



Internet Infrastructure Security

Benno Overeinder
NLnet Labs

The security spectrum

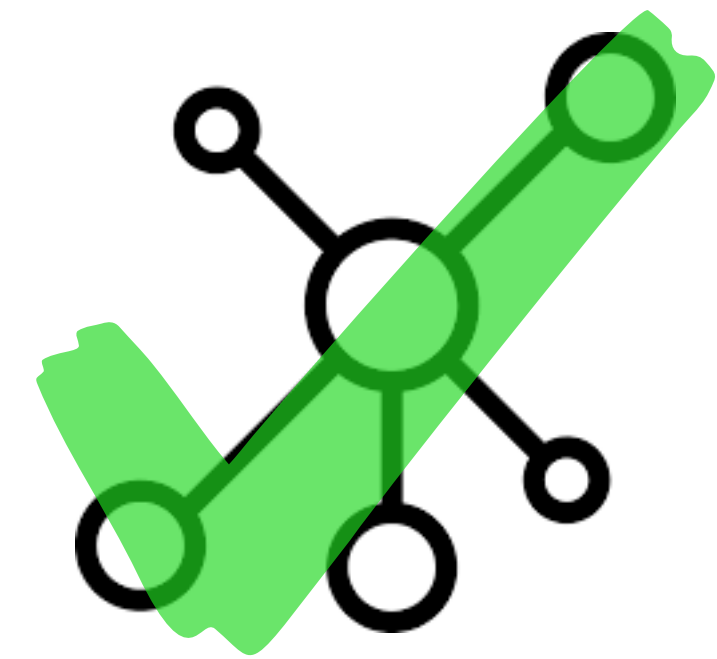
What's in ...
and what's out



The Security Spectrum



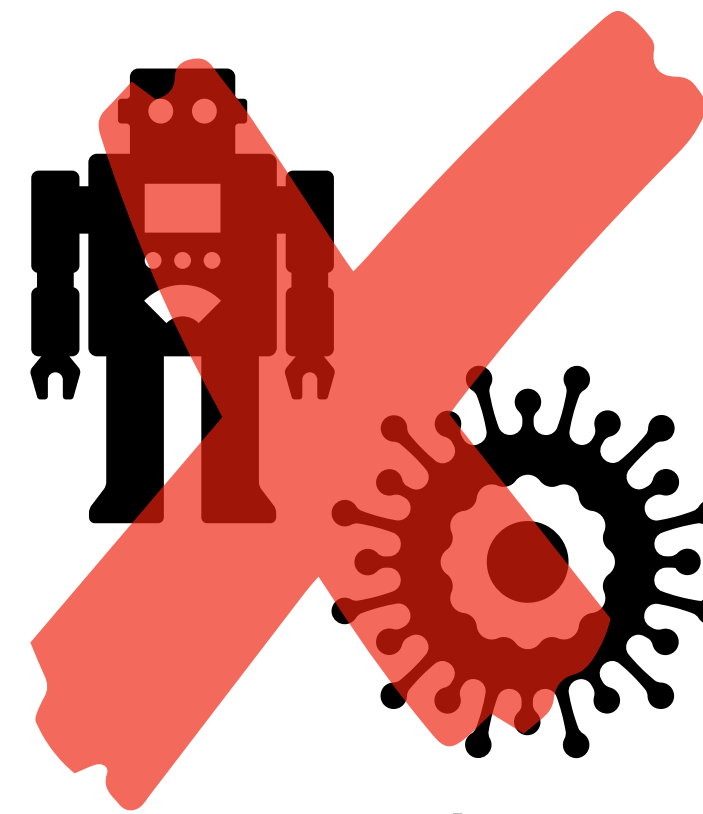
popular CCTV shop name



internet infrastructure



social engineering



botnets and viruses

Message to Take Away

- Security requires an integral approach:
 - not BGP filtering, RPKI or DNS security, but **all** of them
- Security requires a collaborative approach, e.g.:
 - MANRS program
 - DDoS Clearing House
- Security requires transparency
 - open source & open standards

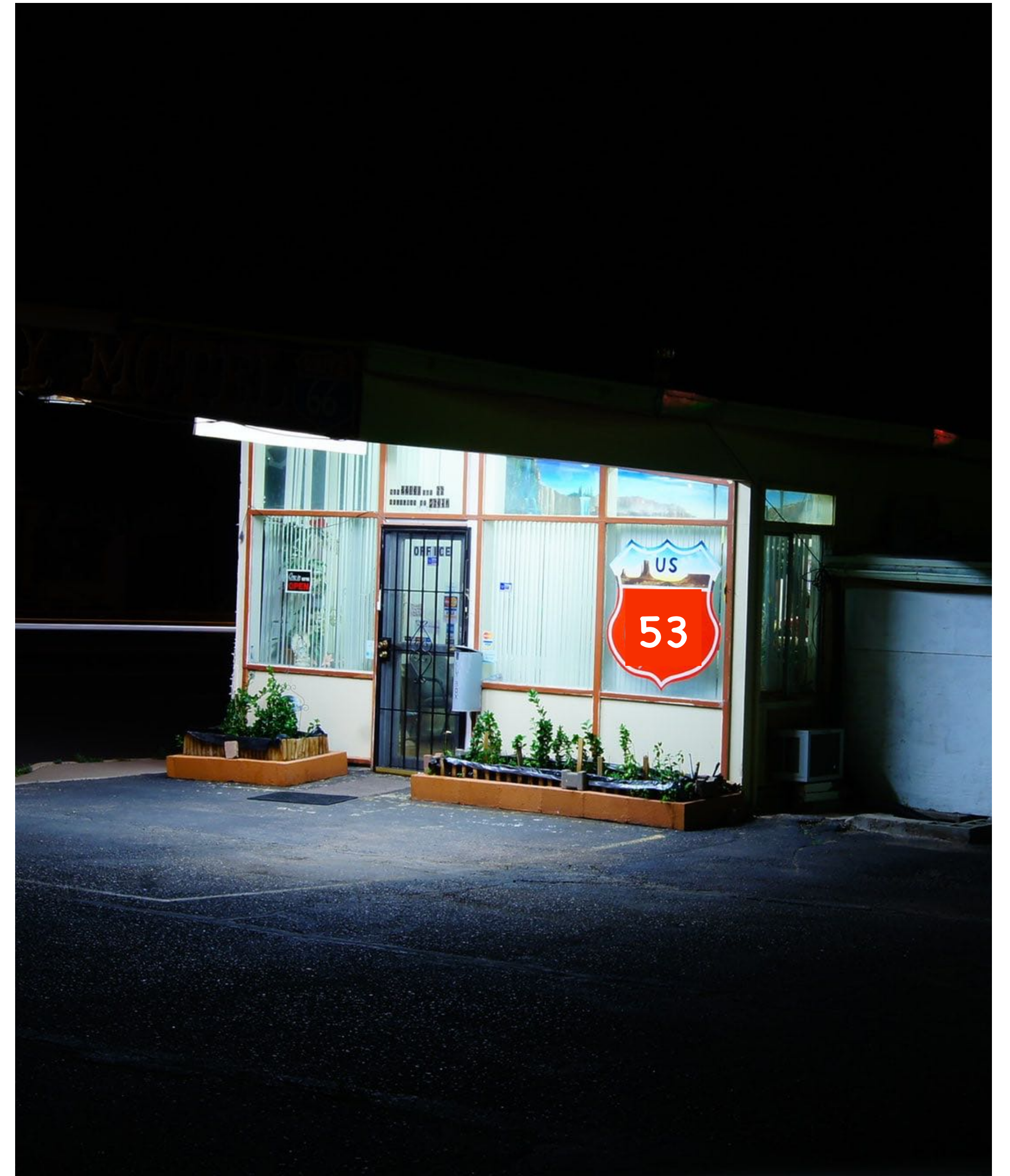


Two High-Profile Examples Explaining Why

AWS Route 53 Hijack
Sea Turtle DNS Hijack



AWS Route 53 Hijack

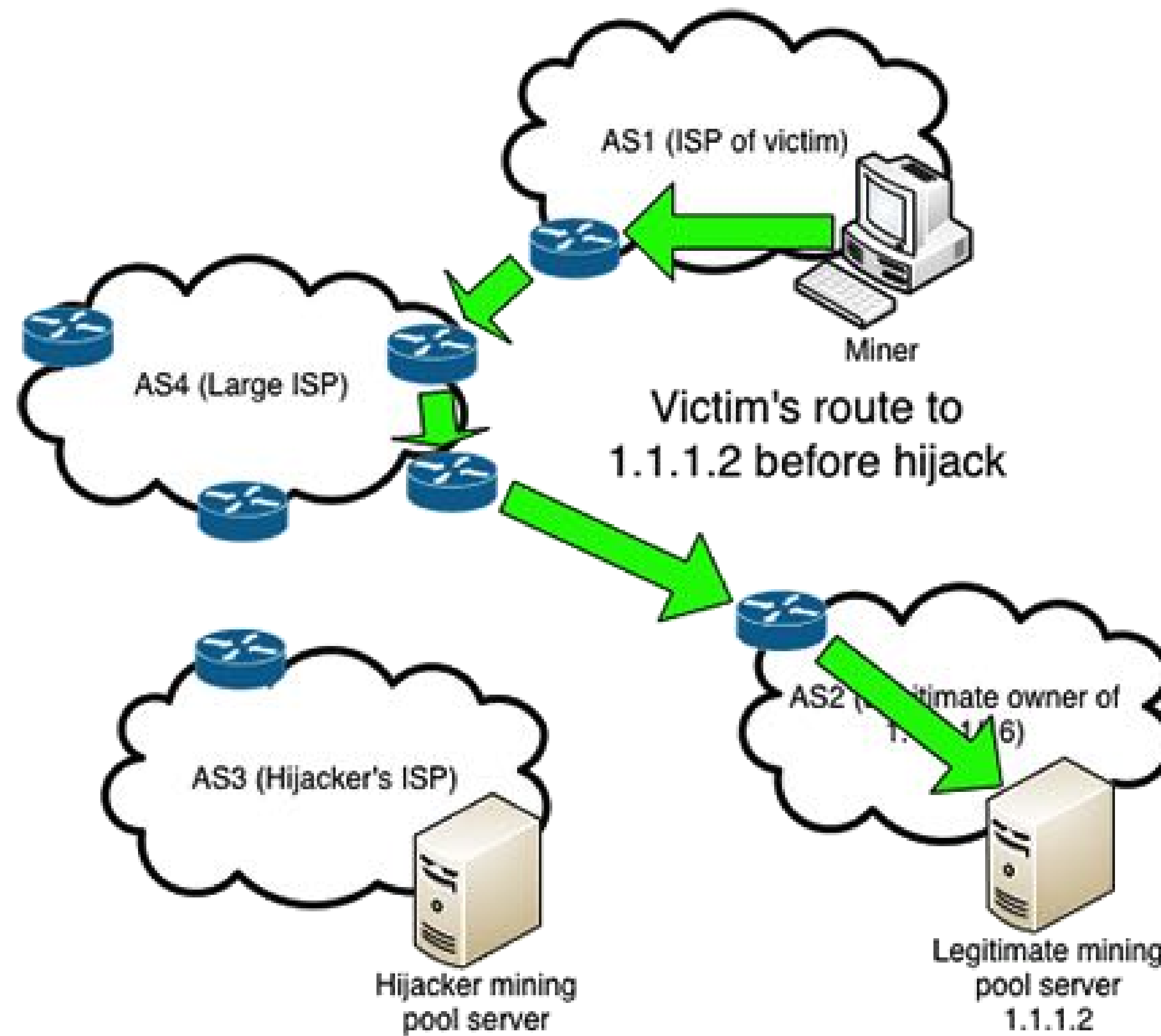


Amazon Route 53 Hijack

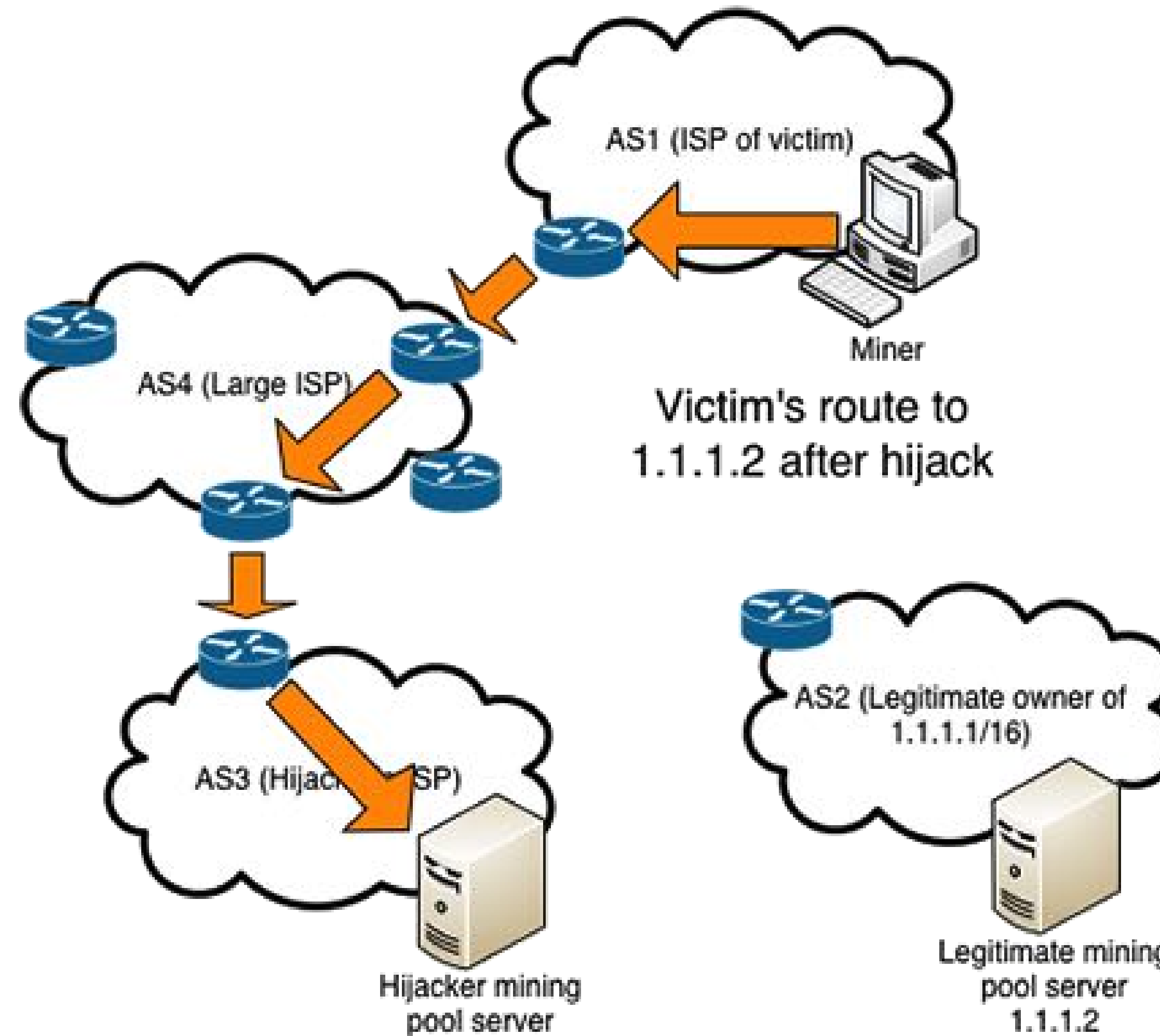
This is not about cryptocurrencies & blockchain!

- Internet routing 'hijack' to steal crypto coins
- Internet routing protocol BGP
 - routing protocol from 1994
 - calculates network reachability and takes routing decisions
 - no security, implicit trust: 'routing by rumour'

Status: All OK



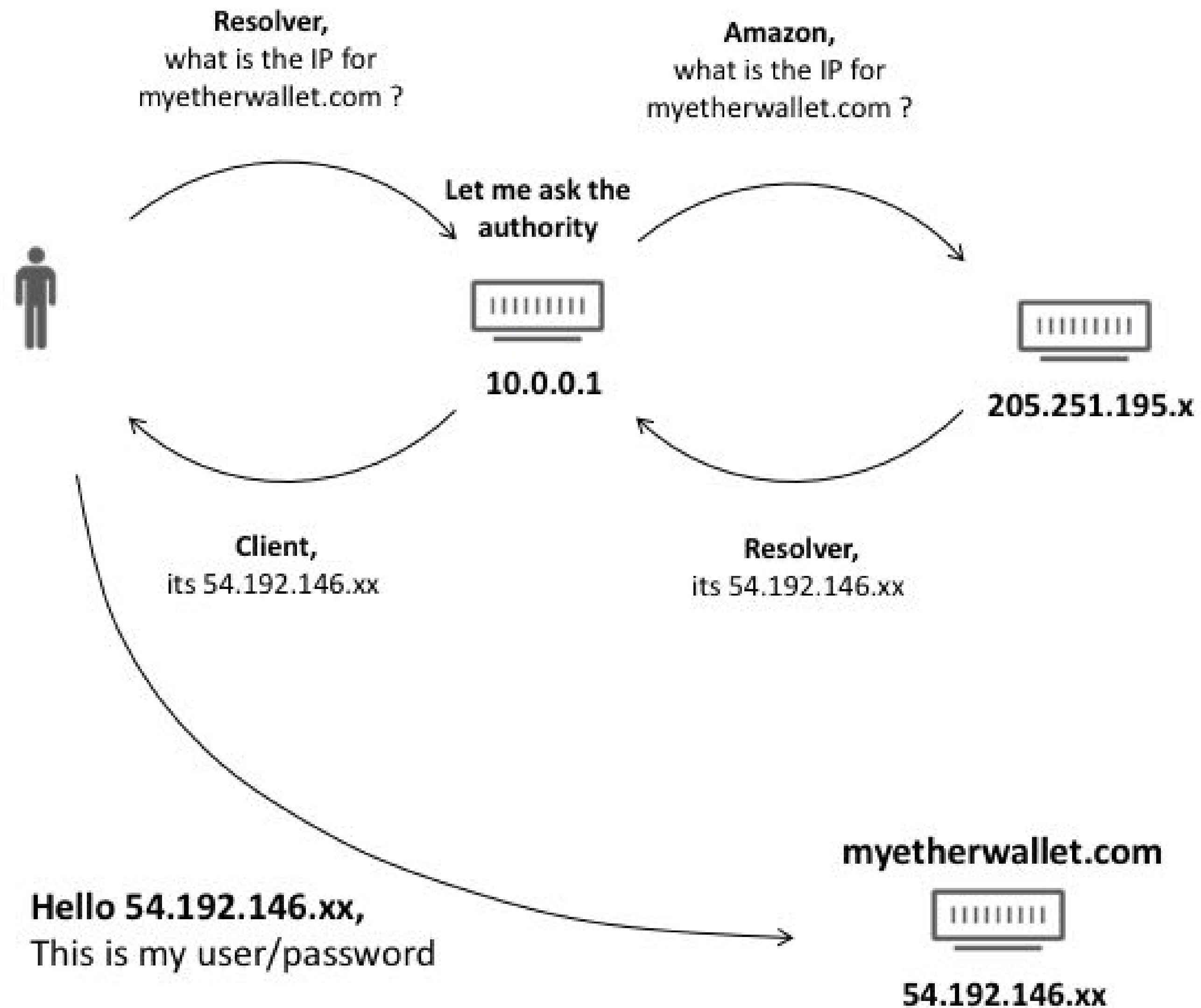
Status: A Route Hijack



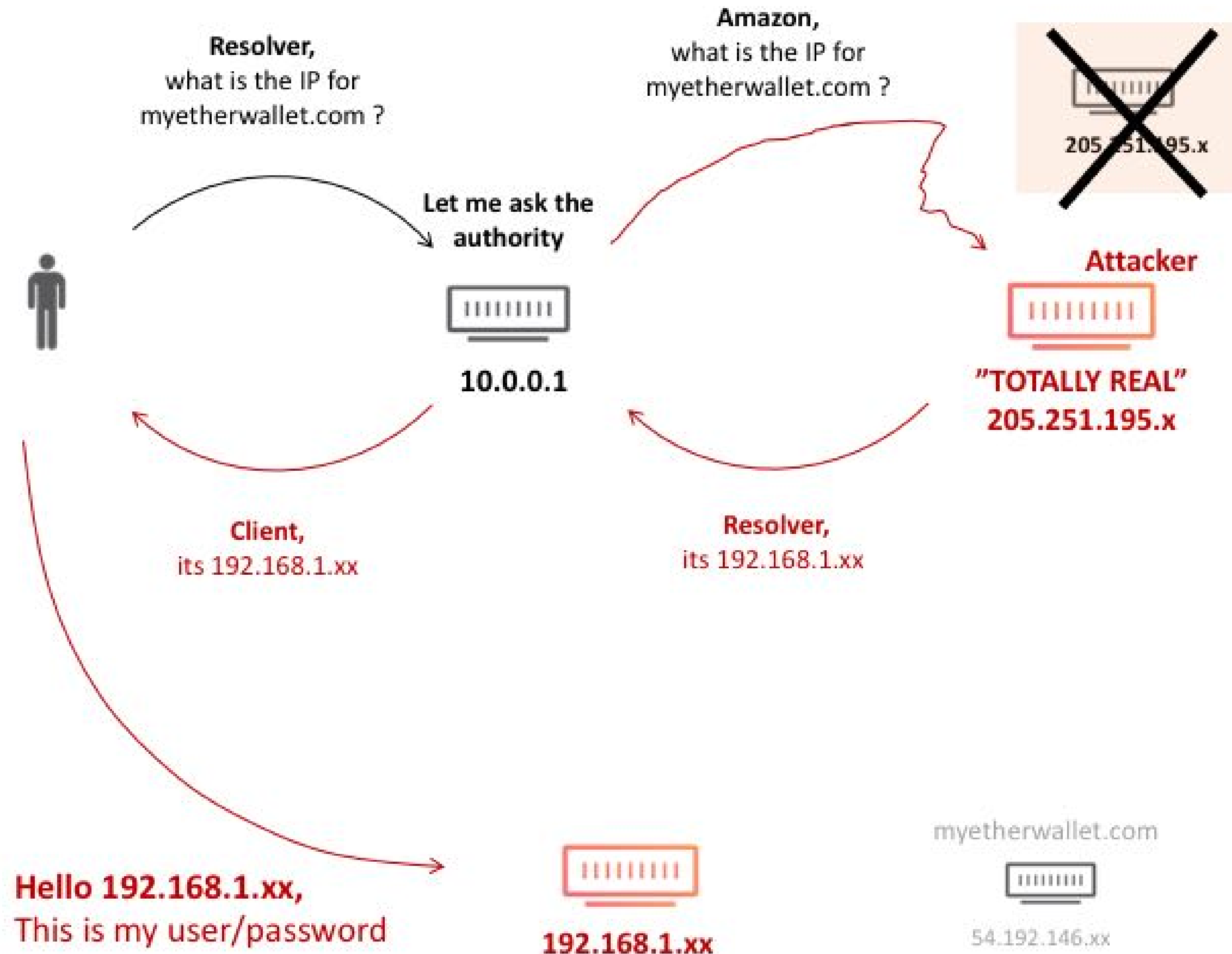
Two-stage Attack: DNS Spoofing

- Intention of Amazon Route 53 hijack: DNS spoofing
- False DNS information
 - cryptocurrency digital wallet: myetherwallet.com
 - not legitimate answer to myetherwallet.com, but the IP address of the attacker

All OK: Amazon Route 53 DNS



Route Hijack: Amazon Route 53 DNS

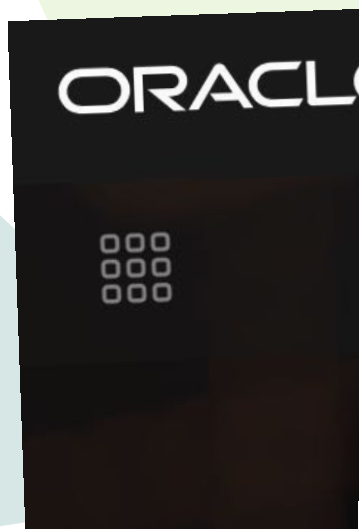


Mitigation of Amazon Route 53 Hijack



Recent News on Route Hijacks

And lesser recent news



WIKIPEDIA
The Free Encyclopedia

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia
- Wikipedia store

Interaction

- Help
- About Wikipedia
- Community portal
- Recent changes
- Contact page

Tools

- What links here
- Related changes

Not logged in Talk Contributions Create account Log in

Article Talk

Read Edit View history

Search Wikipedia



This November is the Wikipedia Asian Month. [Come join us.](#)

AS 7007 incident

From Wikipedia, the free encyclopedia

The **AS 7007 incident** was a major disruption of the [Internet](#) on April 25, 1997, that started with a [router](#) operated by [autonomous system](#) 7007 (MAI Network Services, although sometimes incorrectly attributed to the Florida Internet Exchange^[1]) accidentally leaking a substantial part of its entire [route table](#) to the Internet, creating a routing [black hole](#).

Probably because of a bug in the affected router, the routes leaked were deaggregated to [/24](#) prefixes, which were more specific than the routes originally present on the Internet, and had the [AS path](#) rewritten to 7007, leading the [Border Gateway Protocol](#) (BGP) used by the Internet's routers to prefer the leaked routes. This was then exacerbated by other problems that prevented the routes from disappearing from other networks' routing tables, even after the original router that had sent them had been disconnected. The combination of these factors resulted in an extended disruption of operations throughout the Internet.

Analysis of this event led to major changes in Internet Service Providers' BGP operations intended to mitigate the effects of any subsequent similar events.^[*citation needed*]



BEST PR

How offlin

You
Inter

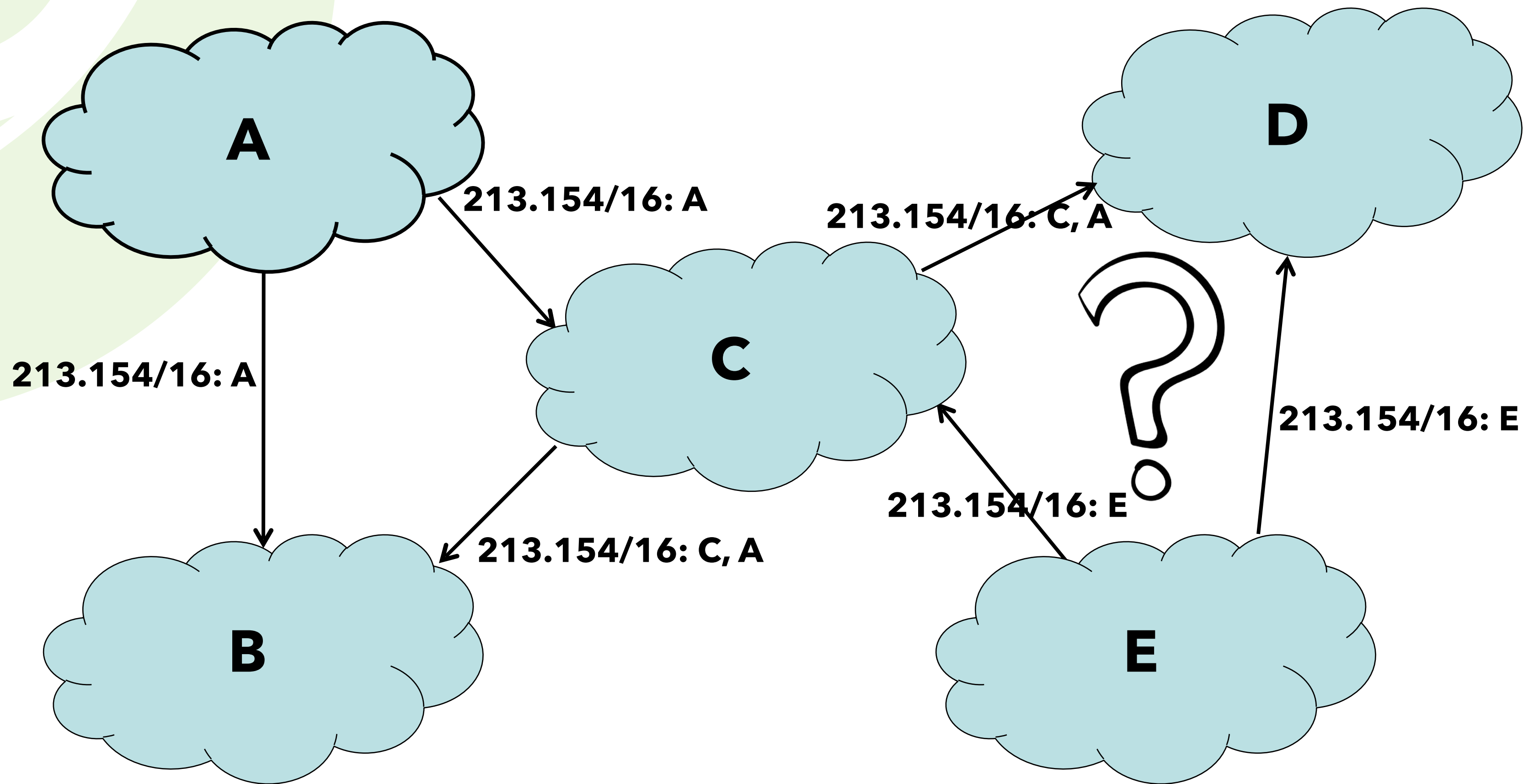
GAMING & CULTURE FOR

na

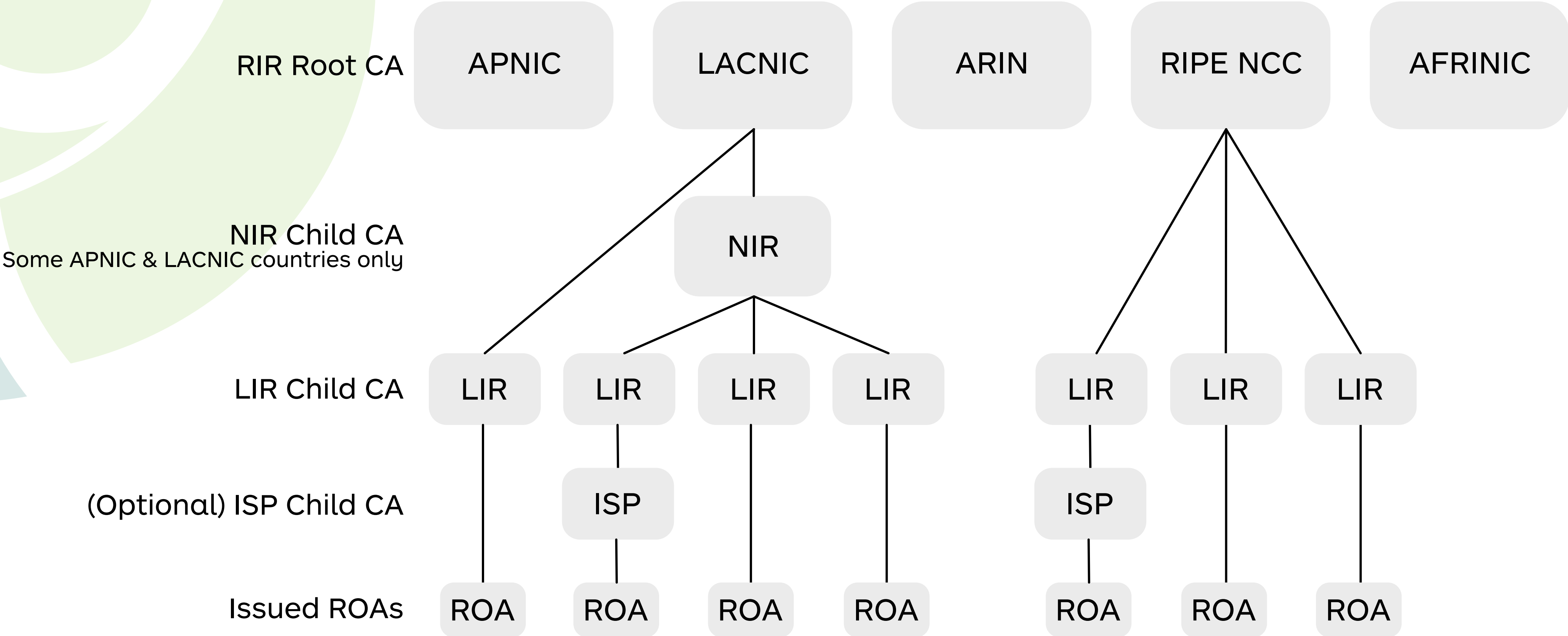
GAMING & CULTURE

aOne, a
, with
ick involved

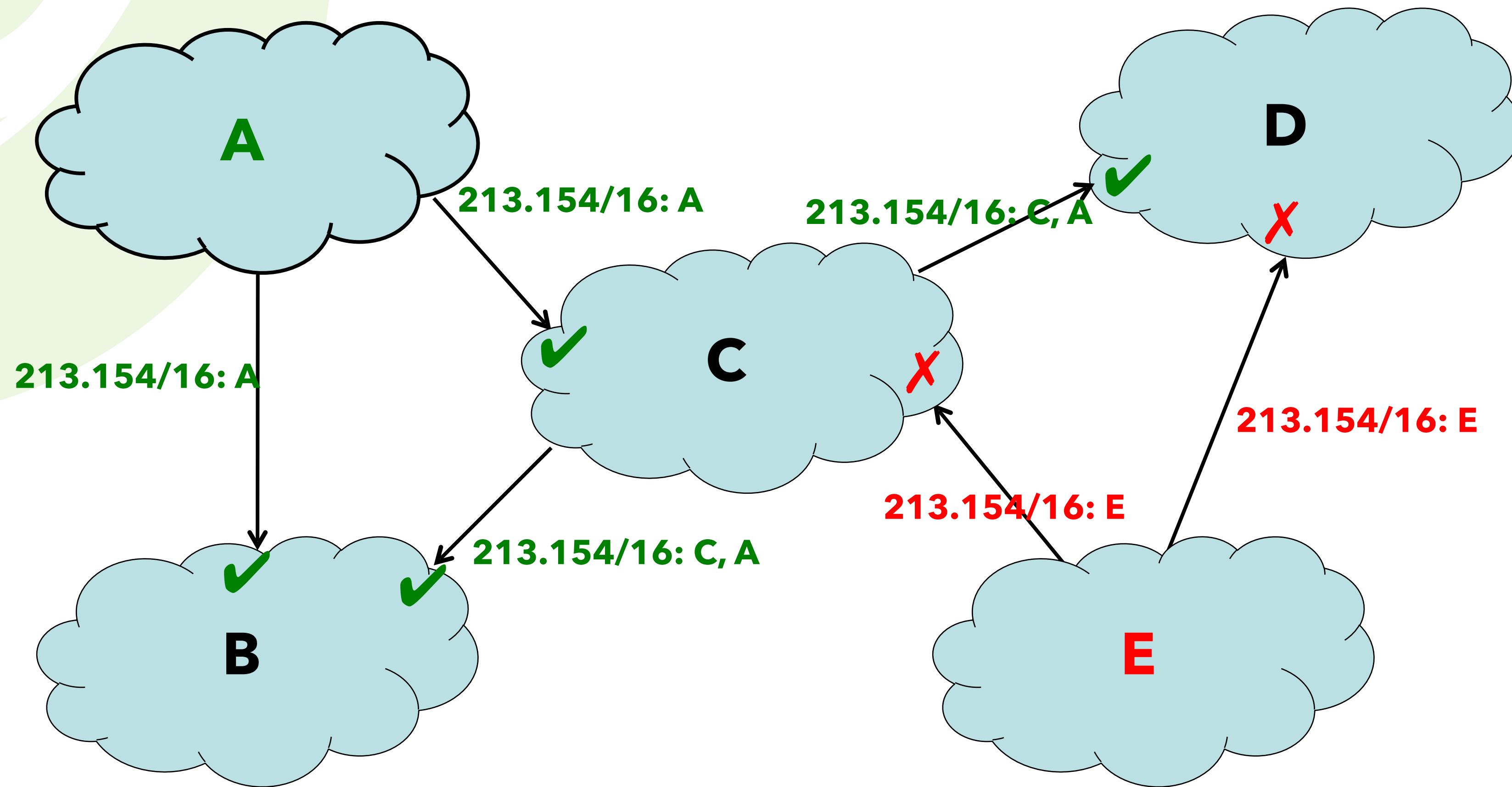
Route Hijacks 101



RPKI Structure

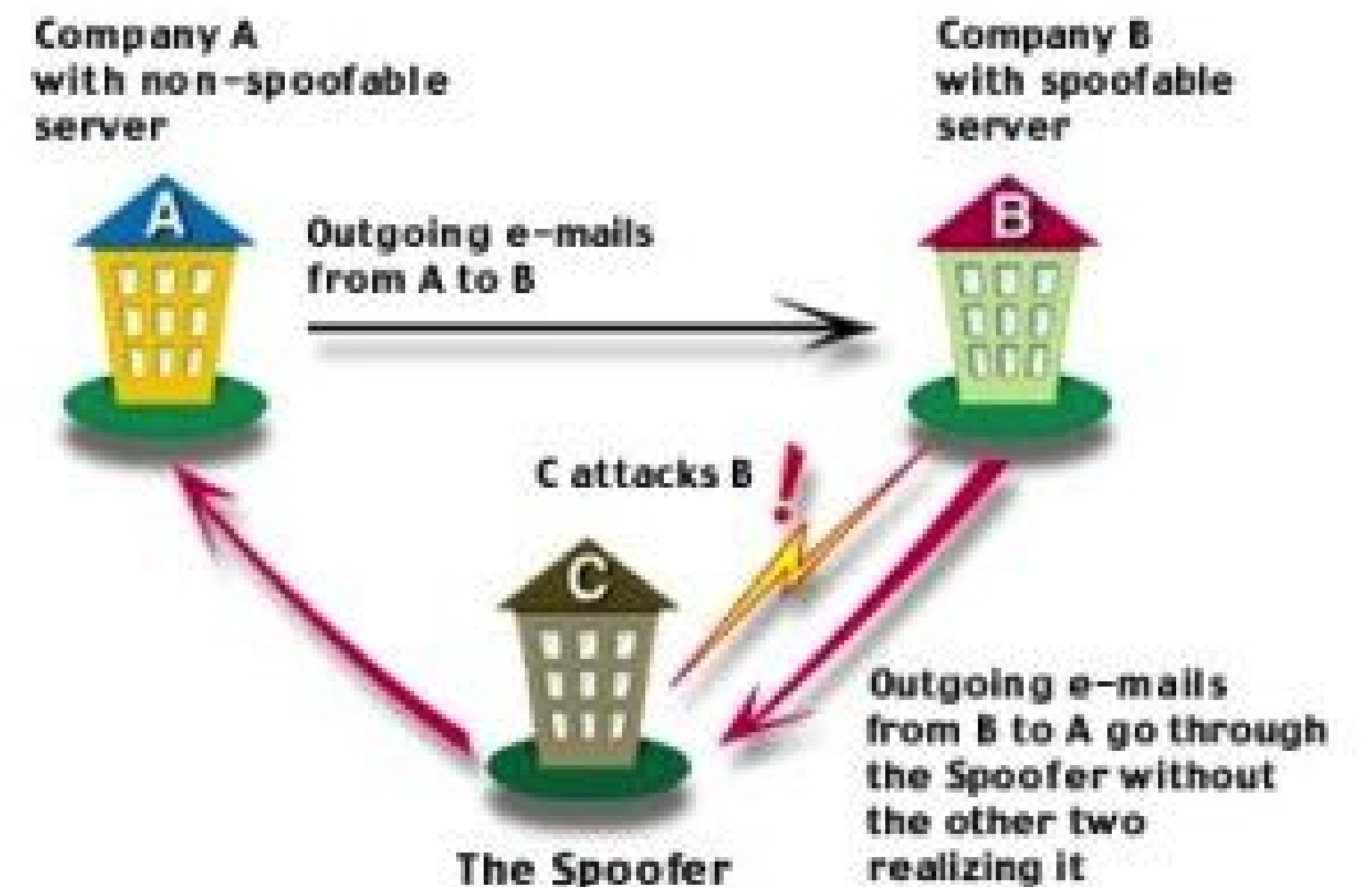


Routing with RPKI Explained



DNS Spoofing

- DNS Spoofing by cache poisoning
 - attacker flood a DNS resolver with phony information with bogus DNS results
 - by the law of large numbers, these attacks get a match and plant a bogus result into the cache
- Man-in-the-middle attacks
 - redirect to wrong Internet sites
 - email to non-authorized email server

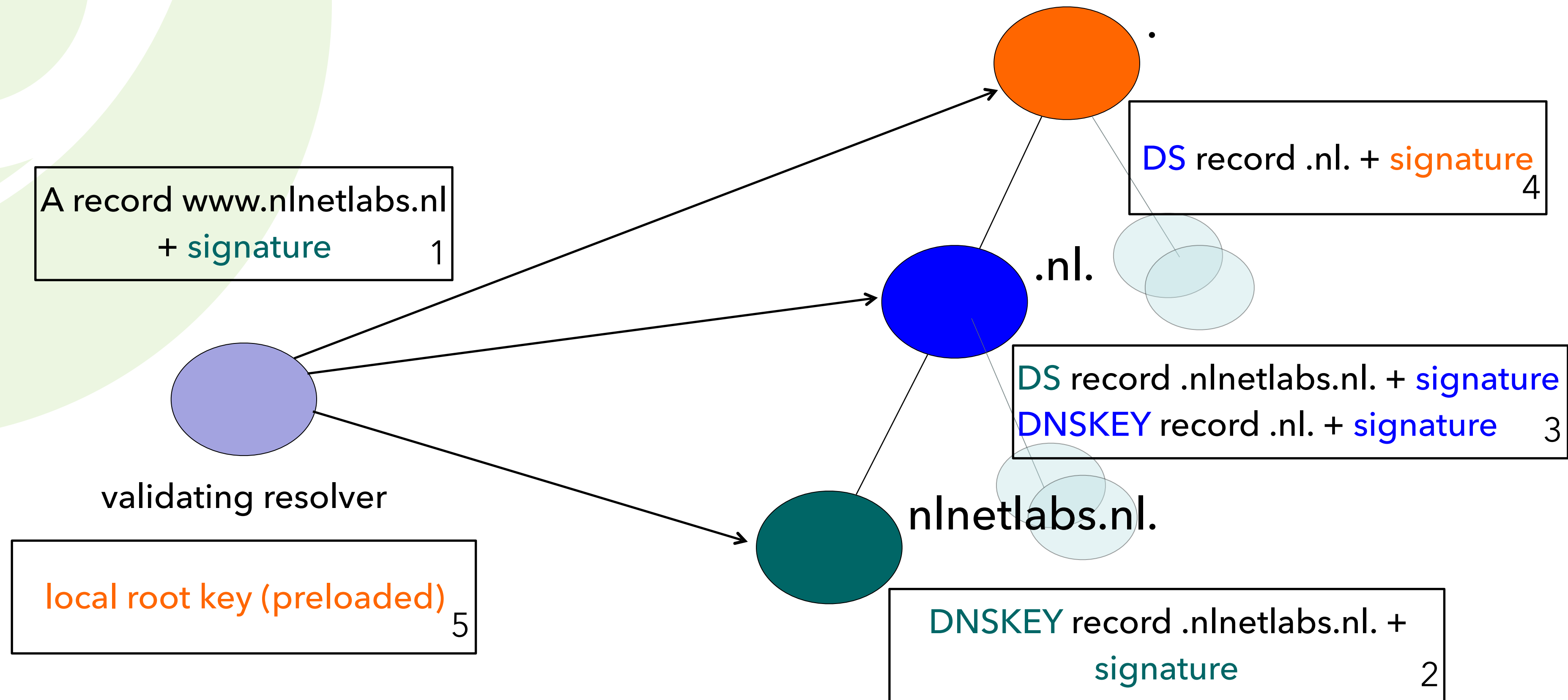


What is DNSSEC? *the one slide version*

- Digital signatures are added to responses by authoritative servers for a zone
 - Validating resolver can use signature to verify that response is not tampered with
 - Trust anchor is the key used to sign the DNS root
- Signature validation creates a chain of overlapping signatures from trust anchor to signature of response

DNSSEC and Validation

in a single picture



Sea Turtle DNS Hijack



Sea Turtle DNS Hijack

Primary targets:

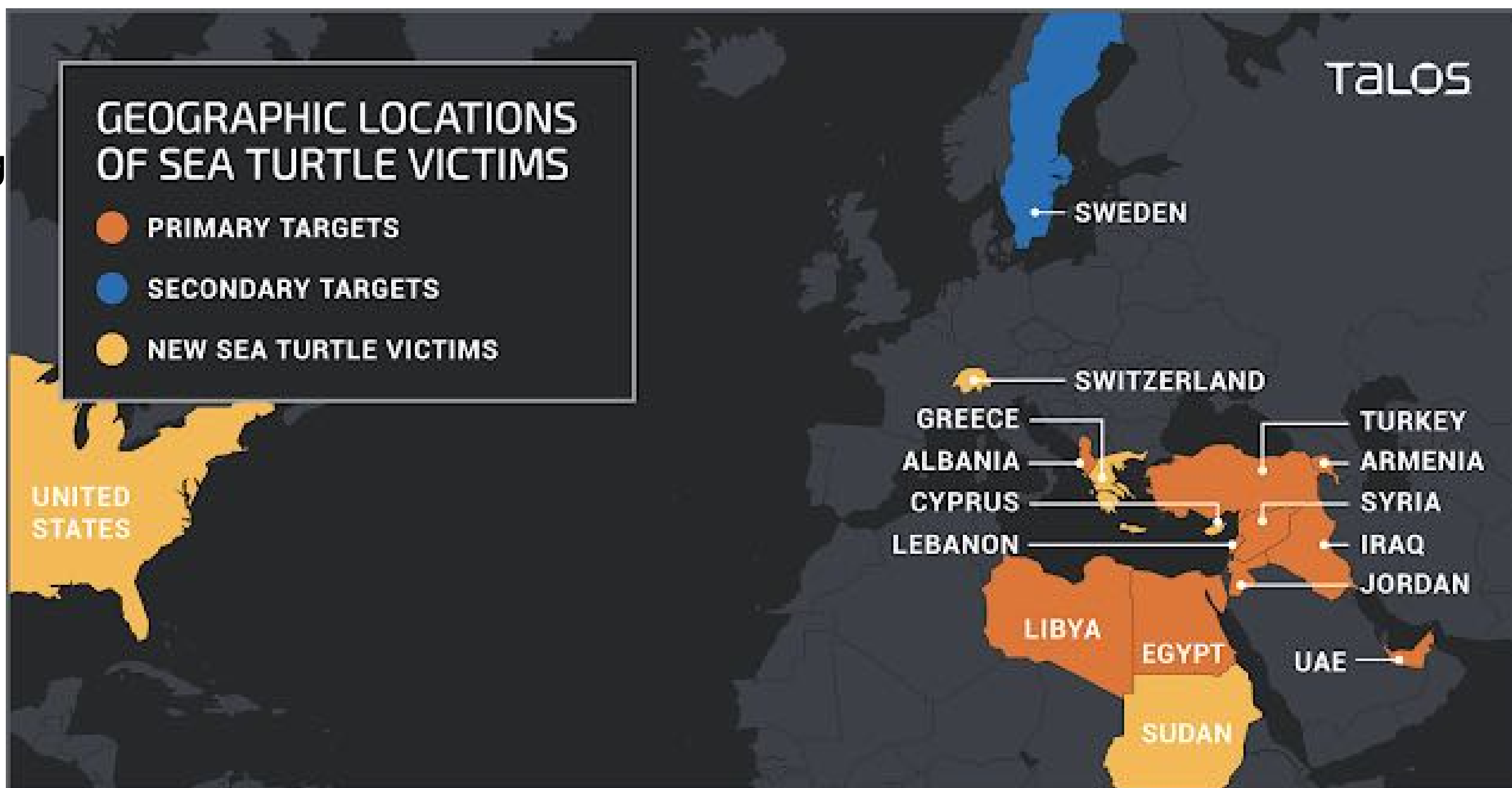
- Government organizations
- Energy companies
- Think tanks
- International non-governmental organizations
- At least one airport

Secondary targets:

- Telecom providers
- Internet service providers
- Registrars and one registry

<https://blog.talosintelligence.com/2019/04/seaturtle.html>

<https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html>



Sea Turtle DNS Hijack (2)

Structure of the attack (credits Packet Clearing House):

- So-called Registrar EPP credentials found in spoil of an attack
 - third party Registrar - Registrar Wholesaler - Registry
- NS records changed for one-hour periods Dec 13, 14, and Jan 2
- Authoritative DNS proxy gives false answers to *Certificate Authority X*
 - Other queries proxied using answers obtained from 8.8.8.8
- *Certificate Authority X* "domain validation" TLS certificate issued
- ... continue with MitM attacks: https, imaps, ...

Mitigation of Sea Turtle DNS Hijack



Defenses

Actual:

- DNSSEC signing / DNSSEC validation
- walking NS/DS delegation from the root
- registry lock (.nl Control with SIDN)

Future:

- CERT pinning/DANE authentication
- authenticate recursive resolver/MDM lock recursive resolver

Collaborative Security



DDoS Attacks

- Routing hygiene and BGP filtering!
 - BCP 38/BCP 84 egress filtering to counter spoofing
 - MANRS Program, Andrei Robachevsky
 - Yet Another talk about BGP filtering, Markus Weber
- Are incentives aligned?
 - operational costs vs. payback of investment

Dutch Anti-DDoS Initiative

- Public-private collaboration in The Netherlands
 - partners are ISPs, IXPs, banks, government agencies, .nl registry and a not-for-profit DDoS scrubbing centre
- Objectives
 - actively exchange expertise on DDoS attacks across operators and sectors
 - develop and operate a "DDoS clearing house" that enables service providers to proactively handle DDoS attacks

DDOS CLEARING HOUSE





NETWORK MEASUREMENT

(PCAP, NET FLOW, IPFIX, SFLOW, LOGS, ...)

DDOS_DISSECTOR



INPUT: NETWORK MEASUREMENT

OUTPUT: DDOS FINGERPRINT (+*NOTES)

FILTERED & ANONYMIZED NETWORK MEASUREMENTS

DDOS_FINGERPRINT_CONVERTERS



INPUT: DDOS FINGERPRINT

OUTPUT: RULE/SIGNATURE FOR SPECIFIC HW/SW SOLUTION(S)
(SNORT, SURICATA, BRO, IPTABLES, EBPF, BGP FLOWSPEC, ...)



DDOSDB

STORE, ENRICH, AND DISTRIBUTE DDOS ATTACK RELATED INFO

VICTIMS

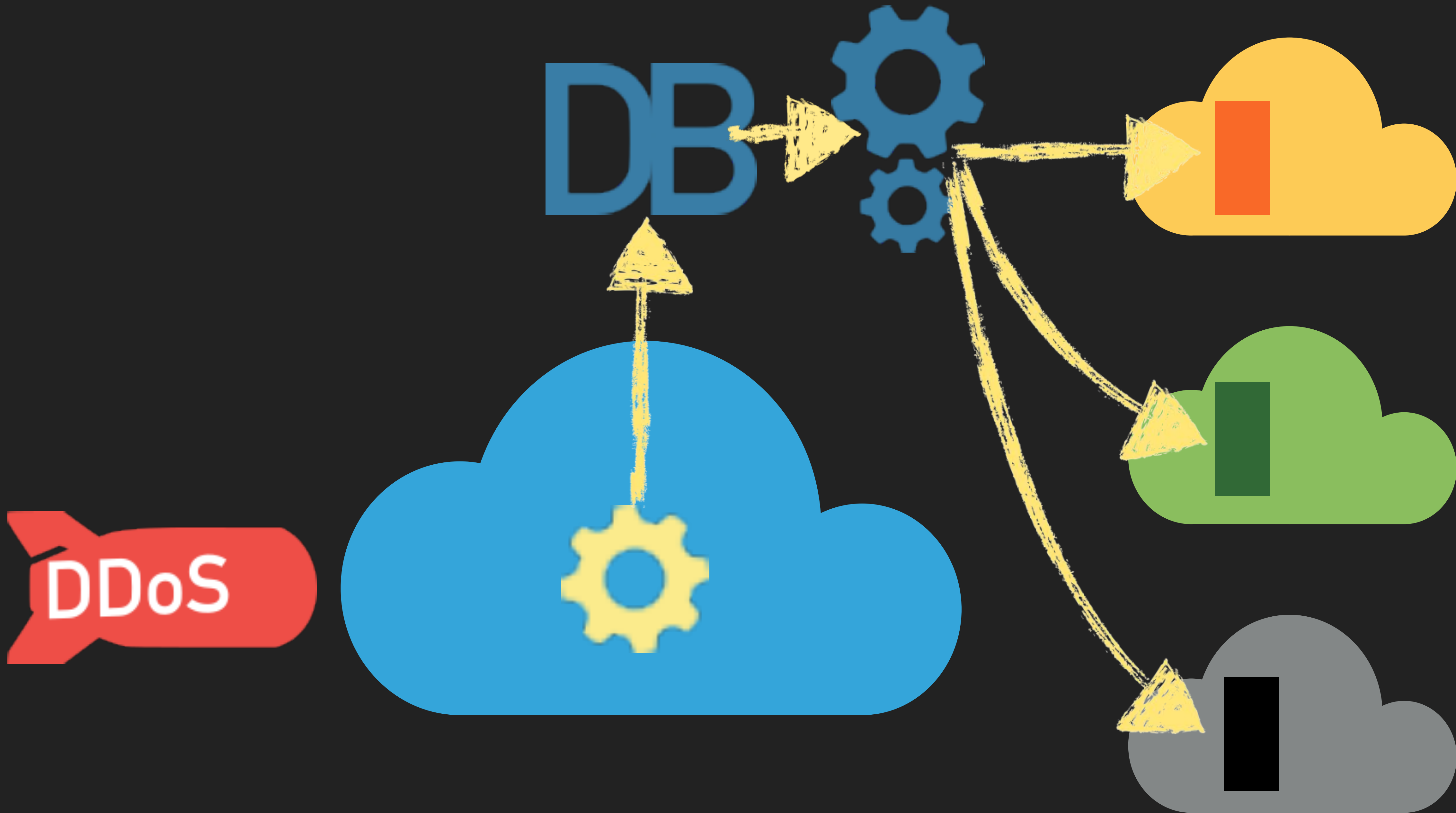
**DDOS
PROTECTION
PROVIDERS**

**NETWORK
OPERATORS
+
CERT/CSIRT**

**LAW
ENFORCEMENT
AGENCIES**

ACADEMIA

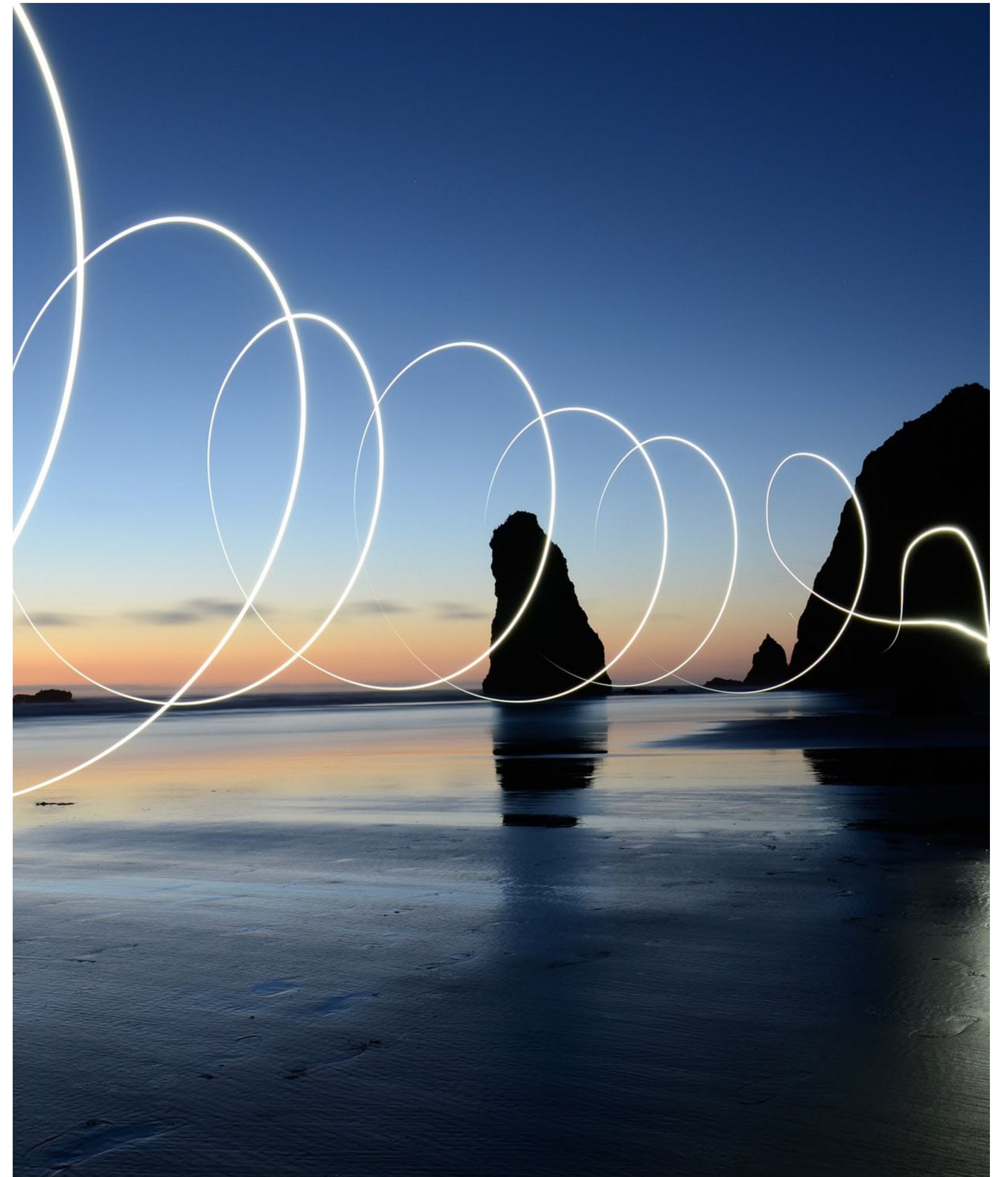




More on the Anti-DDoS Initiative

- One Conference 2019, The Hague
 - Session on Day 2, 2 October 2019:
“Fighting DDoS attacks together on a national scale”
 - Technical presentation
 - Panel discussion

Wrapping-up



Security on Multiple Layers



DNSSEC ✓
TLS ✓
BGP filtering / RPKI ✓

Message to Take Away

- Security requires an integral approach:
 - not BGP filtering, RPKI or DNS security, but **all** of them
- Security requires a collaborative approach, e.g.:
 - MANRS initiative
 - DDoS Clearing House
- Security requires transparency
 - open source & open standards

