

Hijacks – why should we care?

Wednesday, 10 April 2024 13:30 (20 minutes)

Carlos Friças is the Head of RCTS CERT, the CSIRT for the portuguese NREN (FCCN).
This presentation is about network security.

Our previous experience with BGP hijacks comes from handling the case with the notorious Bitcanal hijacker, which was a local internet exchange (Gigapix) member since the previous 4 years, before everything reached the public eye.

This incident led us to deploy local means to observe future cases of hijacking, and we also started a due diligence process regarding joining requests at the internet exchange.

Recently we had another encounter with a newbie hijacker, which seems to have a different motivation.

I plan to also cover some of the latest hijacking cases, based on public data collected from Cloudflare's Radar.

This presentation also intends to work as a callout to everyone not only to publish their route certificates (ROA) but also to start doing route origin validation (ROV), which in most cases will stop the impact of intentional BGP hijacks on your infrastructure.

The information should be useful for the full audience, to raise awareness about this type of tactic.

Primary author: Mr FRIÇAS, Carlos (RCTS CERT (FCCN))

Presenter: Mr FRIÇAS, Carlos (RCTS CERT (FCCN))

Session Classification: Real World Security

Track Classification: Presentation