Internet Infrastructure Security

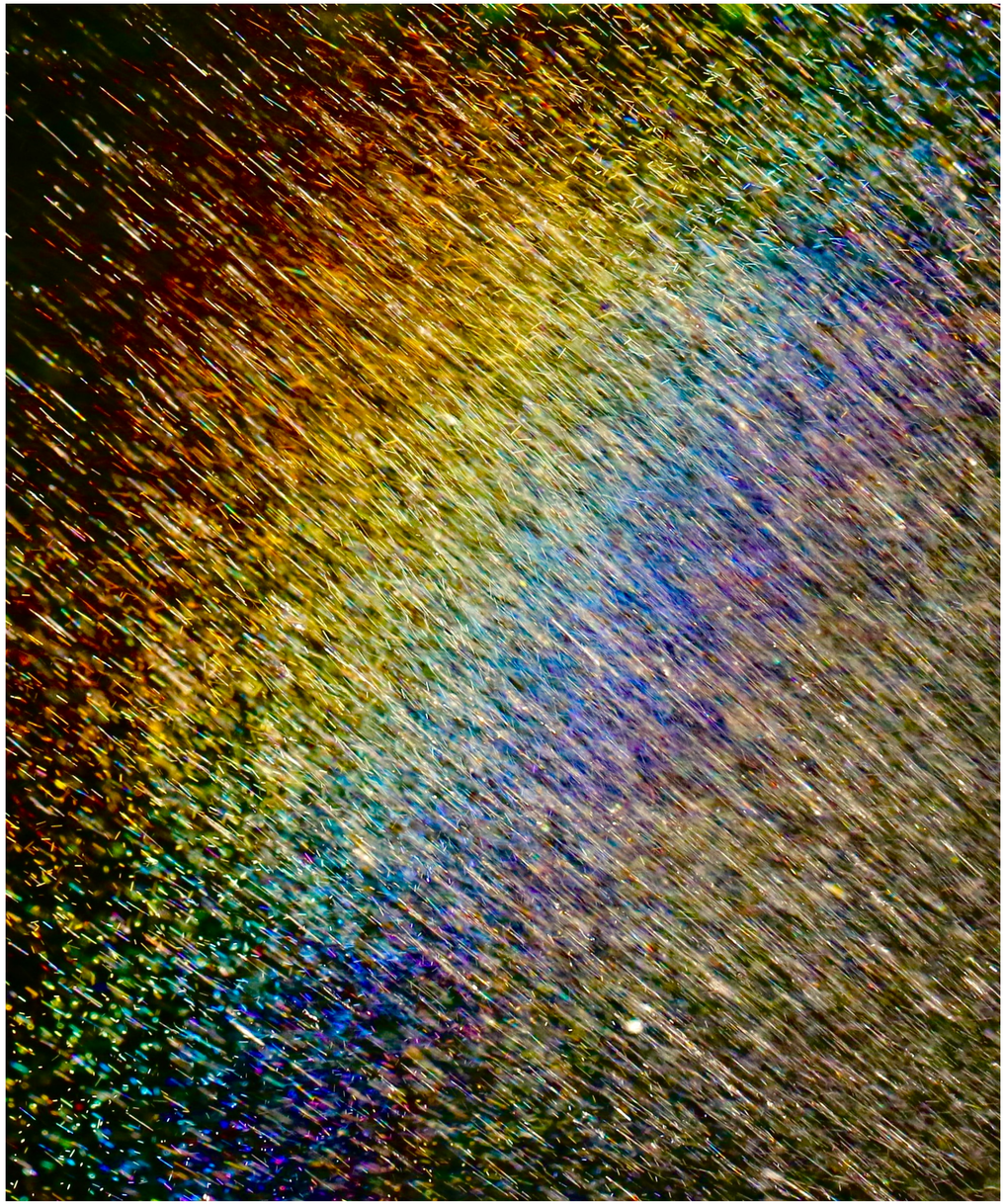
Benno Overeinder
NLnet Labs

NLNETLABS

The security spectrum

What's in …

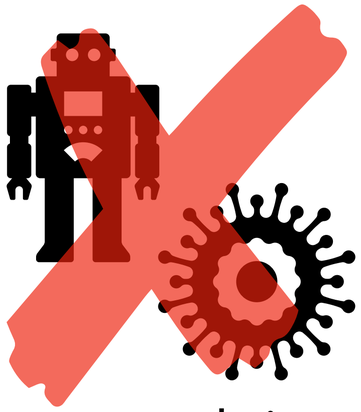
and what's out



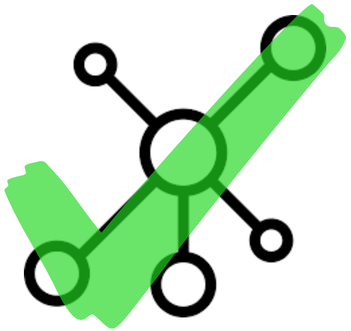
The Security Spectrum

popular CCTV shop name

social engineering



botnets and viruses



internet infrastructure

The Internet Infrastructure Security Spectrum

Infrastructure Security Today at NID'19

- Yet Another talk about BGP filtering
  Markus Weber

- DNS Security
  Bert Hubert

- Update MANRS Program
  Andrei Robachevsky

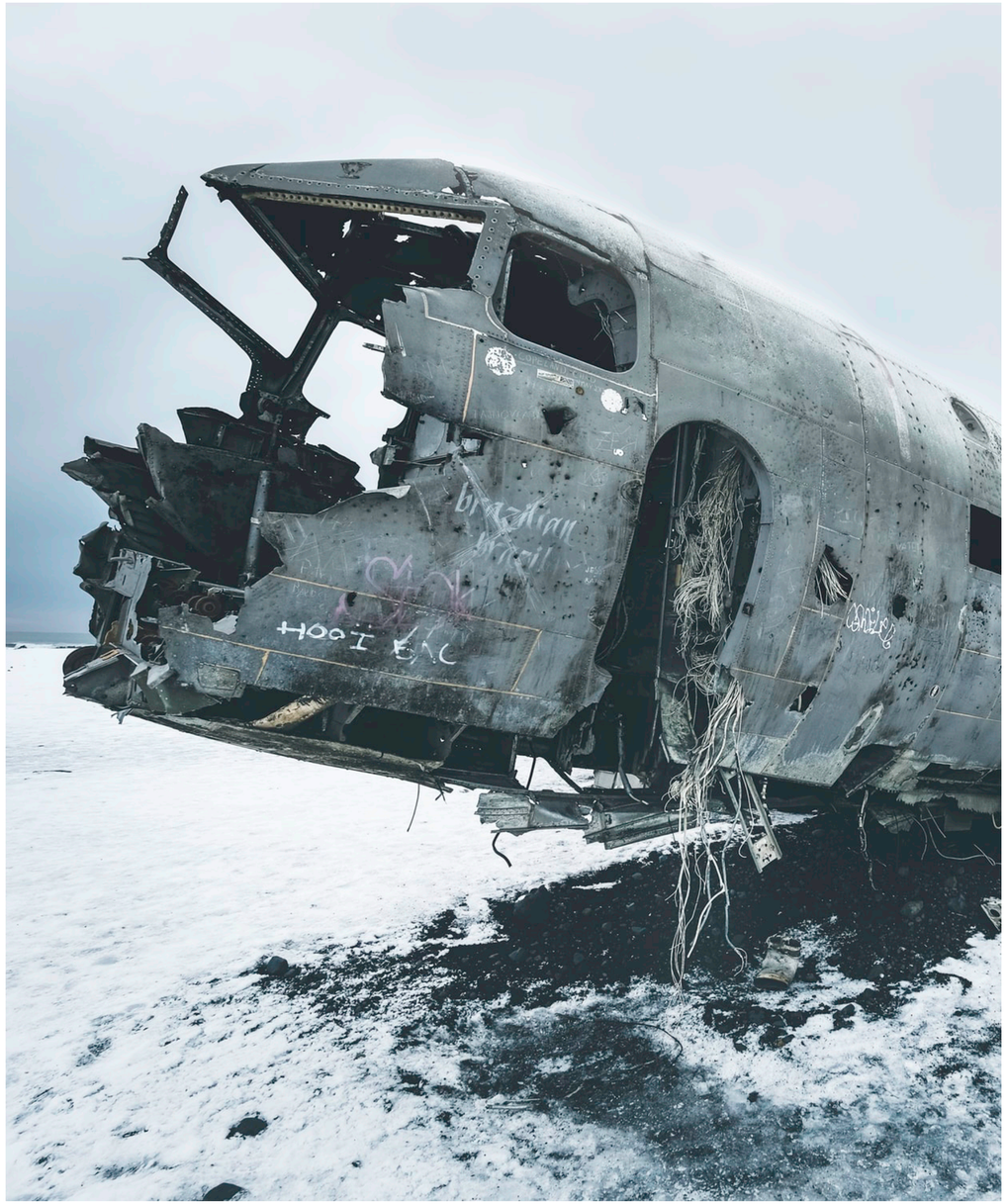
- Managing ROAs and doing Origin Validation. Why?
  Riccardo Stagni

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



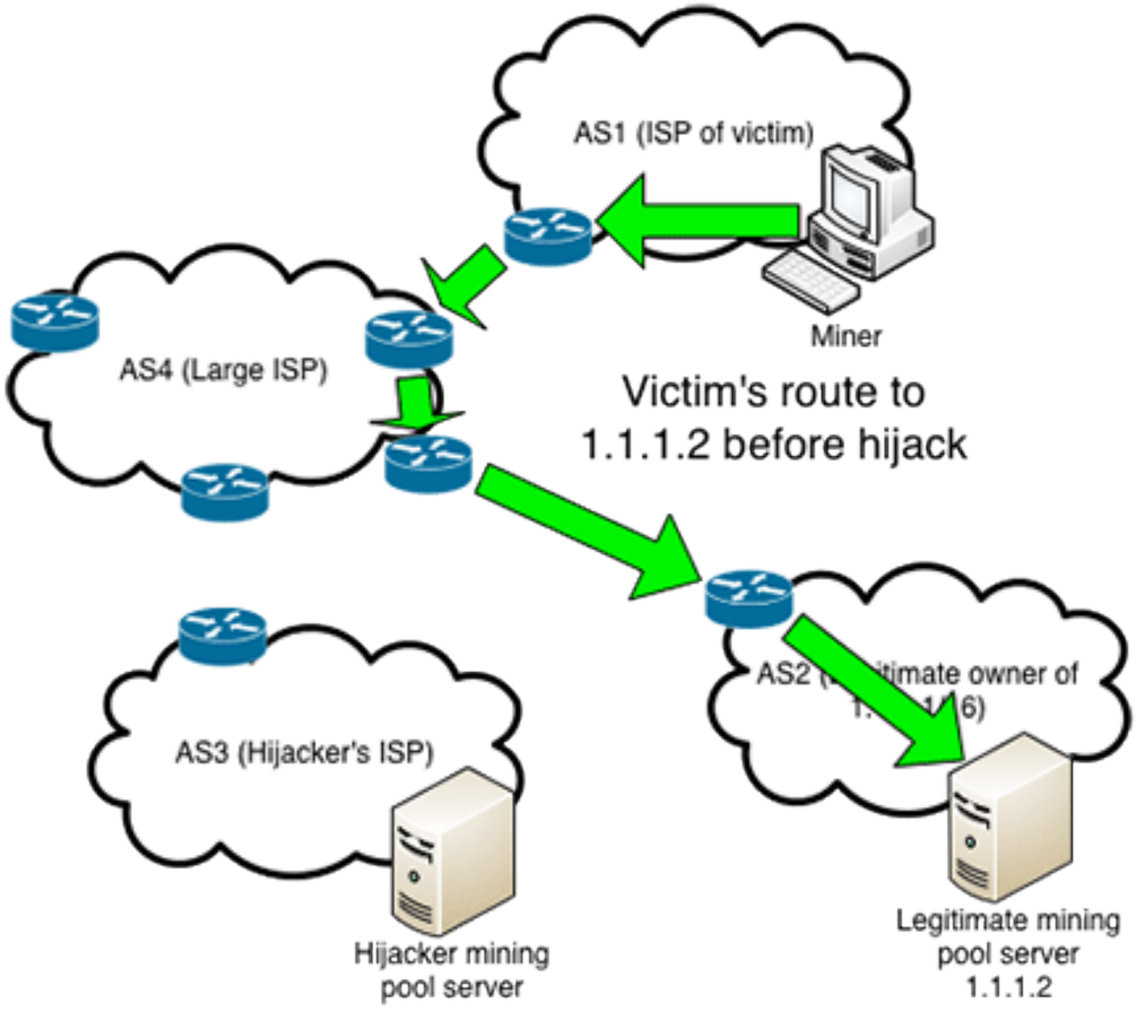
AWS Route 53 Hijack

Amazon Route 53 Hijack

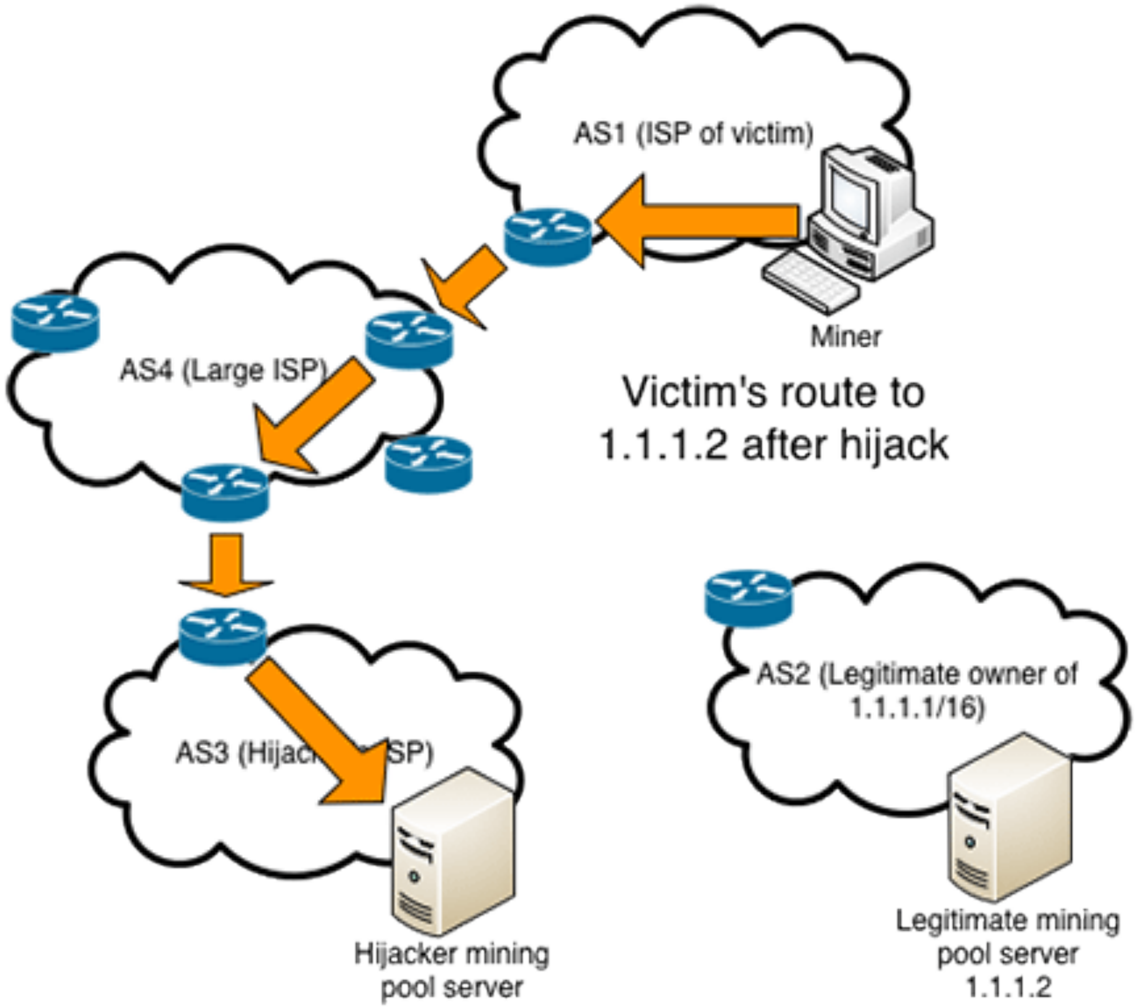
This is not about cryptocurrencies & blockchain!

- 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



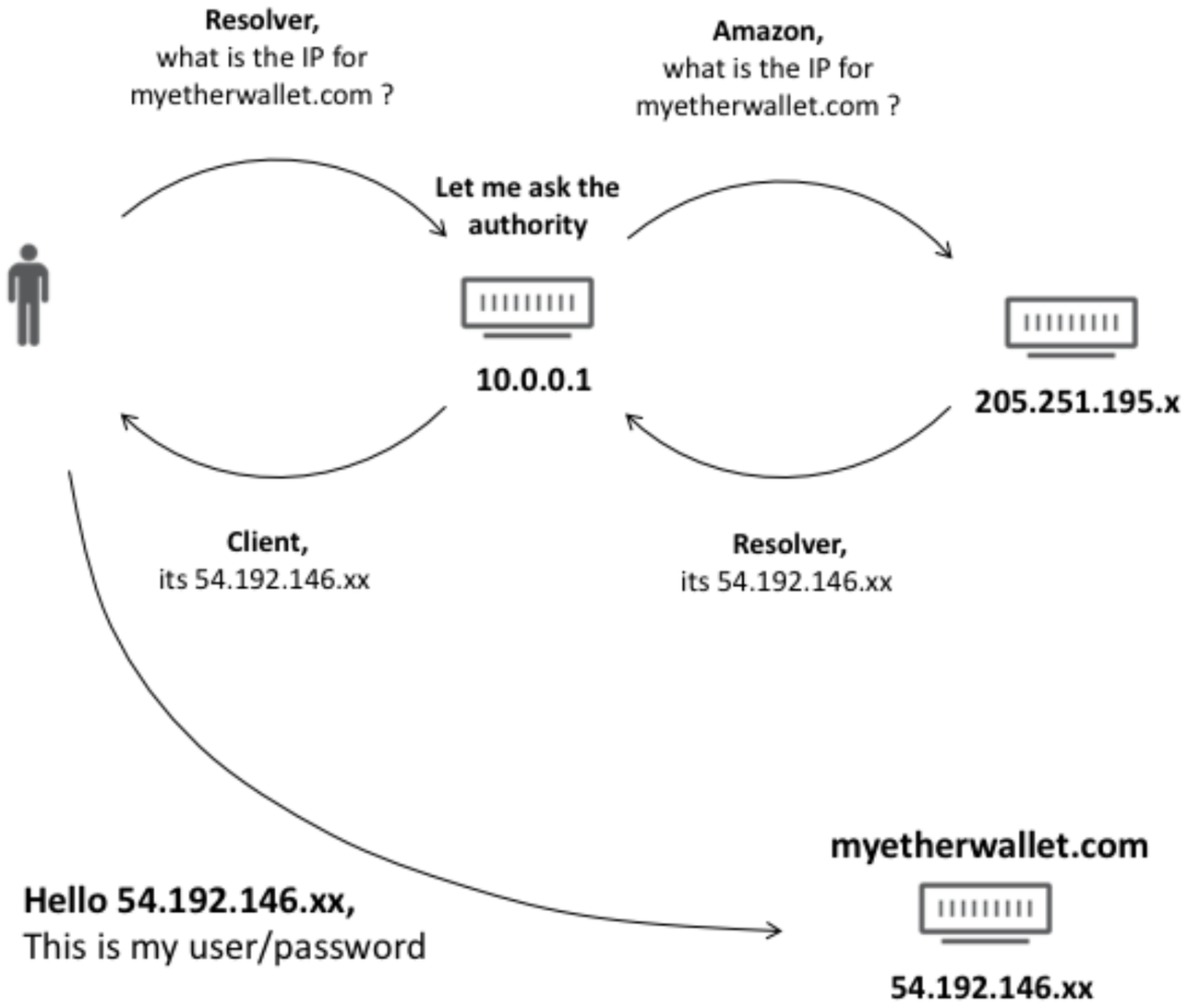
Status: A Route Hijack



Two-stage Attack: DNS Spoofing

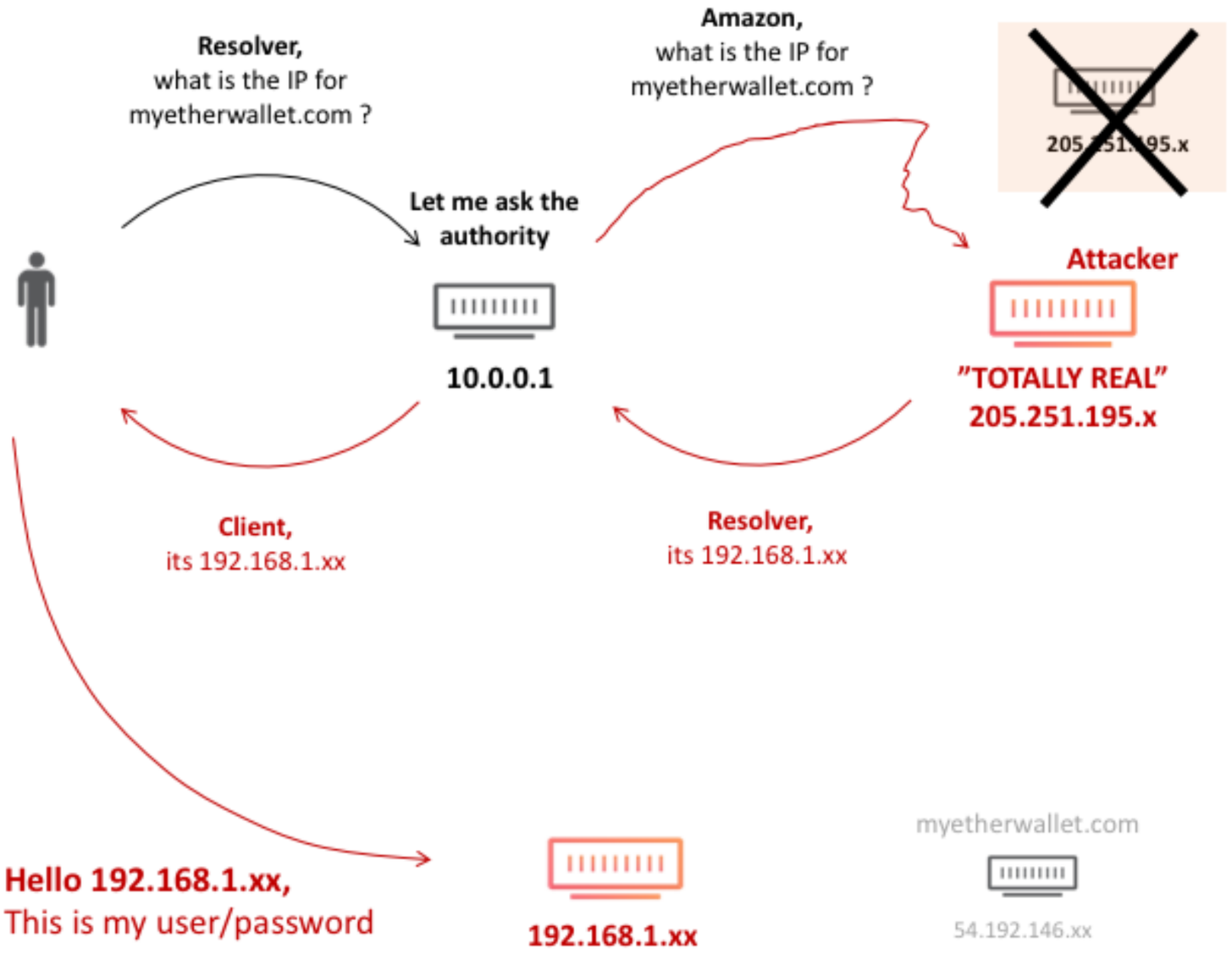
- Intention of Amazon Route 53 hijack: DNS spoofing
- False DNS information
  - cryptocurrency digital wallet: myetherwallet.com
  - not legitimate answer to myetherwallet.com, but the IP address of the attacker

All OK: Amazon Route 53 DNS



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

Route Hijack: Amazon Route 53 DNS



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

Mitigation of Amazon Route 53 Hijack

Sea Turtle DNS Hijack

Sea Turtle DNS Hijack

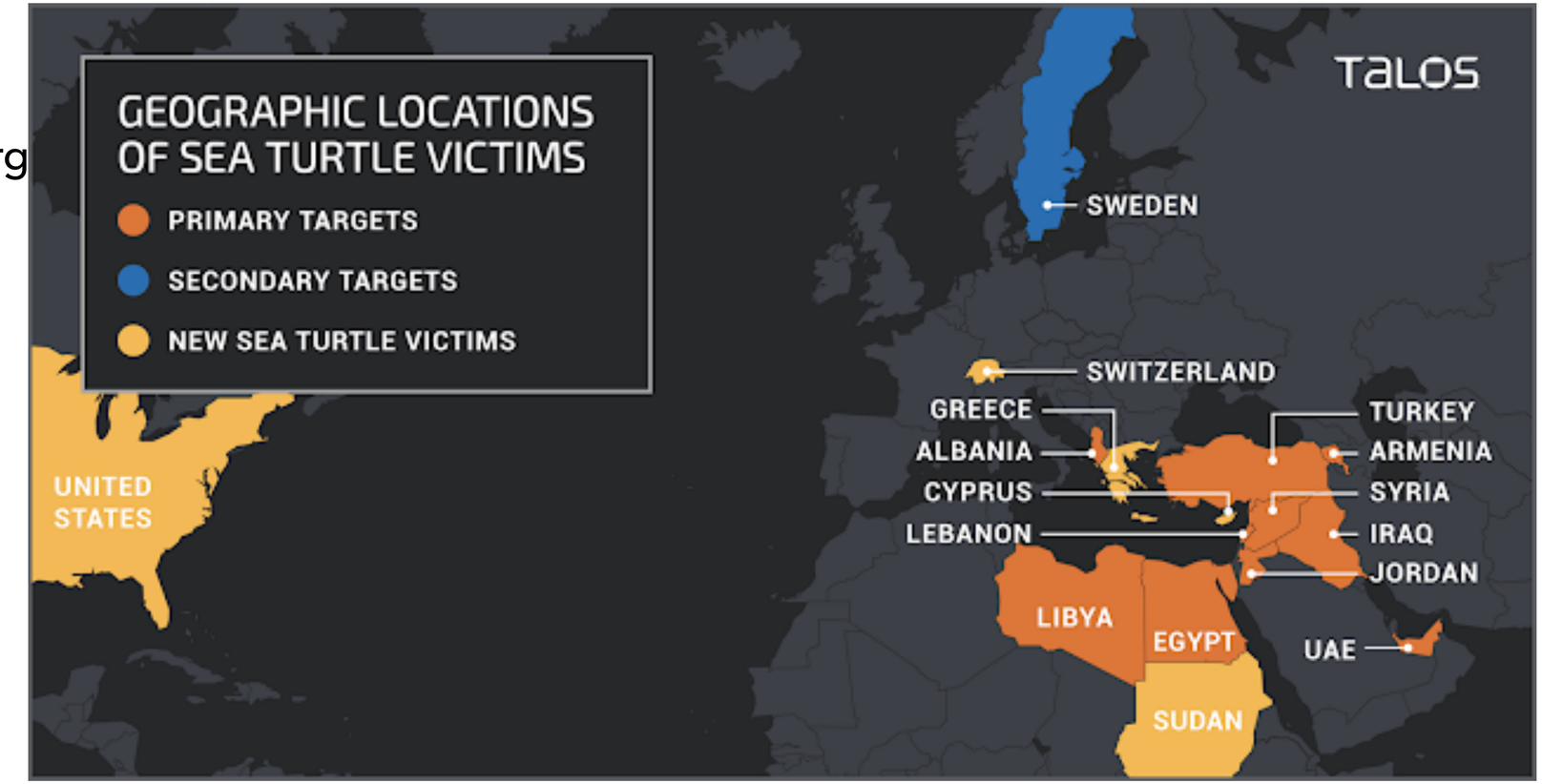
Primary targets:

- Government organizations
- Energy companies
- Think tanks
- International non-governmental org
- 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, …

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

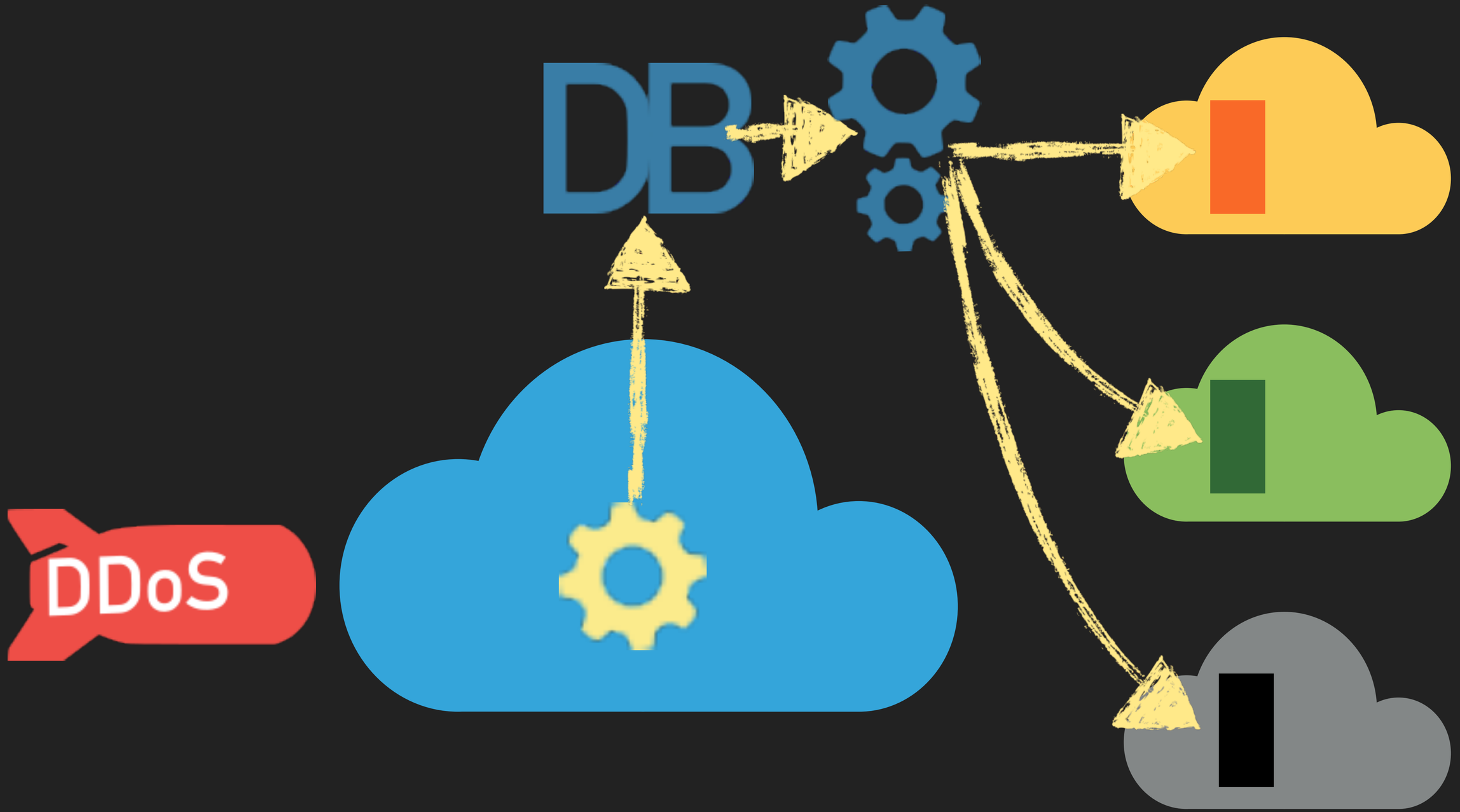
VICTIMS

DDOS PROTECTION PROVIDERS

NETWORK OPERATORS + CERT/CSIRT

LAW ENFORCEMENT AGENCIES

ACADEMIA


DB
DDoS

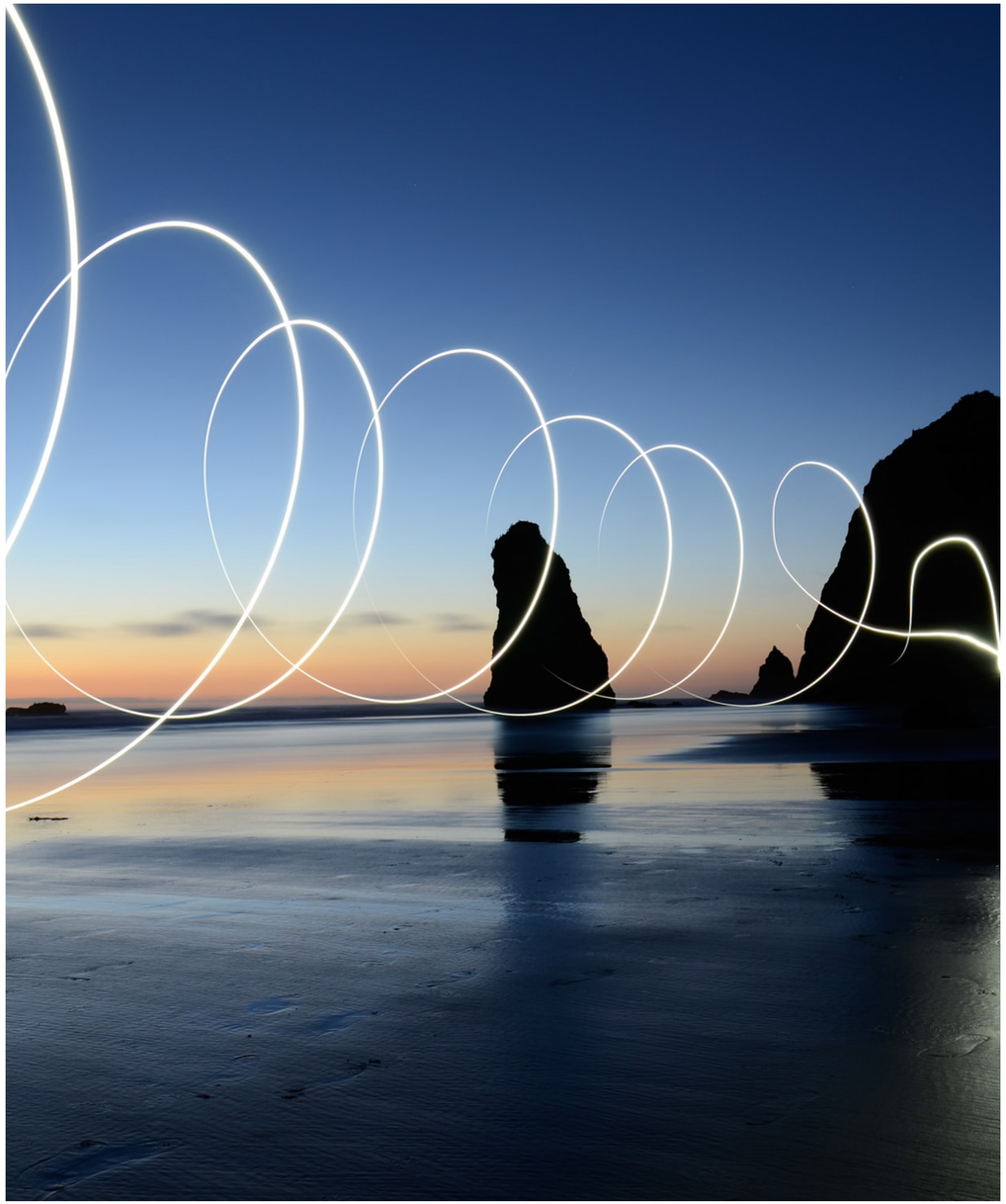
More on the Anti-DDoS Initiative

- One Conference 2019, The Hague
  - Session on Day 2, 2 October 2019:

    “Fighting DDoS attacks together on a national scale”

  - Techical 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