Security .Days

<Prague.CZ>
<9-11 April 2024>

GÉANT

Hijacks: Why should we care?

Carlos Friaças

RCTS CERT

FCCN Unit, FCT, Portugal

Co-funded by
the European Union

Problem Statement

Hijacks happen everyday.

Their impact is mostly ignored.

If faking the origin of a phone call is bad, faking the IP source addresses from where packets are sent to others is also bad.

Background

Image from Krebsonsecurity

This talk is about Network Security.

My previous experience with BGP hijacks comes from handling the case with the notorious Bitcanal hijacker.

Bitcanal was connected to our local Internet eXchange (in Lisbon) since 2013, before their hijacks reached public eye in 2018.

Background

After 2018 we deployed local means to observe future cases of (BGP) hijacking, and we also started a due diligence process regarding joining requests at the Internet eXchange we manage.

Last year i stumbled on another (very small, very different) case.

Again, this other actor is also from my country.

What is a (BGP) Hijack?

An improper network announcement

Golden rule: You only announce your prefixes, or your customers’

If not, there is a possible hijack involved

B.G.P. – Border Gateway Protocol, Concepts

TCP, session oriented

Multiprotocol, IPv4 & IPv6

I announce my prefixes to others, I receive prefixes from others

Upstreams & Peers

Internet eXchanges, Route servers

Inbound & Outbound traffic

Country borders <> Internet borders

What is a Hijack? What is a Leak?

Intentional announcements vs. Accidents

«Who can tell if that is a Hijack or a Leak?»

We need to know which network prefixes and autonomous systems are involved!

(but we can, because announcements are recorded!)

Why does someone do this?

To divert someone else's traffic

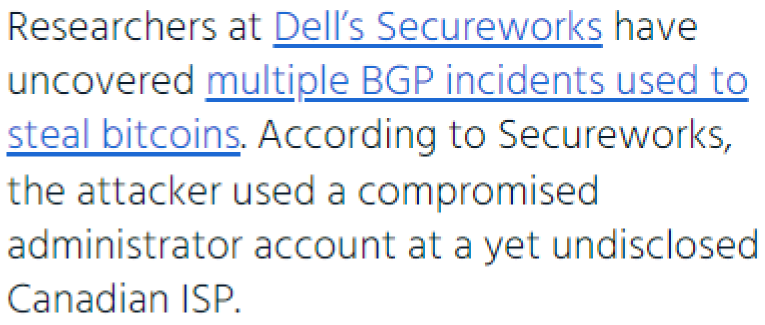
To break communication between nodes

To escape attribution & Law enforcement

To avoid paying for IPv4 resources

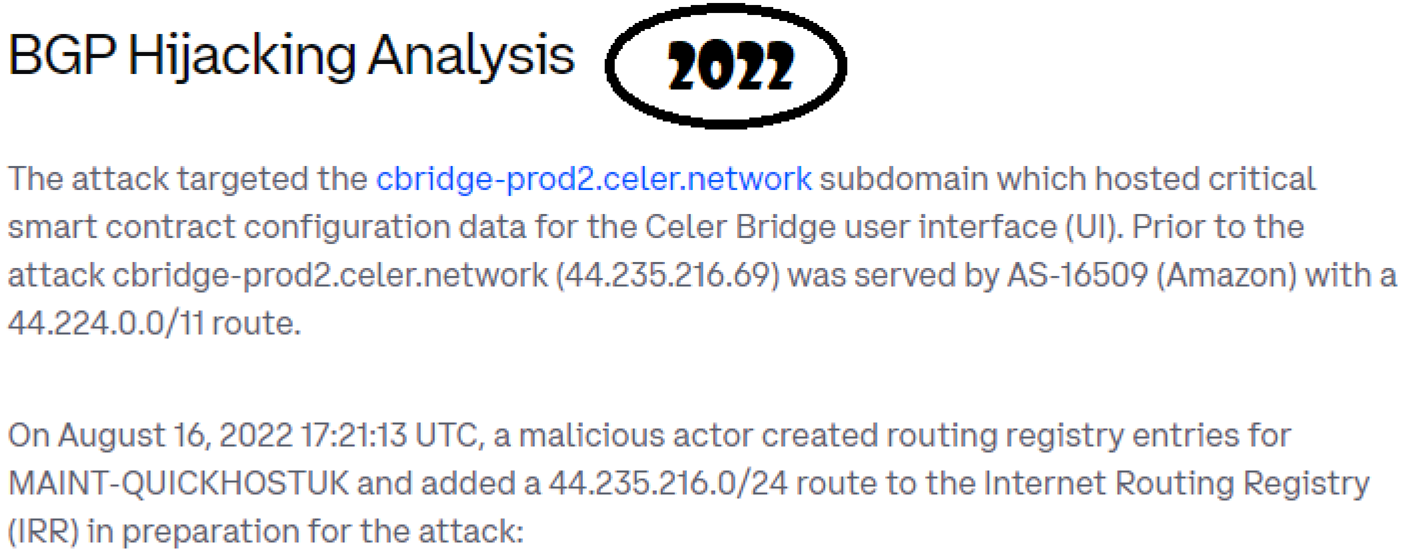
…to steal cryptocurrencies (2014-2022)

2014



Researchers at Dell's Secureworks have uncovered multiple BGP incidents used to steal bitcoins. According to Secureworks, the attacker used a compromised administrator account at a yet undisclosed Canadian ISP.

2022



BGP Hijacking Analysis

The attack targeted the cbridge-prod2.celer.network subdomain which hosted critical smart contract configuration data for the Celer Bridge user interface (UI). Prior to the attack cbridge-prod2.celer.network (44.235.216.69) was served by AS-16509 (Amazon) with a 44.224.0.0/11 route.

On August 16, 2022 17:21:13 UTC, a malicious actor created routing registry entries for MAINT-QUICKHOSTUK and added a 44.235.216.0/24 route to the Internet Routing Registry (IRR) in preparation for the attack:

2017

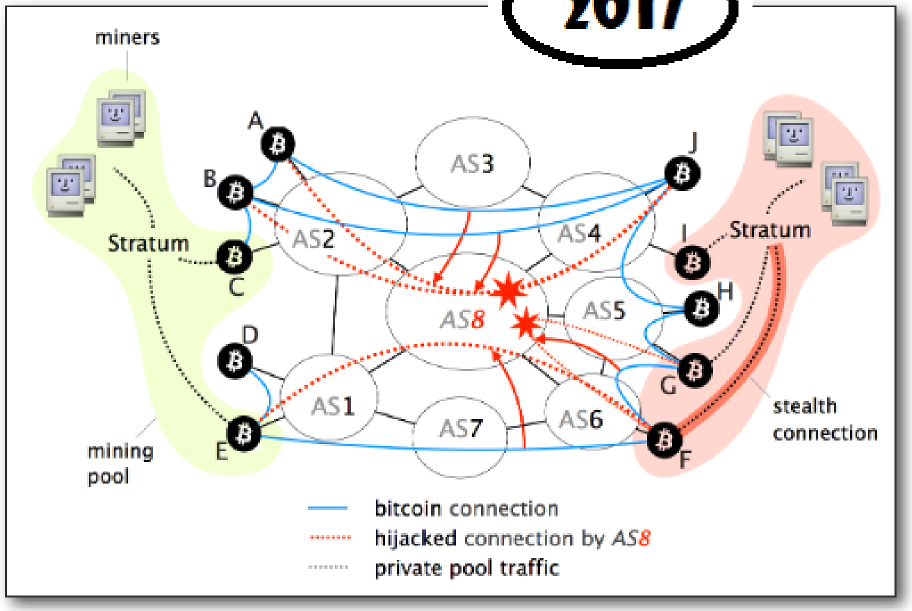
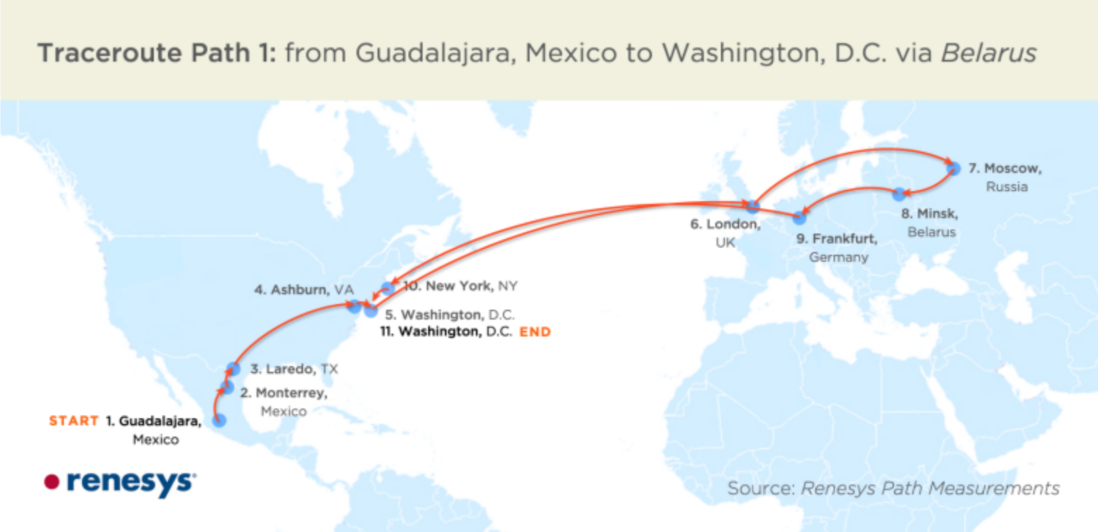


Illustration of how an AS-level adversary (AS8) can intercept Bitcoin traffic by hijacking prefixes to isolate the set of nodes P = (A, B, C, D, E).

Notable Hijacking Incidents

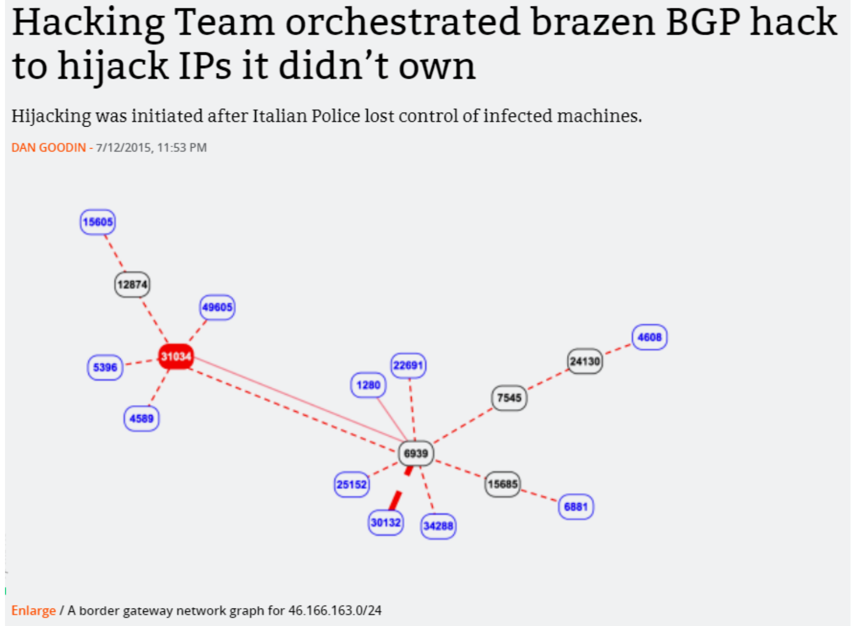
ptcl

YouTube



Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*

Source: *Renesys Path Measurements*



Hacking Team orchestrated brazen BGP hack to hijack IPs it didn't own

Hijacking was initiated after Italian Police lost control of infected machines.

DAN GOODIN - 7/12/2015, 11:53 PM

Enlarge / A border gateway network graph for 46.166.163.0/24

Examples: Looking at what Cloudflare records

Looking at incidents classified as ‘hijacks’ with a duration bigger than 4 hours

IPv4 prefixes only

Marked as «RPKI Invalid»

CLOUDFLARE

CLOUDFLARE BLOG

Routing information now on Cloudflare Radar

Examples: Looking at what Cloudflare records

50.230.13.0/24 announced by AS33567 (US) instead of AS397487 (US), 14 hours, 2024-03-24

46.253.129.0/24 announced by AS212217 (GB) instead of AS210727 (GB), 6 hours, 2024-03-23

157.254.217.0/24 announced by AS203377 (TR) instead of AS14618 (US), 14 hours, 2024-03-23

Examples: Looking at what Cloudflare records

«Comcast Cable Communications» announced a prefix from «Baltimore Ravens Limited Partnership»

Probably a case where the ISP announces the customer’s prefix as his own

«BB-Online UK Ltd» announced a prefix from «Buy Limited»

Whois data is very similar. Probably sibling companies. But what if they are competition?

«Mehmet Uzunca» announced a prefix from «Amazon.com»

The hijacked /24 is marked as «Redhat (C10658942)».

Reverse DNS includes nameservers ns1.nativechip.org and ns2.nativechip.org

Examples: Looking at what Cloudflare records

All the 3 cases are hijacks (certainly not leaks)

The legitimate owners did create route certificates (ROA) to protect these prefixes

The last case is worrying. What happened during those 14 hours?

Why are hijacks possible?

Route Origin Validation (ROV) is still low.

(Picture from the APNIC Blog)

RPKI Invalids should be dropped

People still accept signed papers (LOA) in order to accept routes

These can be easily forged

So, what can we do?

Talk to your networking people about this

MANRS

Consider joining Mutual Agreed Norms for Routing Security

Embrace RPKI: Publish your ROAs (route certificates)

DROP invalid routes (in realtime)

So, what can we do?

Discontinue the acceptance of LOAs

Rely solely on RPKI

> «If you are authorized to announce it, then prove it!»

Ongoing effort at the netsec-sig at FIRST

Takeaways

A more secure exchange of Internet routes is needed

Hijacks happen everyday, and why they happen is very diverse

Prefix/Network ownership is demonstrable with RPKI

You can also help!

References

- radar.cloudflare.com/routing
- www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents
- www.internetsociety.org/blog/2014/08/bgp-hijacker-steals-bitcoins
- hackingdistributed.com/2017/05/01/bgp-attacks-on-btc
- www.coinbase.com/blog/celer-bridge-incident-analysis
- www.kentik.com/blog/bgp-hijacks-targeting-cryptocurrency-services
- manrs.org

Any questions?

Co-funded by
the European Union