# CryptoCurrency Hacked using BGP Hijacking

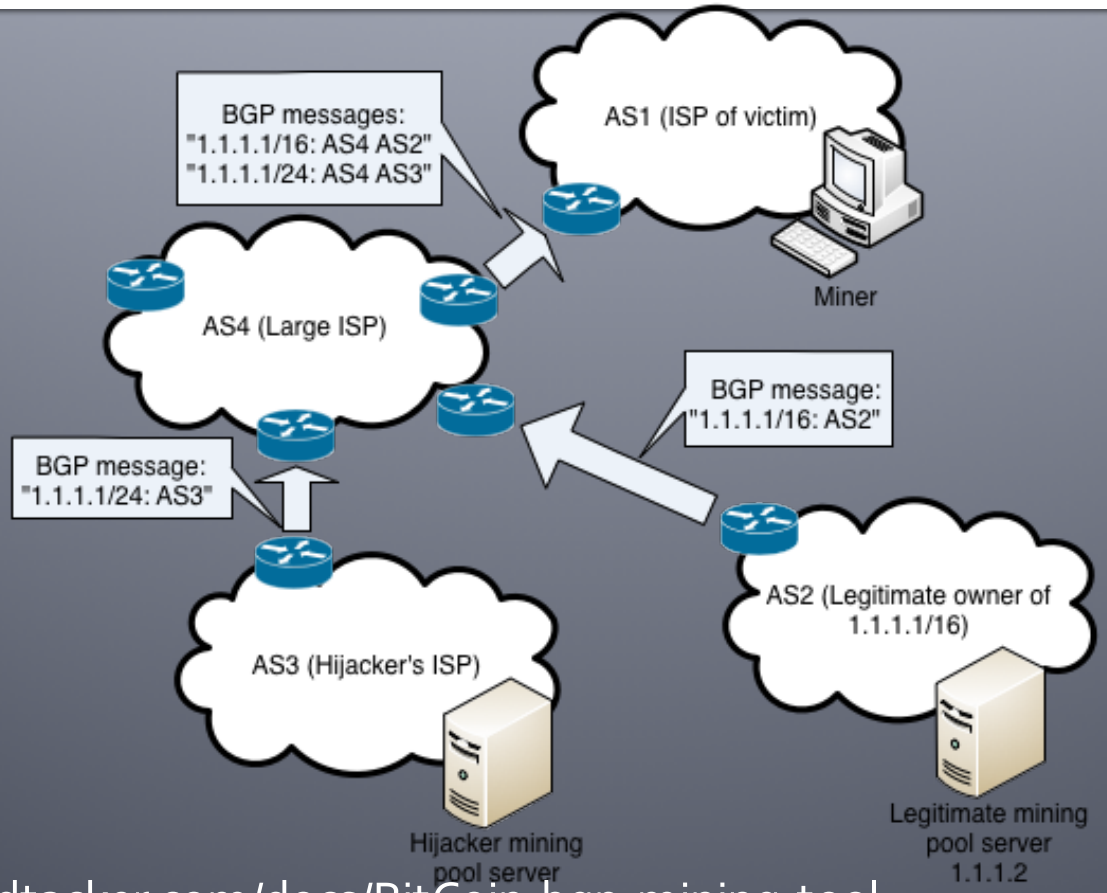
## Case Study: eNet & Myetherwallet.com

Manutsiri Chansutthirangkool
CISSP, CISM, CRISC, AWSCSA, COBIT5(F), ITIL(F), MCT, Security+, Project+, CTT+
Lecturer: Mahidol University
Cyber Security Manager: Bigfish Enterprise Limited

# Agenda

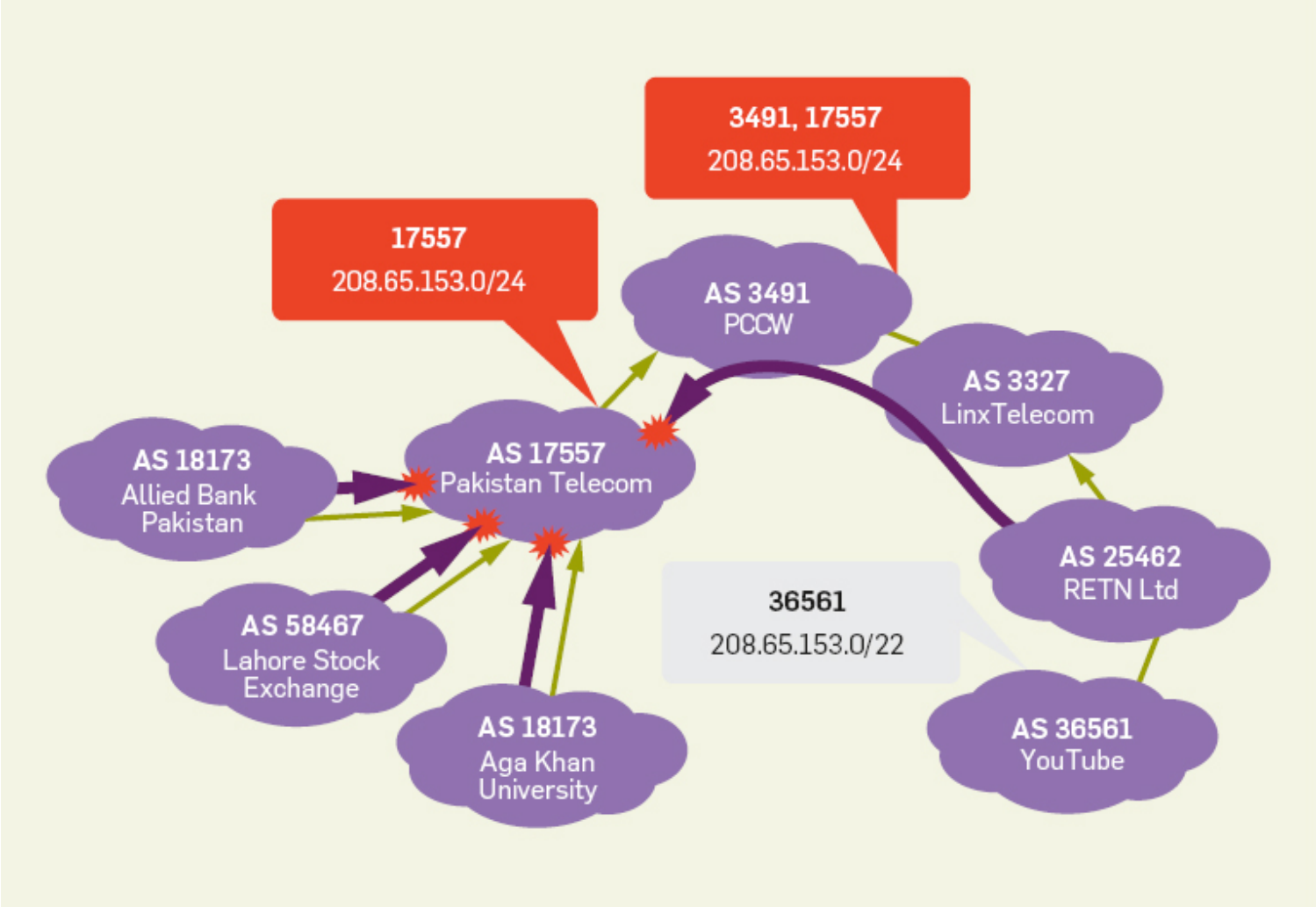
- BGP Hijacking
- Our Case Study
- How to Prevent

# BGP Hijacking




http://www.cloudtacker.com/docs/BitCoin-bgp-mining-tool

# 24 Feb, 2008
# Pakistan Telecom hijack Youtube

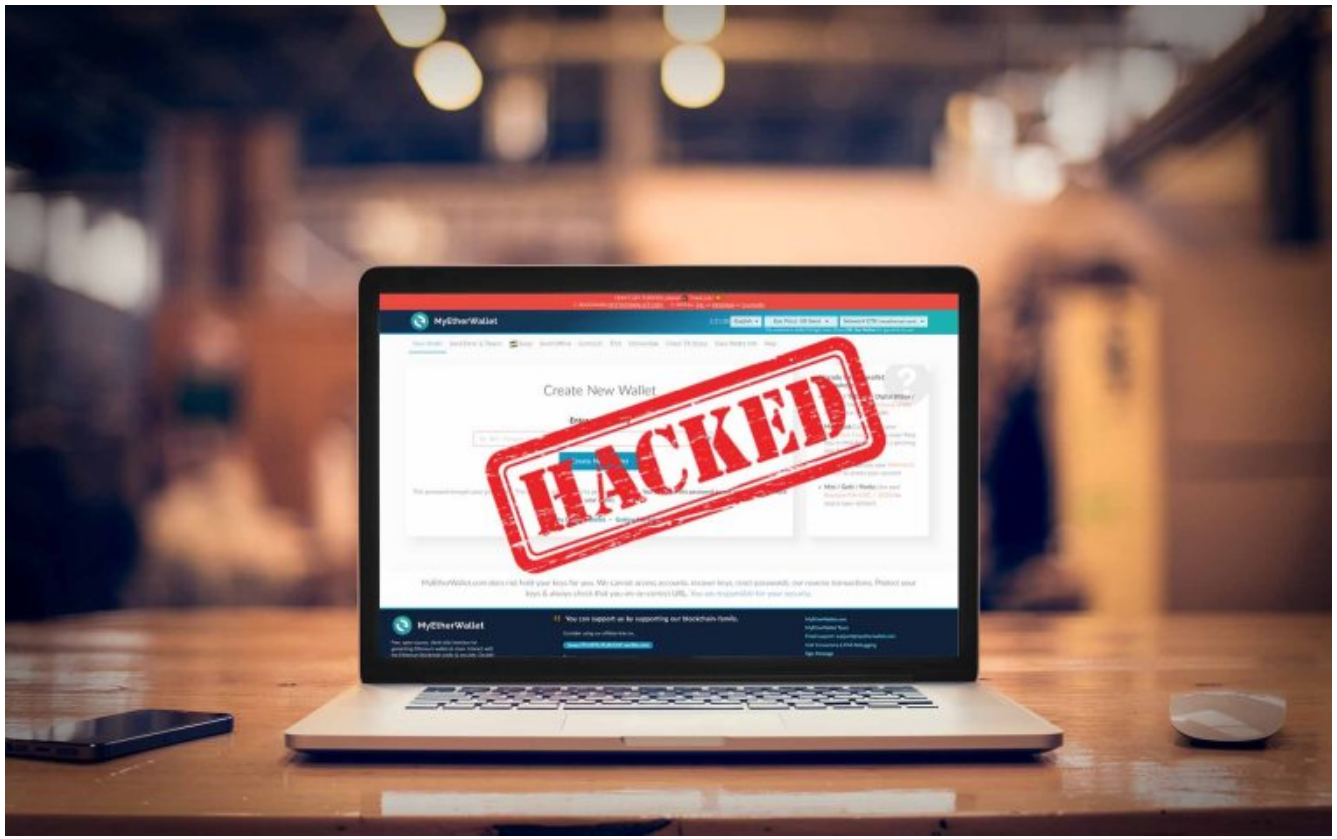



https://cacm.acm.org/magazines/2014/10/178781-why-is-it-taking-so-long-to-secure-internet-routing/abstract

# Our Case Study

## Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

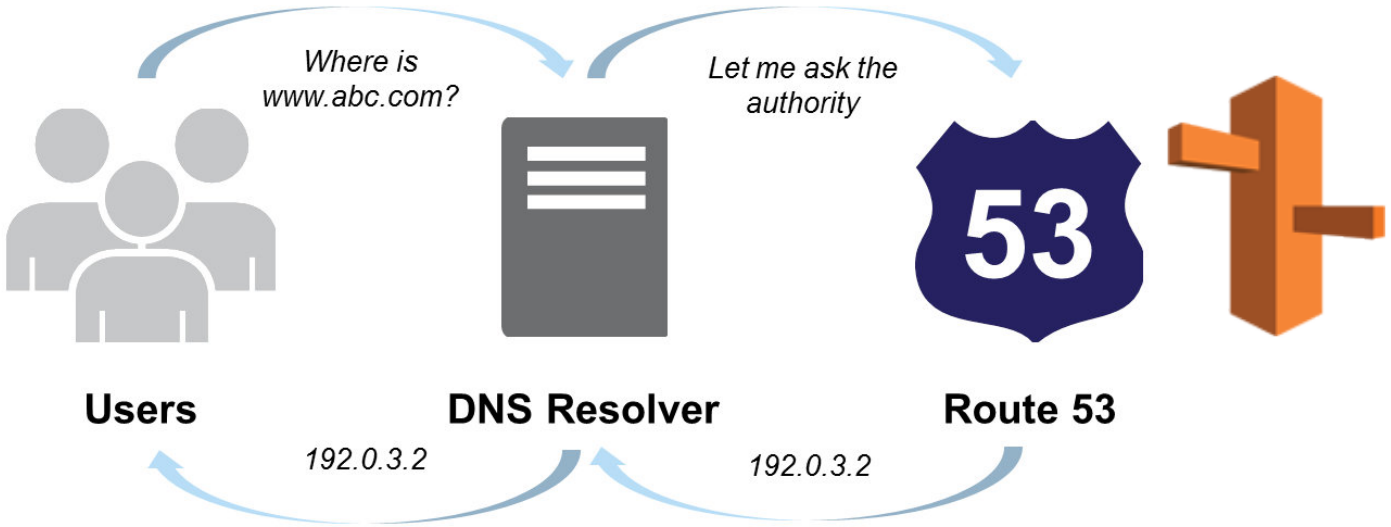
By Russell Brandom | @russellbrandom | Apr 24, 2018, 1:40pm EDT




https://securitynews.io/

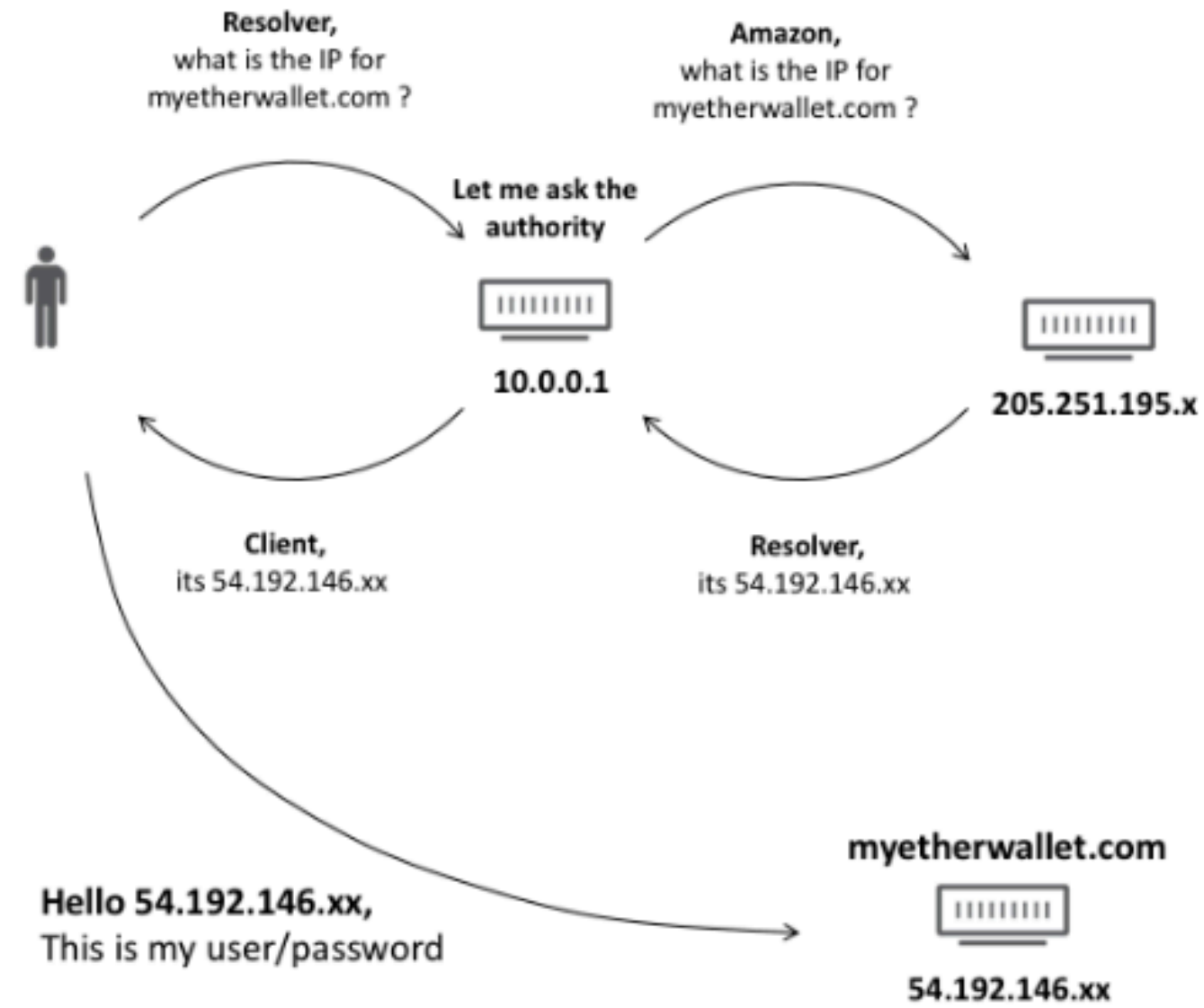
# MyEtherWallet.com

- Free, open-source, client-side interface for generating Ethereum wallets & more.
- Using AWS Route53 as its Authoritative name server



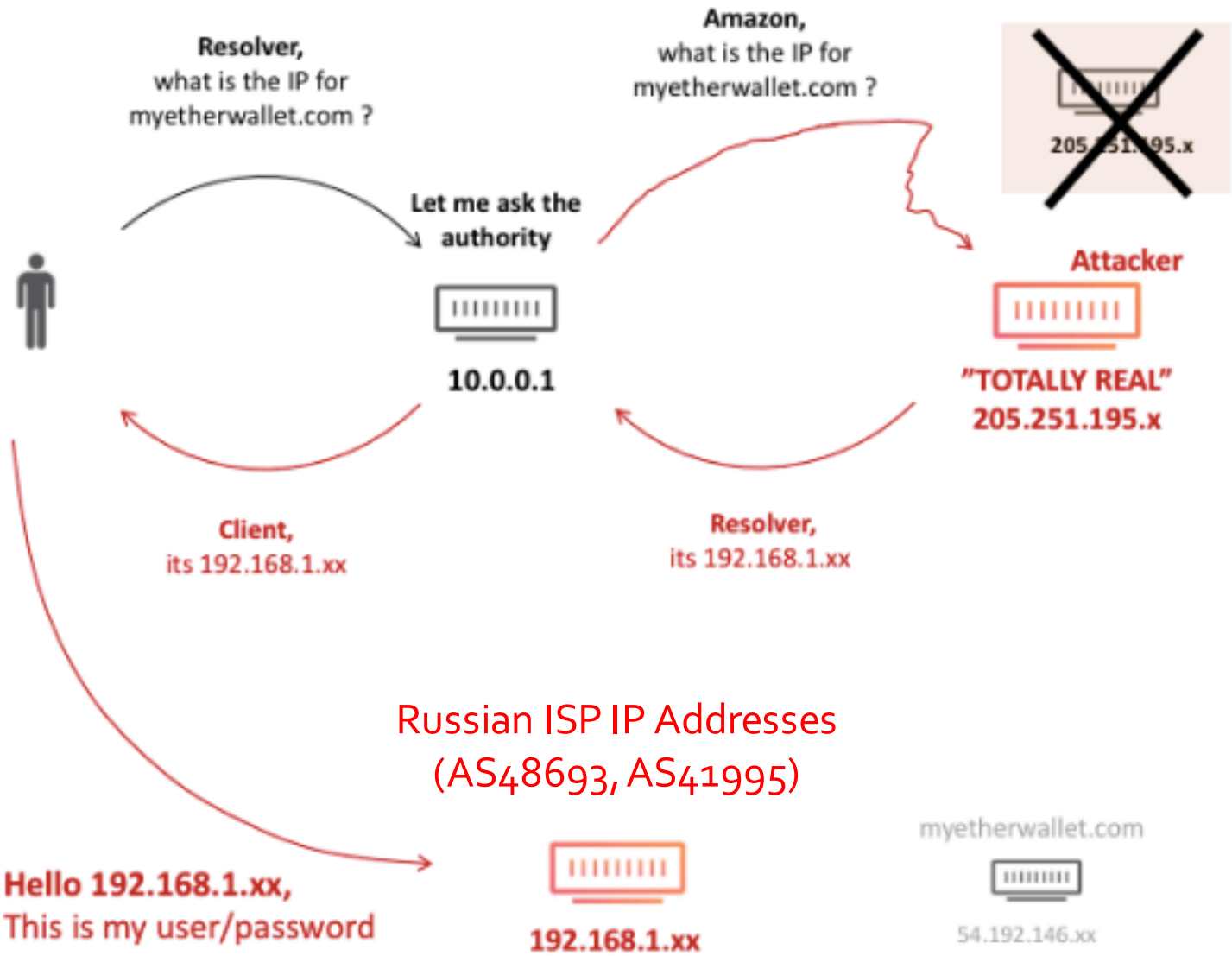

https://www.innofied.com/amazon-route-53/

# Normal situation




https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/

# 11:05:00 UTC – 12:55:00 UTC 24 April 2018



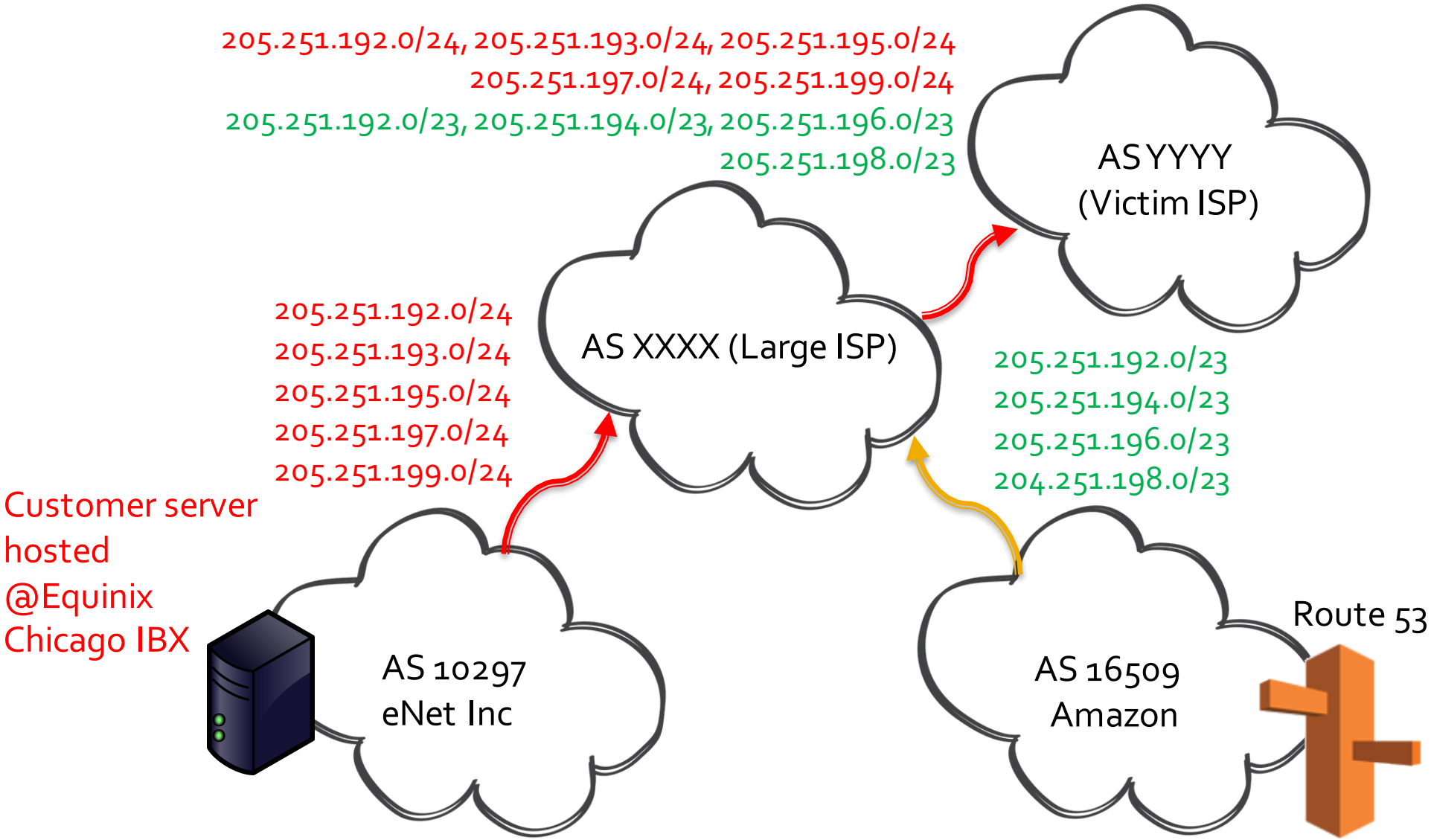

https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/

# AWS Route53 Prefix

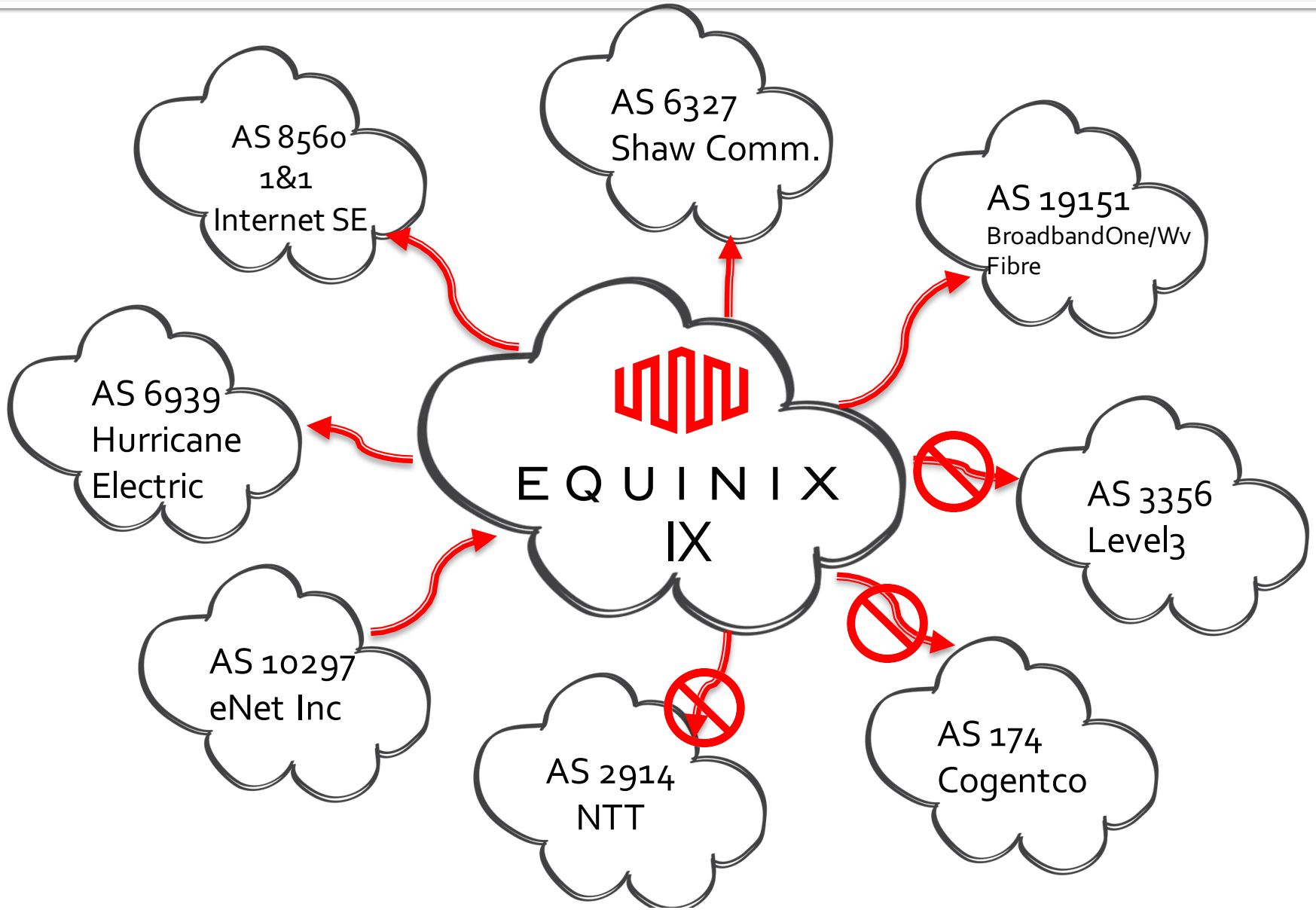
- Route53 Prefix advertised by AWS (AS16509)
  - 205.251.192.0/23
  - 205.251.194.0/23
  - 205.251.196.0/23
  - 204.251.198.0/23

https://www.innofied.com/amazon-route-53/

# AWS Route53 Prefix Hijacking via eNet Inc.

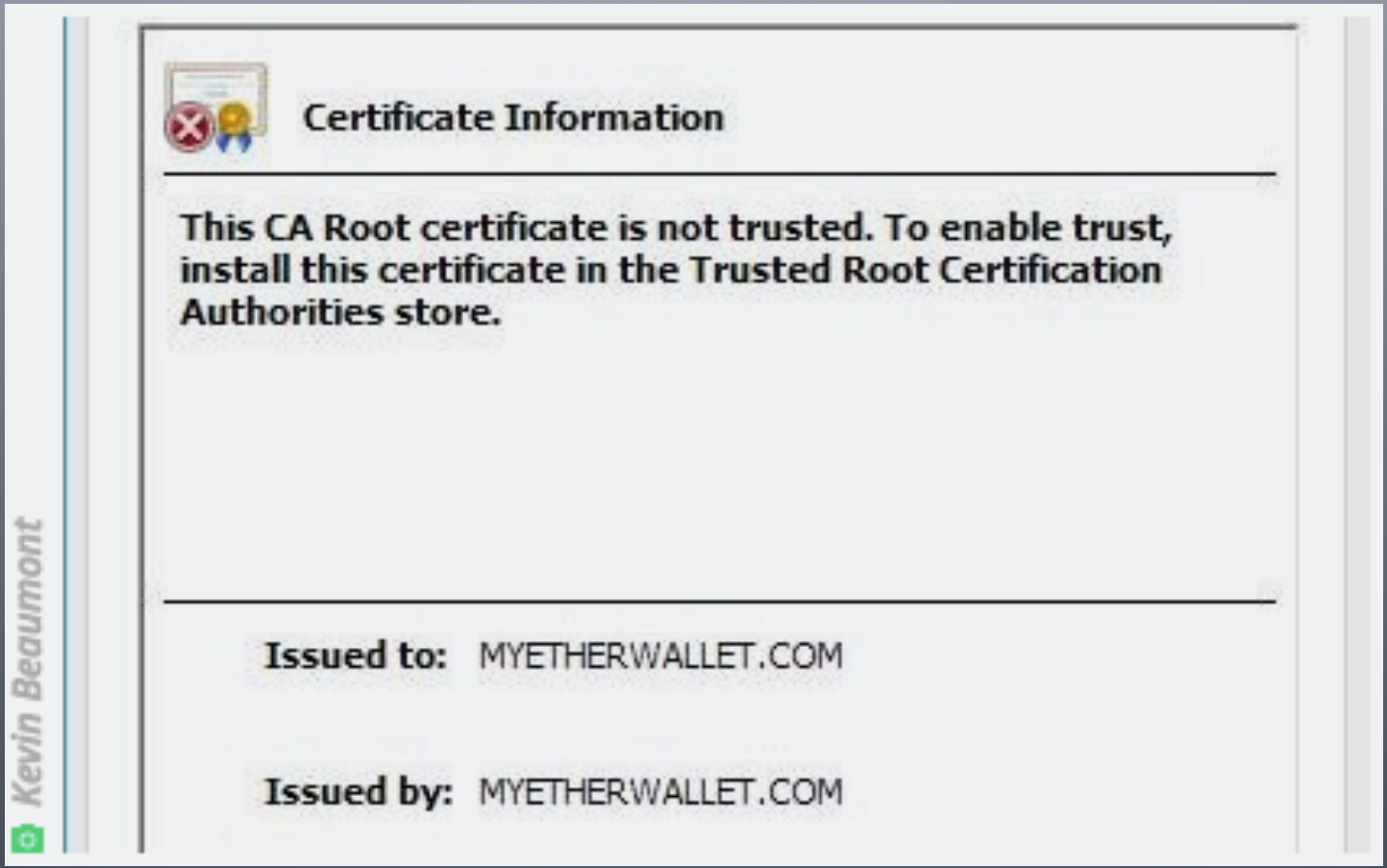


# Equinix Chicago IX



# How to Prevent

End-user level

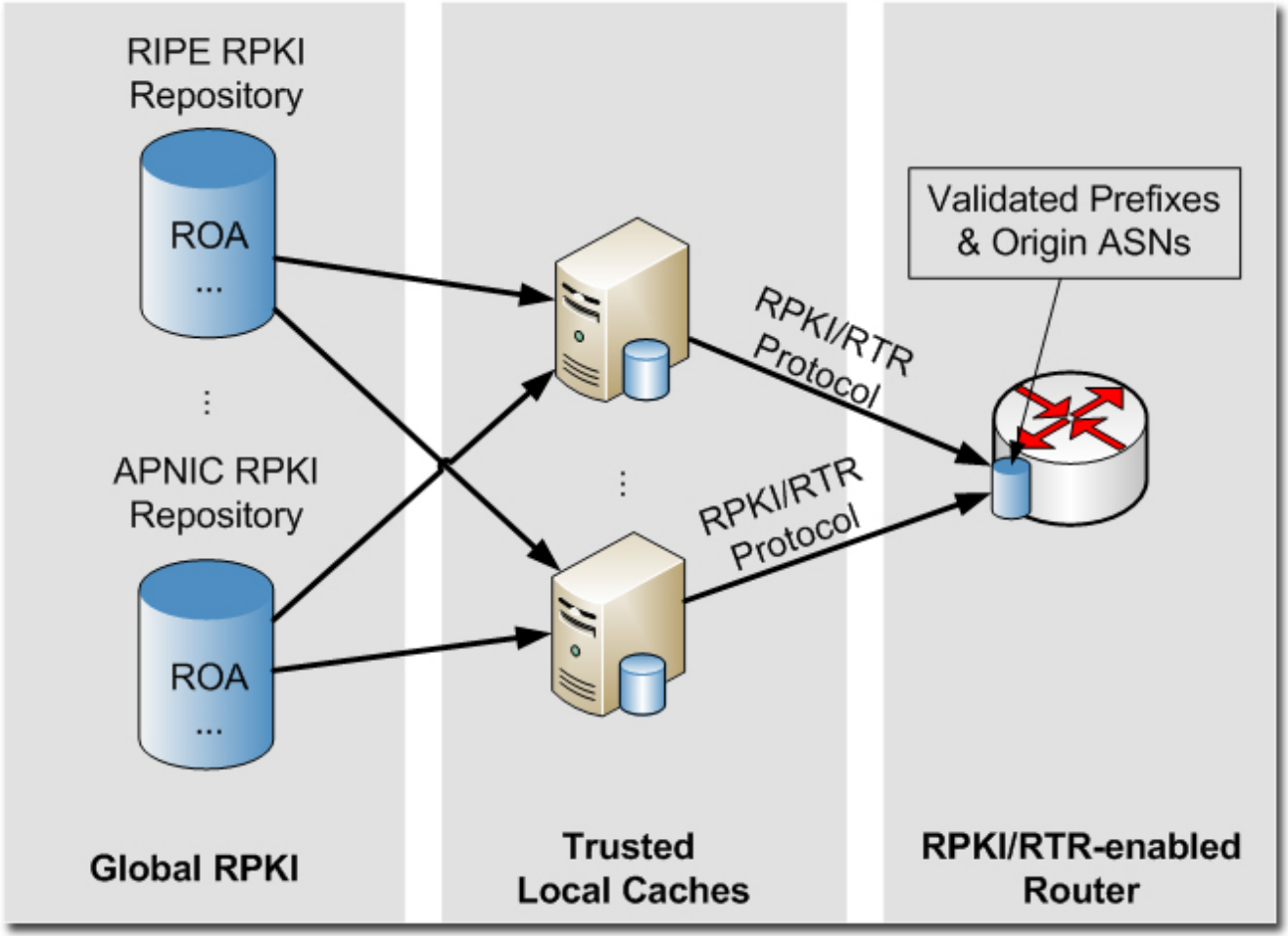


# ISP Level
# Route filtering

- Using filtering to prevent advertisement of incorrect routing information
  - Using IRR to produce prefix filters
    - Specific-prefix outbound filtering from your network to peers and upstreams
    - Specific-prefix inbound filtering from customers
    - Specific-prefix inbound filtering of peers to your network

https://www.manrs.org/guide/filtering/

# ISP Level RPKI Validator




http://rtrlib.readthedocs.io/en/latest/intro.html

# Join MANRS Programme

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to eliminate the most common routing threats
- https://www.manrs.org


Thank
You