The Stability of the Internet: Identifying and Mitigating Risks

Benno Overeinder
NLnet Labs

Kivi lezing, 21 November 2018

NLNETLABS

The Pivotal Question in the Study

- Internet is a constantly evolving socio-technical system to facilitate new forms of interaction
  - the technical fundaments change with it, this is only a snapshot
- Many things can go badly wrong, but
  - “What threatens National Security and how bad is it?”

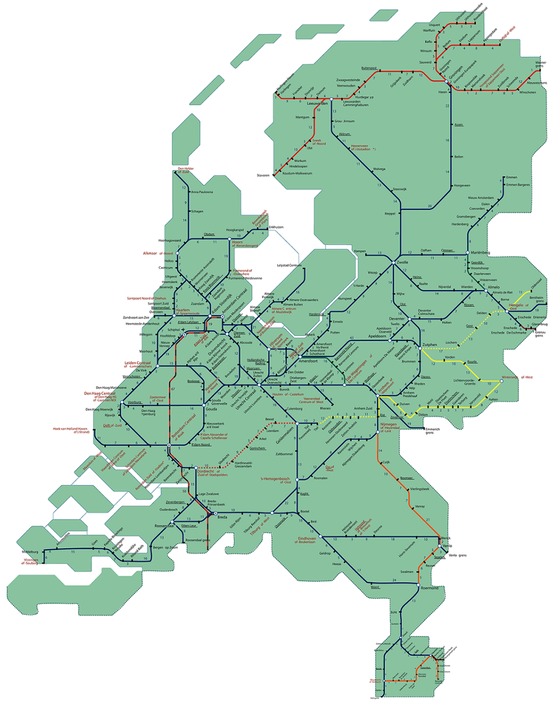
Some Context of the Study

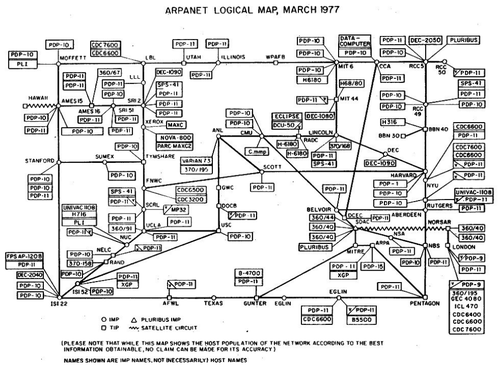
- Study by TNO in collaboration with NLnet Labs
  - TNO: expertise covering all aspects of study
  - NLnet Labs: technical expertise in stocktaking & analysis of risks
  - interview of 20+ national and international Internet experts
- Caveat
  - TNO and NLnet Labs executed this study on our own behalf
  - no endorsement by governmental departments in any way

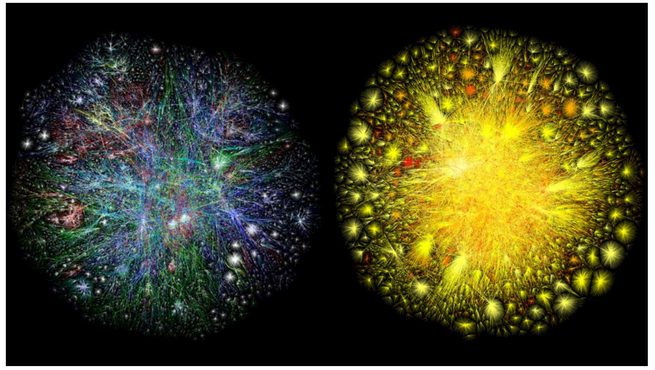
About the Internet

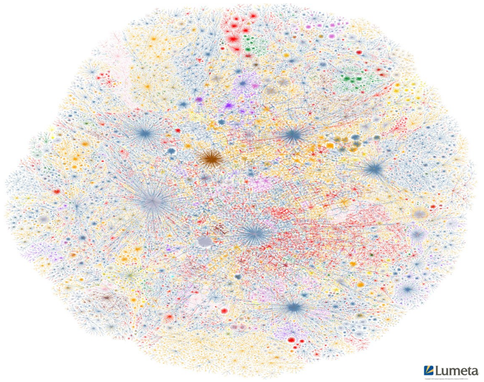
- The Internet ‘invariants’ (Internet Society, 2012)
  - global reach, integrity
  - general purpose
  - supporting innovation without requiring permission
  - accessible
  - interoperability and mutual agreement
  - collaboration
  - reusable (technology) building blocks
  - no permanent favourites
- Additional properties of the Internet infrastructure
  - no central control or coordination
  - no global network policies
  - high degree of redundancy

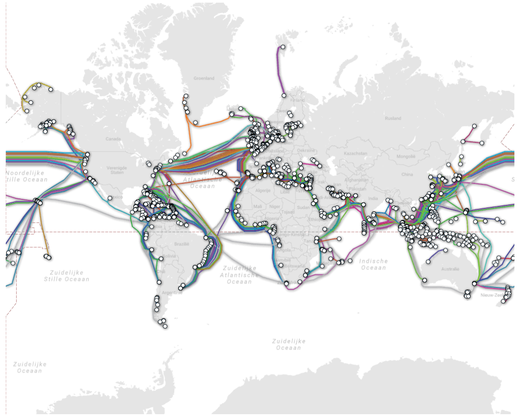
An Analogy











Spoorwegnet NL

Internet

An Analogy (2)

- Spoorwegnet NL
  - clear number of nodes and connections
  - centrally designed and controlled
  - the timetable for all traffic is fixed and trains follow fixed routes
  - detour is impossible or takes time (change timetable, limit speed)
- Routing over the Internet
  - large number of nodes and connections (limited overview)
  - grown organically
  - routes are not fixed but are determined via routing
  - ‘detour’ is possible from almost every hub and costs almost no time (in general not noticeable for most users)

An Analogy (3)

Bomb-on-a-Hub Scenario

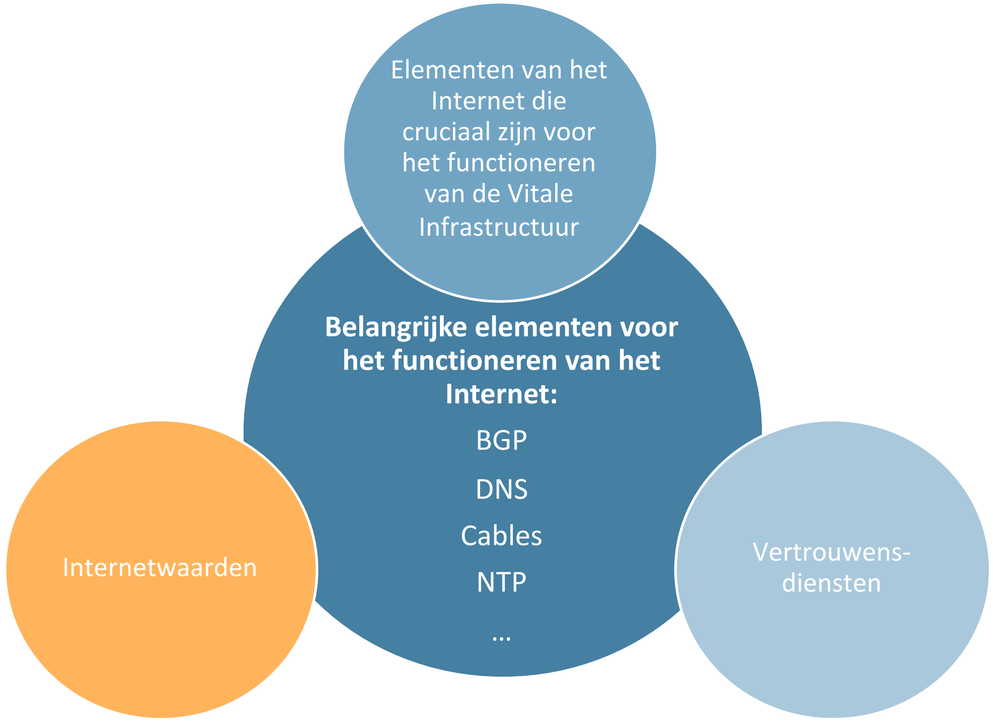
- Drop-out Utrecht Centraal Station
  - local train traffic falls out
  - many national train traffic is disrupted by central location Utrecht CS
  - ‘diversion’ is not possible – must first be planned for the entire network
- Central hub?
- Large Internet Exchange failure
  - ‘local’ Internet traffic disrupted (private peering and peering via other Exchanges continues to work)
  - with routing, ‘regional’ traffic dynamically finds new ways and a new optimum
  - global Internet traffic experiences no or very short disruption

Internet – Critical Infrastructure – National Security

- The Internet is fundamentally different from most other Critical Infrastructures
  - The perspective of a ‘fundament’ or ‘core’ fits well on relatively homogeneous, hierarchical systems such as a railway, drinking water or electricity network but is of limited value on the Internet consisting of a patchwork of local configurations
  - What constitutes a threat to the National Security from a decentralized, self-organizing system that is slightly different everywhere?

Perspectives on the Fundament

- What is a ‘foundation’ depends on how you look at the Internet
  - the Internet as a technical infrastructure
  - the Internet as a collection of Internet applications/Internet services (including trust services)
  - the Internet as a collection of values: the ‘Internet invariants’



Important Elements for the Functioning of the Internet

- Border Gateway Protocol (BGP) – especially routing tables
- Domain Name System (DNS) – in particular root servers and DNS providers
- Network Time (NT) – in particular the Network Time Protocol (NTP)
- Components of the physical Internet infrastructure
  - cables (fiber optics)
  - major Internet Exchanges
  - large data centers

Building Blocks of the Internet: BGP & DNS

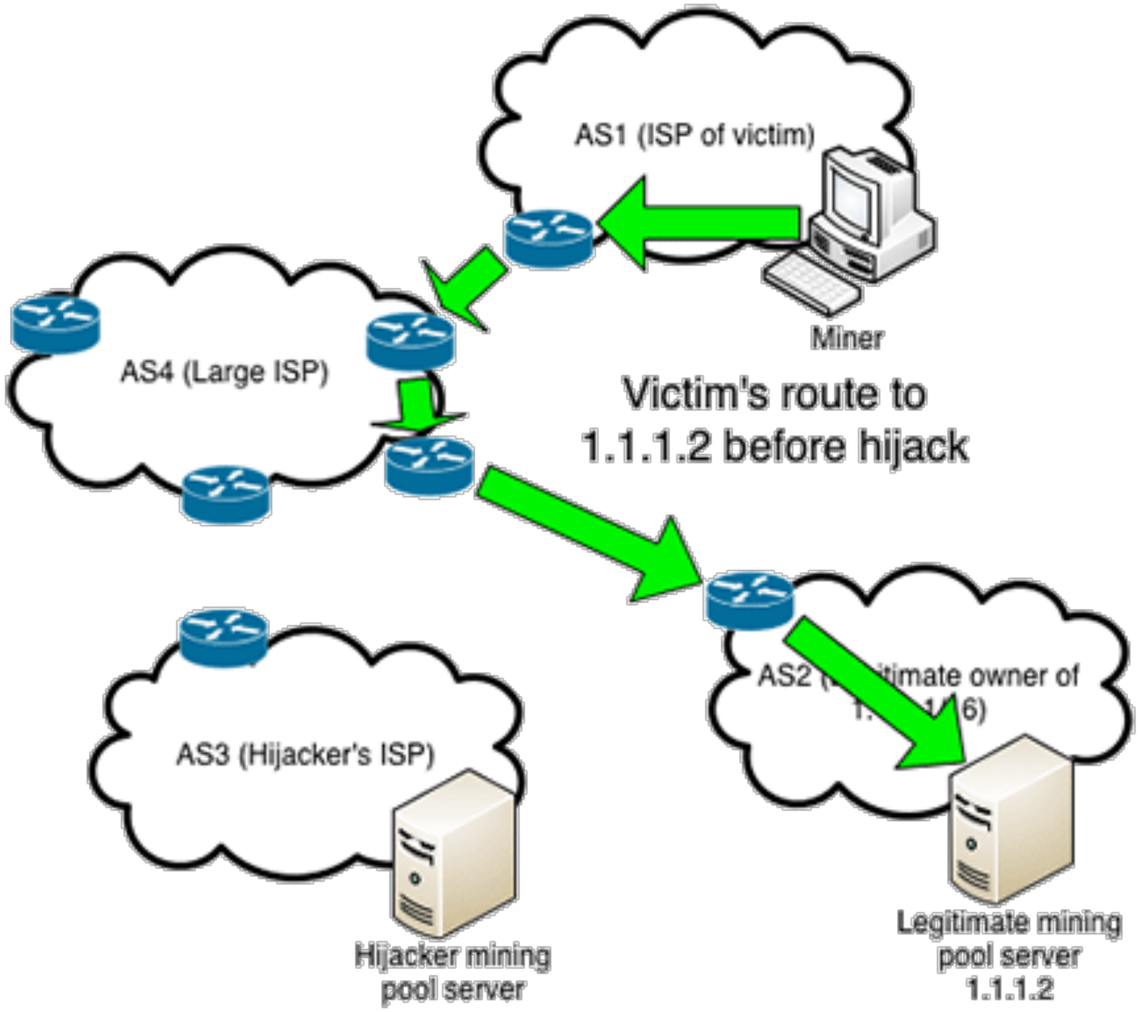
Risks and Mitigation

Amazon Route 53 Hijack

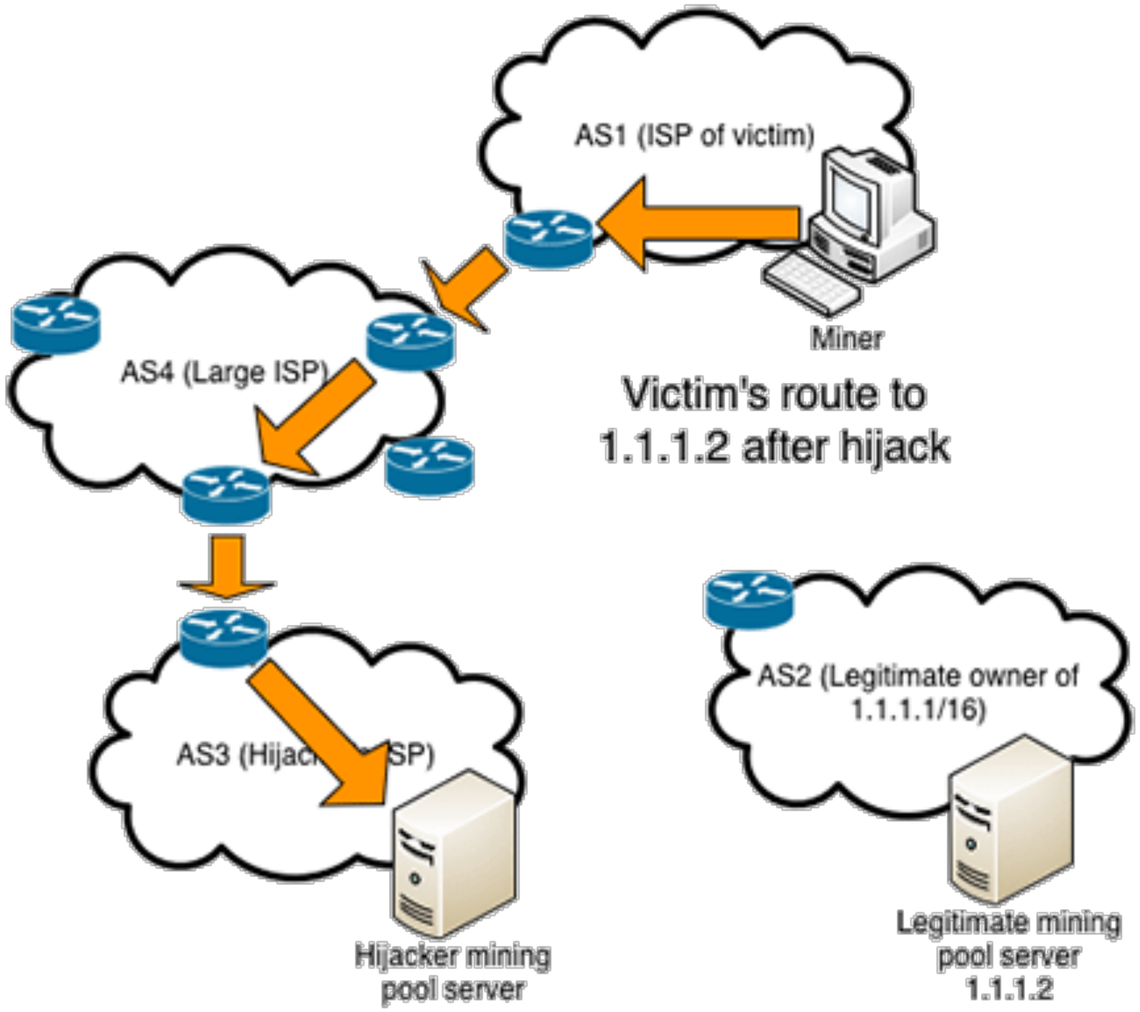
This is not about cryptocurrencies & blockchain!

- 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



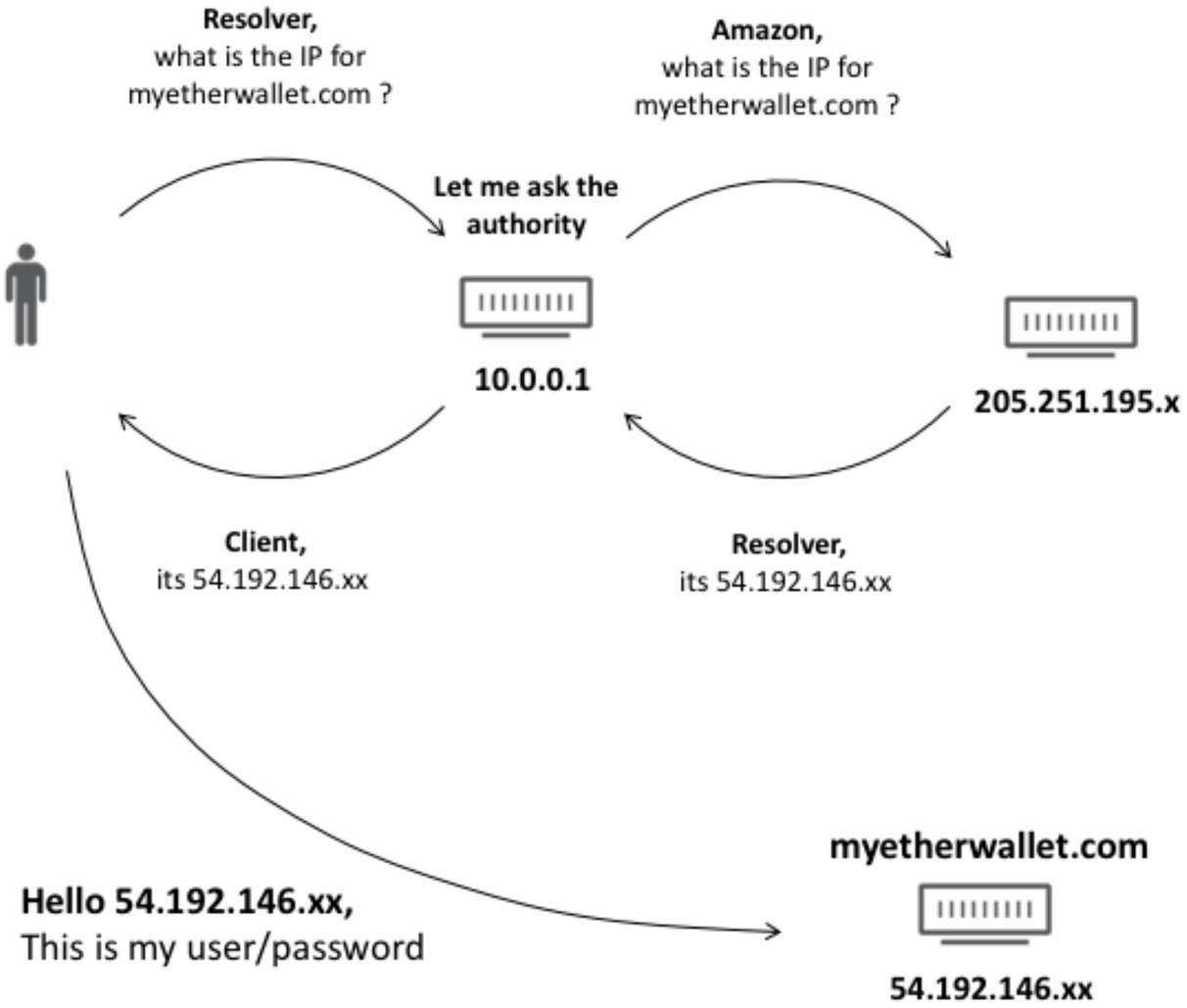
Status: A Route Hijack



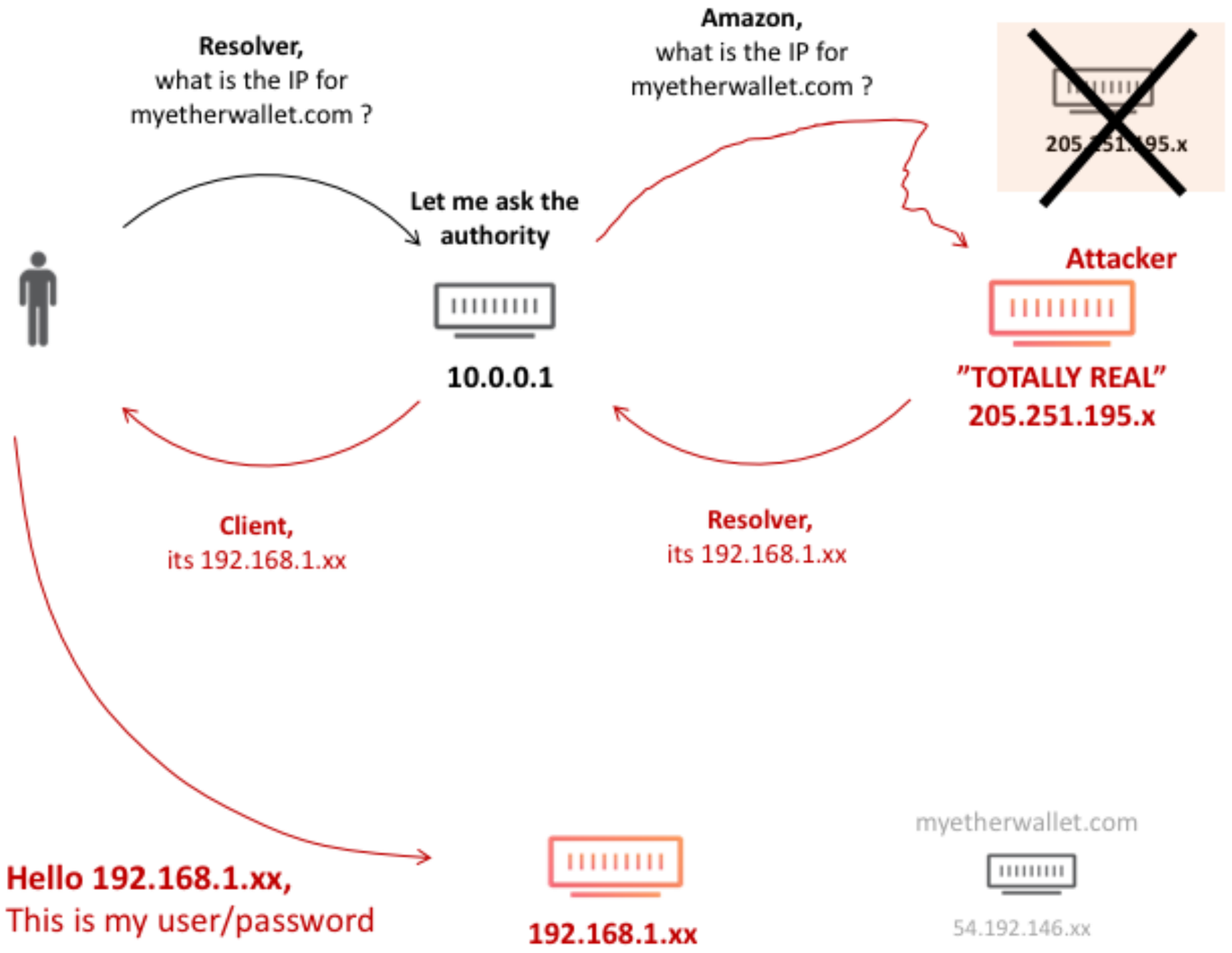
Two-stage Attack: DNS Spoofing

- 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



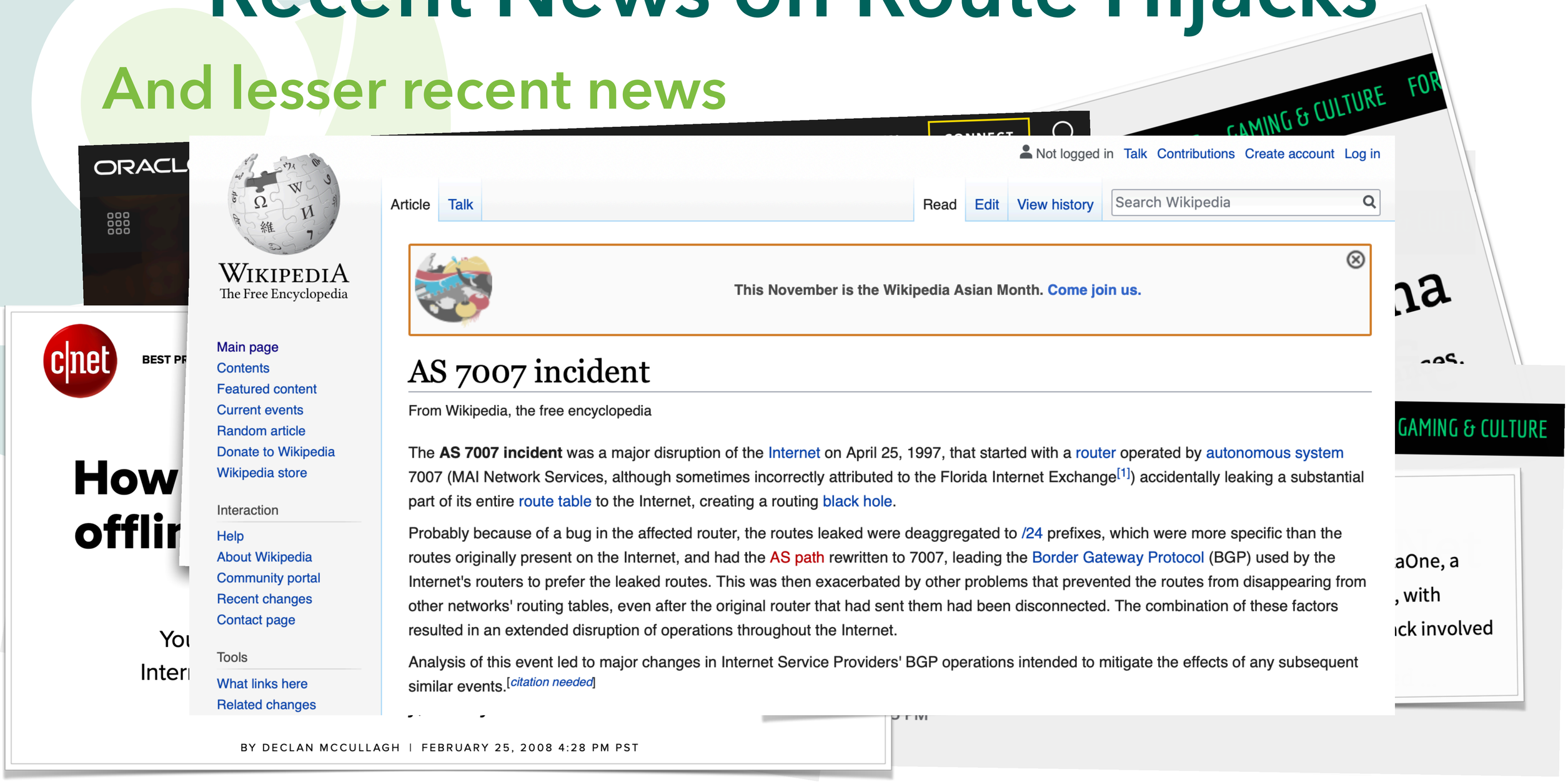
Route Hijack: Amazon Route 53 DNS



Mitigation of Amazon Route 53 Hijack

Recent News on Route Hijacks

And lesser recent news



Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

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

This November is the Wikipedia Asian Month. Come join us.

AS 7007 incident

From Wikipedia, the free encyclopedia

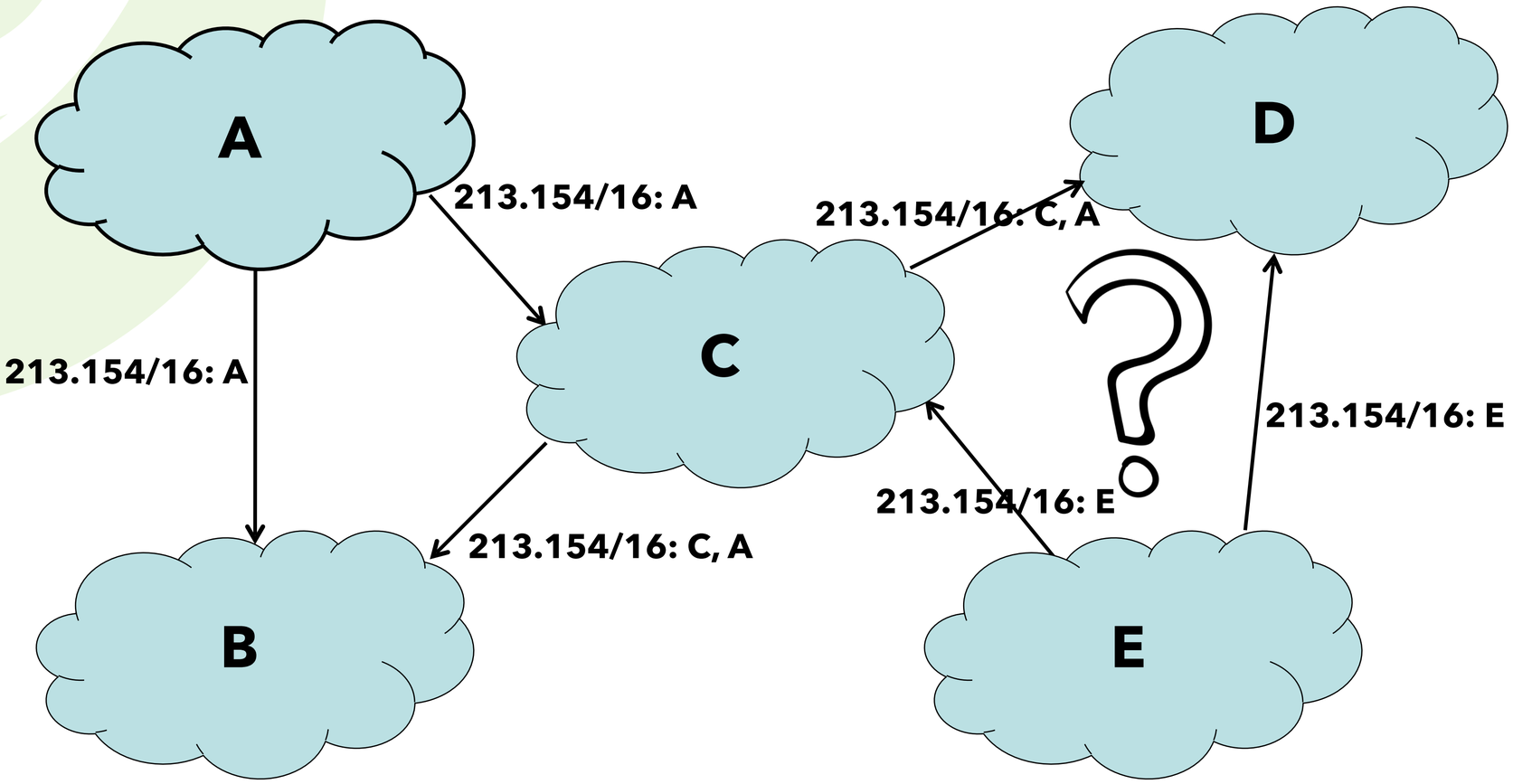
The **AS 7007 incident** was a major disruption of the Internet on April 25, 1997, that started with a router operated by autonomous system 7007 (MAI Network Services, although sometimes incorrectly attributed to the Florida Internet Exchange[1]) accidentally leaking a substantial part of its entire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

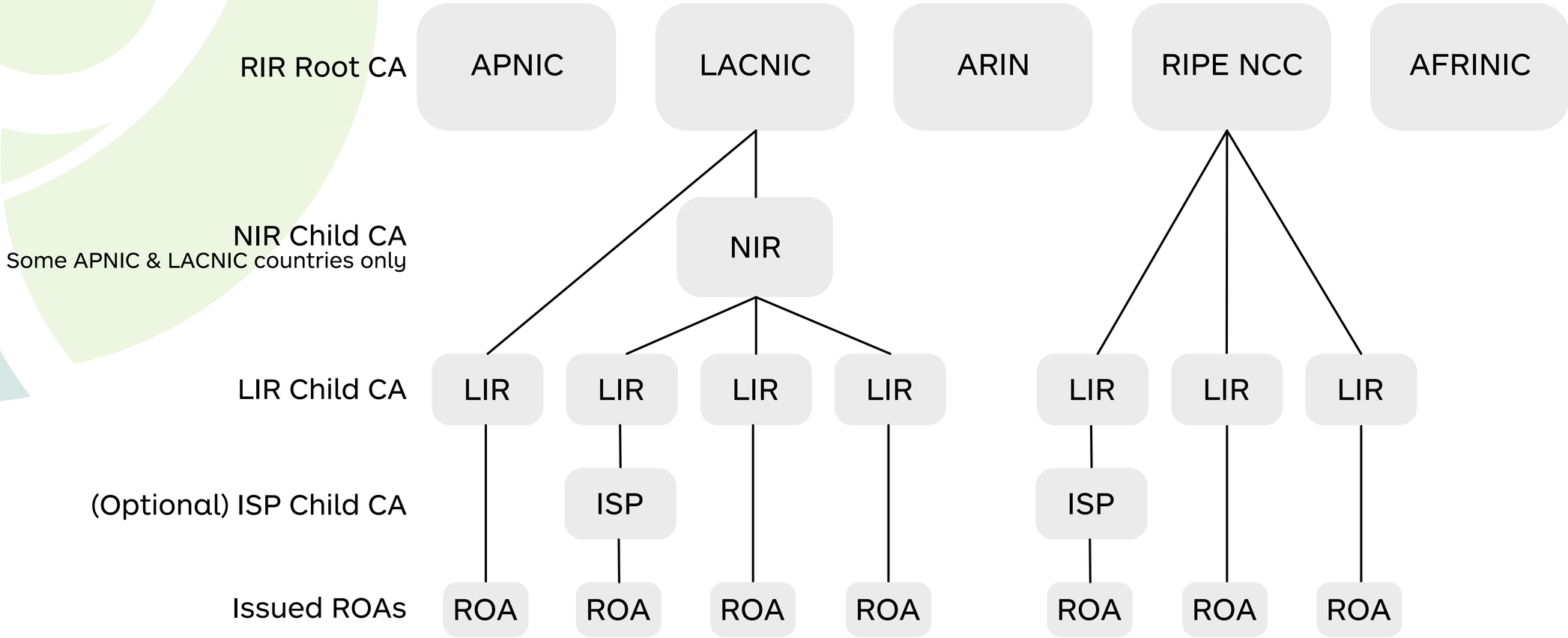
Analysis of this event led to major changes in Internet Service Providers' BGP operations intended to mitigate the effects of any subsequent similar events.[*citation needed*]

BY DECLAN MCCULLAGH | FEBRUARY 25, 2008 4:28 PM PST

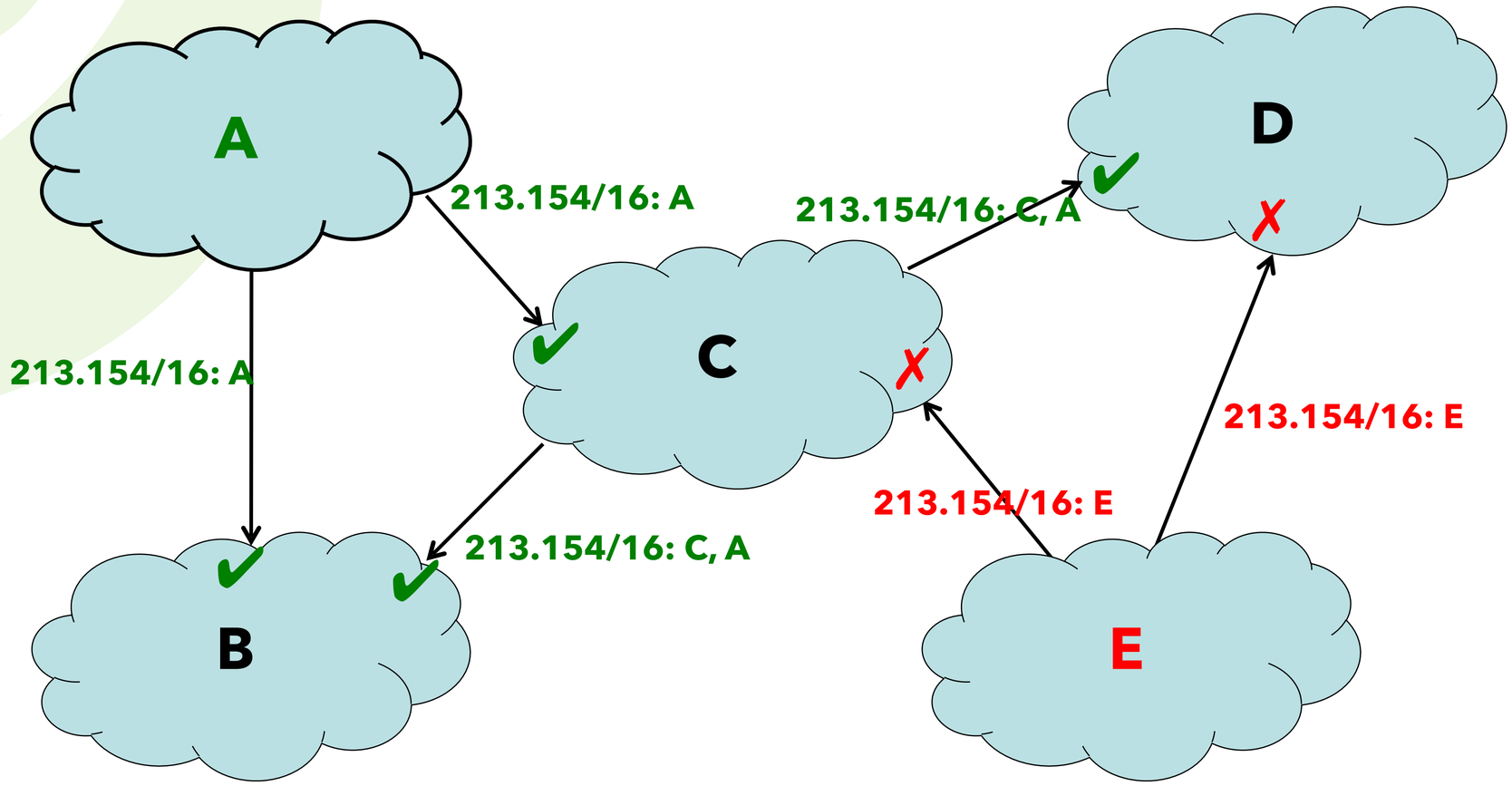
Route Hijacks 101



RPKI Structuur

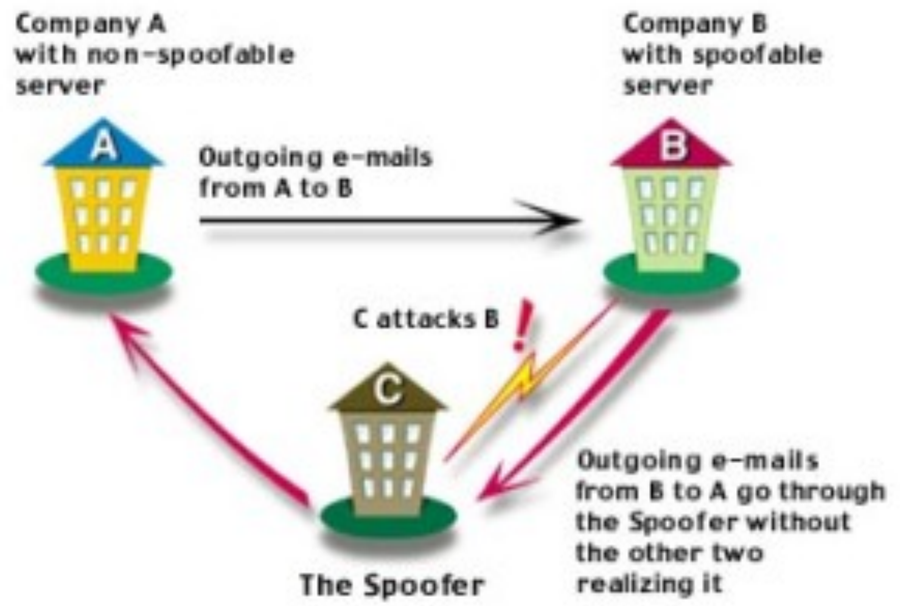


Routing with RPKI Explained



DNS Spoofing

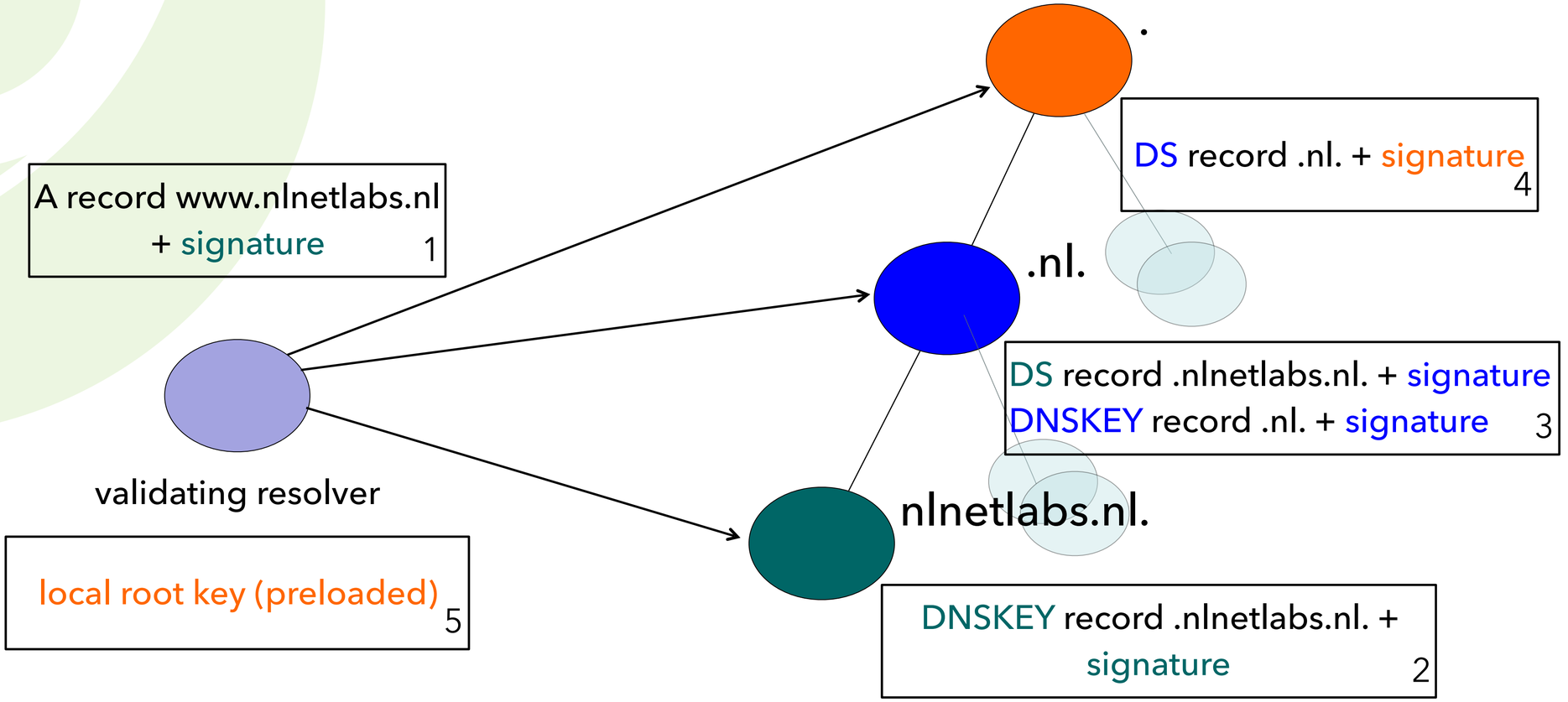
- DNS Spoofing by cache poisoning
  - attacker flood a DNS resolver with phony information with bogus DNS results
  - by the law of large numbers, these attacks get a match and plant a bogus result into the cache
- Man-in-the-middle attacks
  - redirect to wrong Internet sites
  - email to non-authorized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



Taking RPKI & DNSSEC Further

- BGP path validation
  - Currently ‘route origin validation’
  - Methods
    - BGPSEC hard to deploy (IETF RFC)
    - AS_PATH verification using RPKI (IETF draft)
- DNSSEC as a (alternative to) Web PKI
  - DANE: DNS based authentication of named entities

Risk Analysis TNO–NLnet Labs Report

- DNS risks and vulnerabilities
  - spoofing (as presented above), impact on integrity
  - DDoS of DNS root name servers (A–M), impact on availability
- BGP risks and vulnerabilities
  - route hijacks and leaks: misconfiguration or (bad) intent
  - impact on availability, integrity and confidentiality

Risk Analysis TNO-NLnet Labs Report (2)

Not presented, but part of study

- Network time NTP protocol risks and vulnerabilities
  - accurate time (w/ some margins) is essential for many services and operations
  - misconfiguration or manipulations can impact trust services, auditing of financial transactions, etc.
- Components of the physical Internet infrastructure: cables (fiber optics), major Internet Exchanges and large data center
  - impact of a physical incident is reduced availability, in general localised by redundancy in infrastructure
  - sea cables are ‘different’: less redundancy and higher impact with incidents

Summary

- The outcome of the survey is a framework for analysis for the risk category ‘Deterioration of the functioning of the Internet’ within the Nationaal Veiligheidsprofiel
- The Internet seems fragile
  - daily BGP and DNS incidents
  - cable, data center en IXPs disruptions
  - but has shown great resiliency