgp.he.net. But even that data from bgp.he.net dramatically understates the case, I'm sorry to say. According to the more complete and up-to-the-minute data that I just now fetched from RIPEstat, the real number of hijacked routes is more on the order of 130 separate hijacked routes for a total of 224,512 IPv4 addresses:

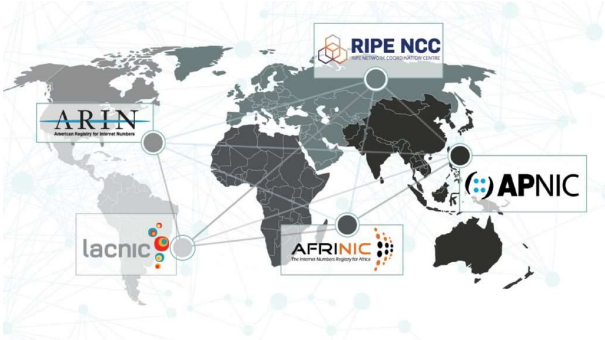
https://pastebin.com/raw/Jw1my9Bb

Dyn & Krebs on Security

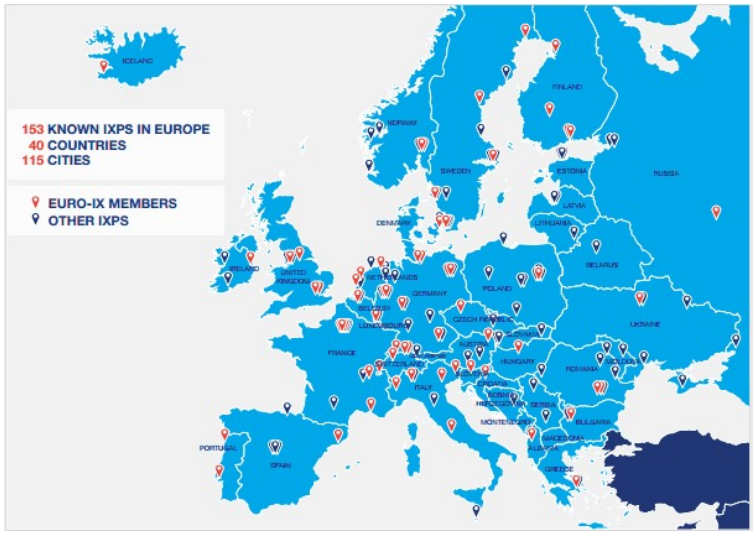
It started with a lengthy email to the NANOG mailing list on 25 June 2018: independent security researcher Ronald Guilmette detailed the suspicious routing activities of a company called [redacted], whom he referred to as a "Hijack Factory." In his post, Ronald detailed some of the Portuguese company's most recent BGP hijacks and asked the question: why [redacted]'s transit providers continue to carry its BGP hijacked routes on to the global

Hijackers: Modus Operandi

- RIPE NCC Recognized Broker
- IP address block Transfers
- Simulating Customers

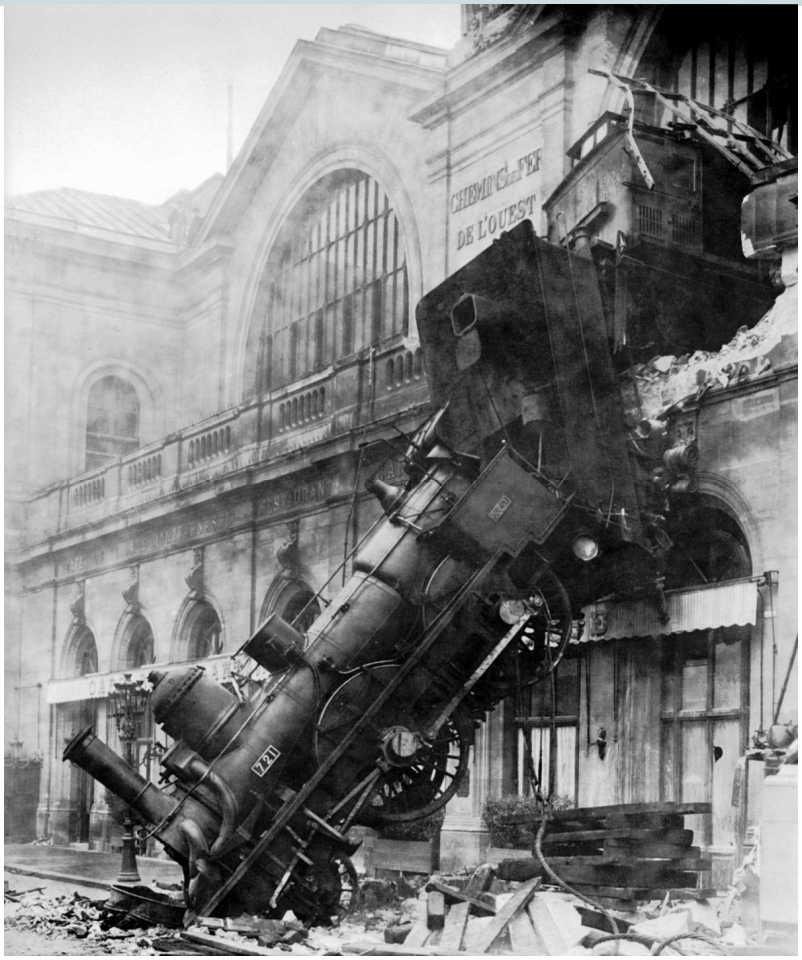


Hijackers: Modus Operandi



- Presence at Internet Exchange Points
- Several Companies and LIRs
- Uncover? Restart with new names & numbers

Trust-based Model for Global Routing?



Policy: Proposals at RIRs failed

- Withdrawn at RIPE
- Rejected at LACNIC

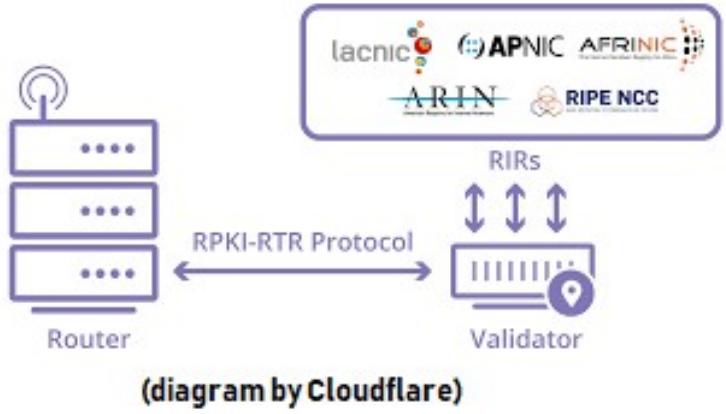
- Determined ‘Out-of-Scope’ in ARIN (Advisory Council & Board of Trustees) and APNIC (Chairs)

Policy: Proposals at RIRs failed

- Main idea was to take out hijackers from RIRs
  - after two (continuous & intentional) offences
- Hurdle #1: RIRs stay away from routing
- Hurdle #2: Risk of lawsuits towards RIRs

What to do next?

- Policy axis failed, back to Technical axis



(diagram by Cloudflare)

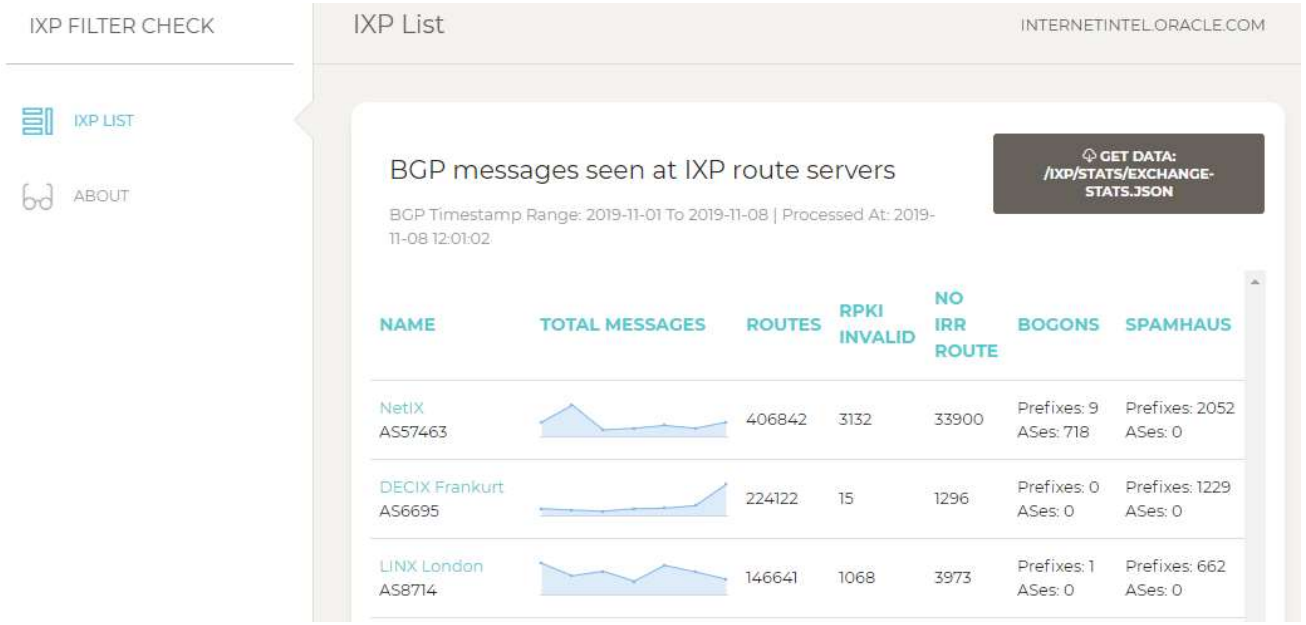
- Identify hijacks (and hijackers) when possible
  - Reach out to people who can warn other people

Excellent Research

- Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table
  - By: Cecilia Testart and Philipp Richter *(MIT)*, Alistair King *(CAIDA, UC San Diego)*, Alberto Dainotti *(CAIDA, UC San Diego)*, David Clark *(MIT CSAIL)*
  - [slides] https://conferences.sigcomm.org/imc/2019/presentations/p100.pdf
  - [video] https://vimeo.com/showcase/6531379/video/369121888#t=1624s

Excellent Tool

- IXP Filter Check
  - https://map.internetintel.oracle.com/ixp/#/ixp/list



Thanks! Obrigado!

<info@cert.rcts.pt>