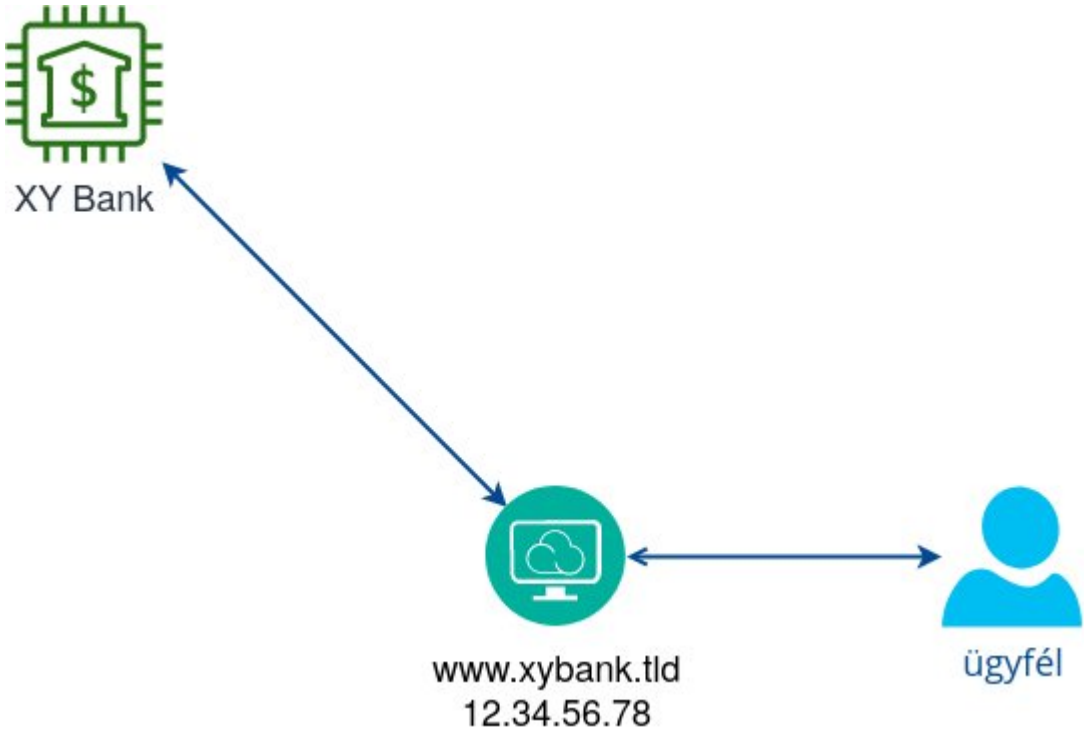
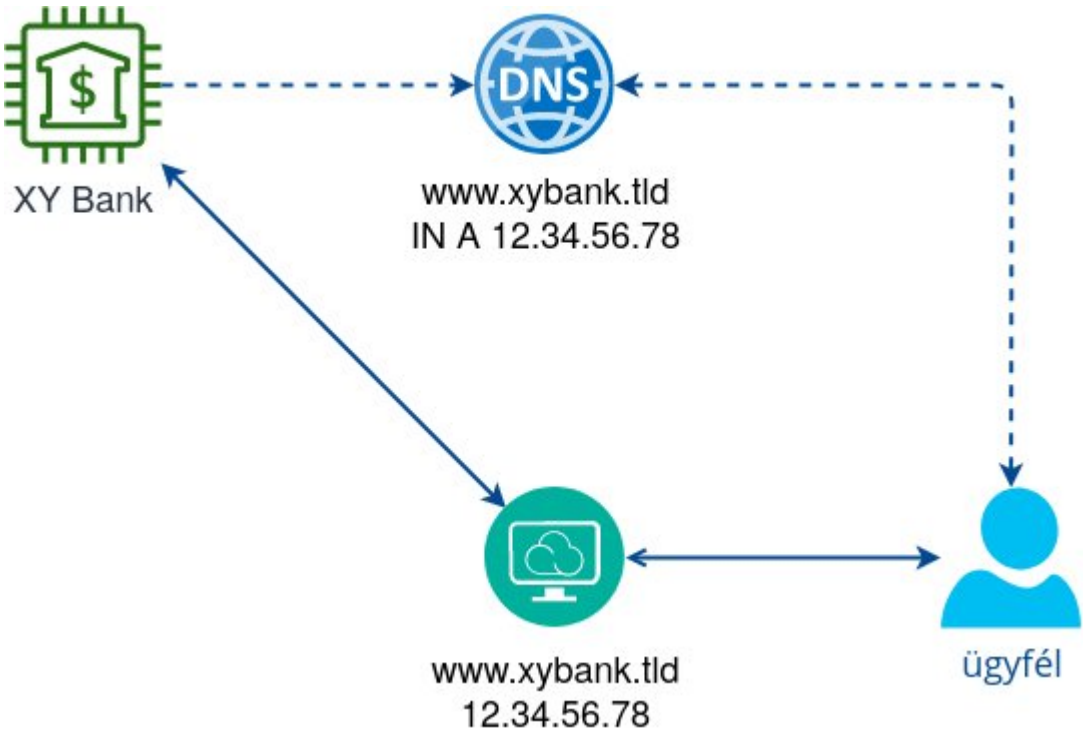
Támadási ablak kitárása a DNS segítségével

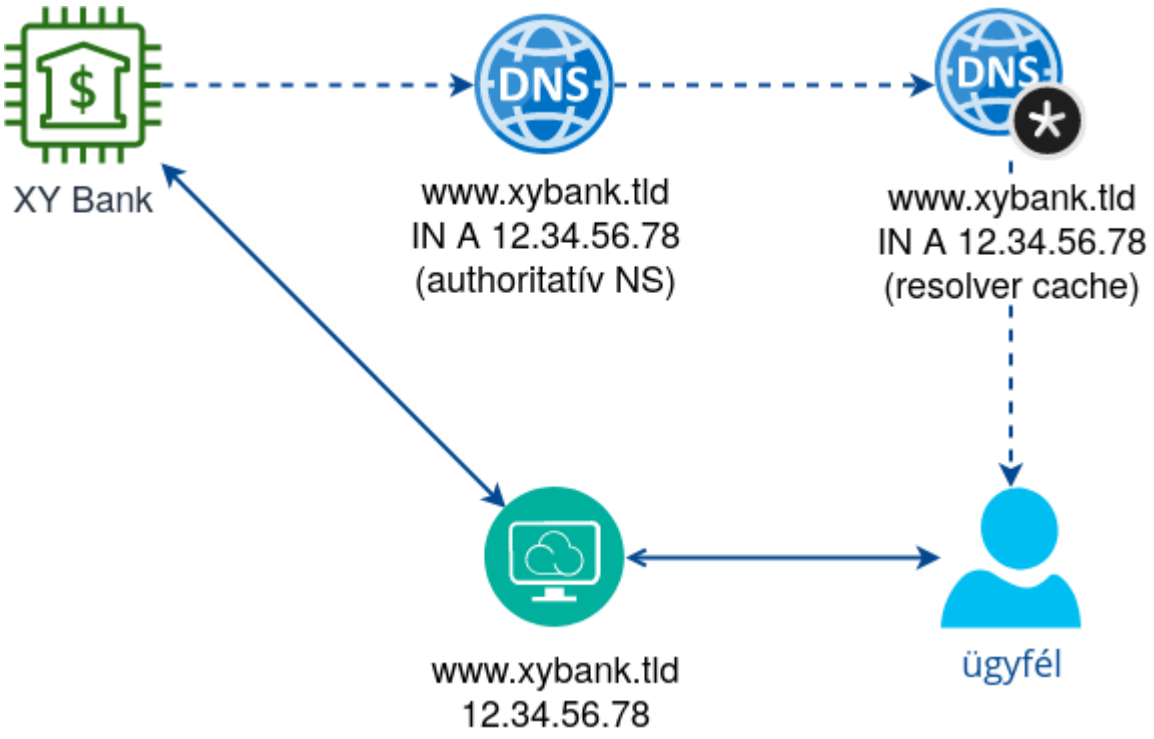
Biztonsági incidens kezelése, mitigáció, esettanulmány egy képzeletbeli DNS incidens kapcsán

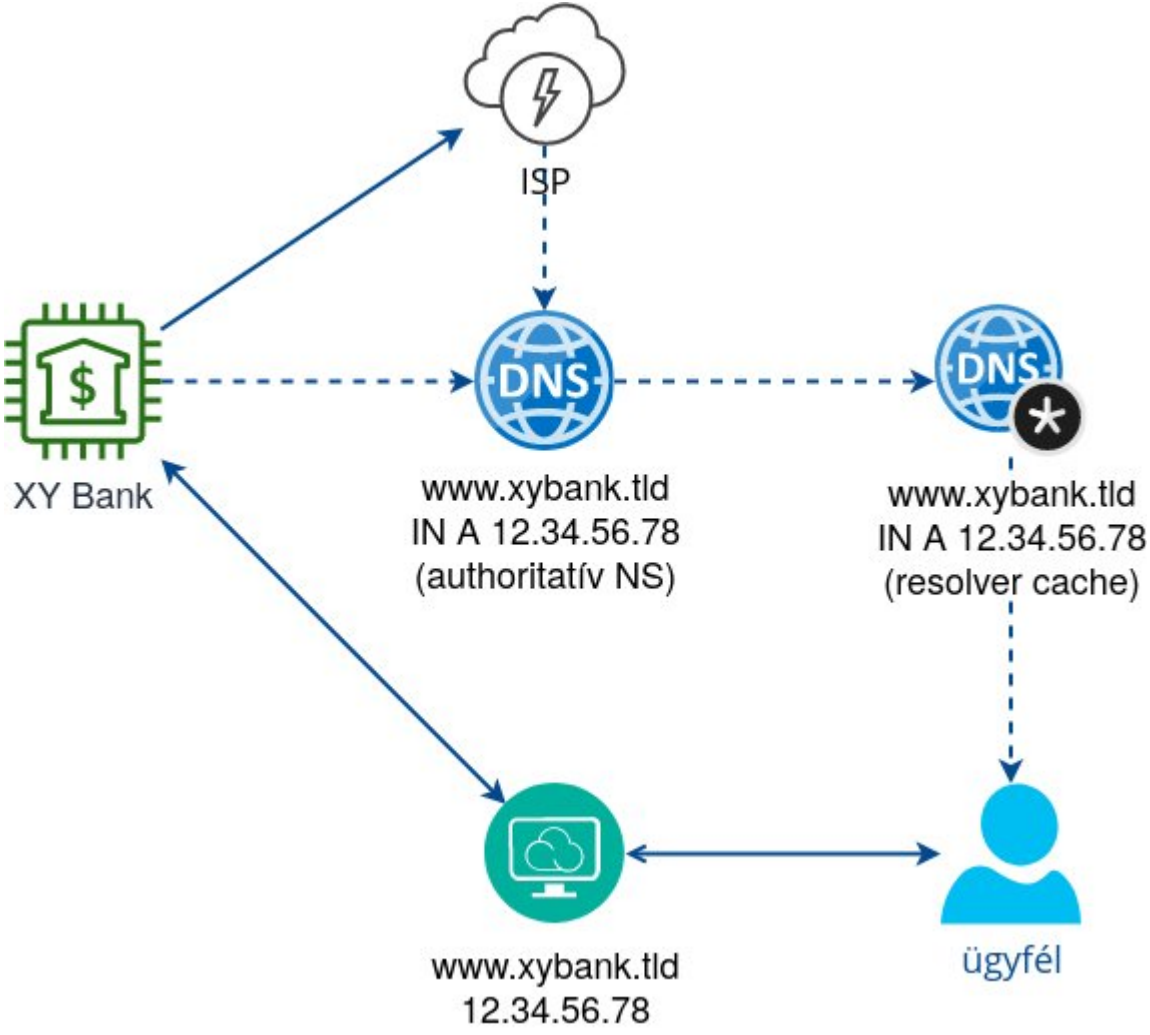
Rigó Ernő, SZTAKI
<rigo@sztaki.hu>

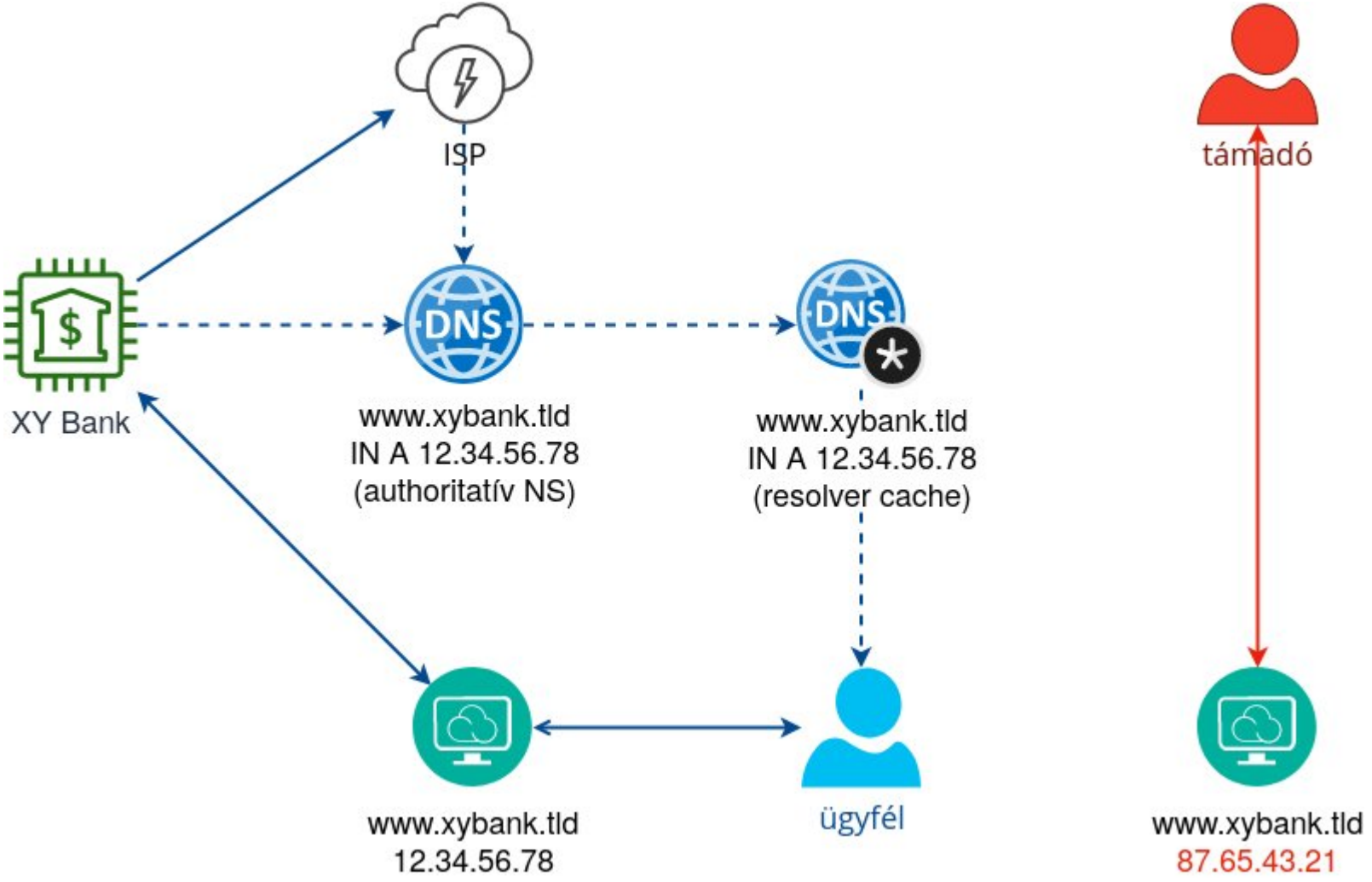
Az incidens

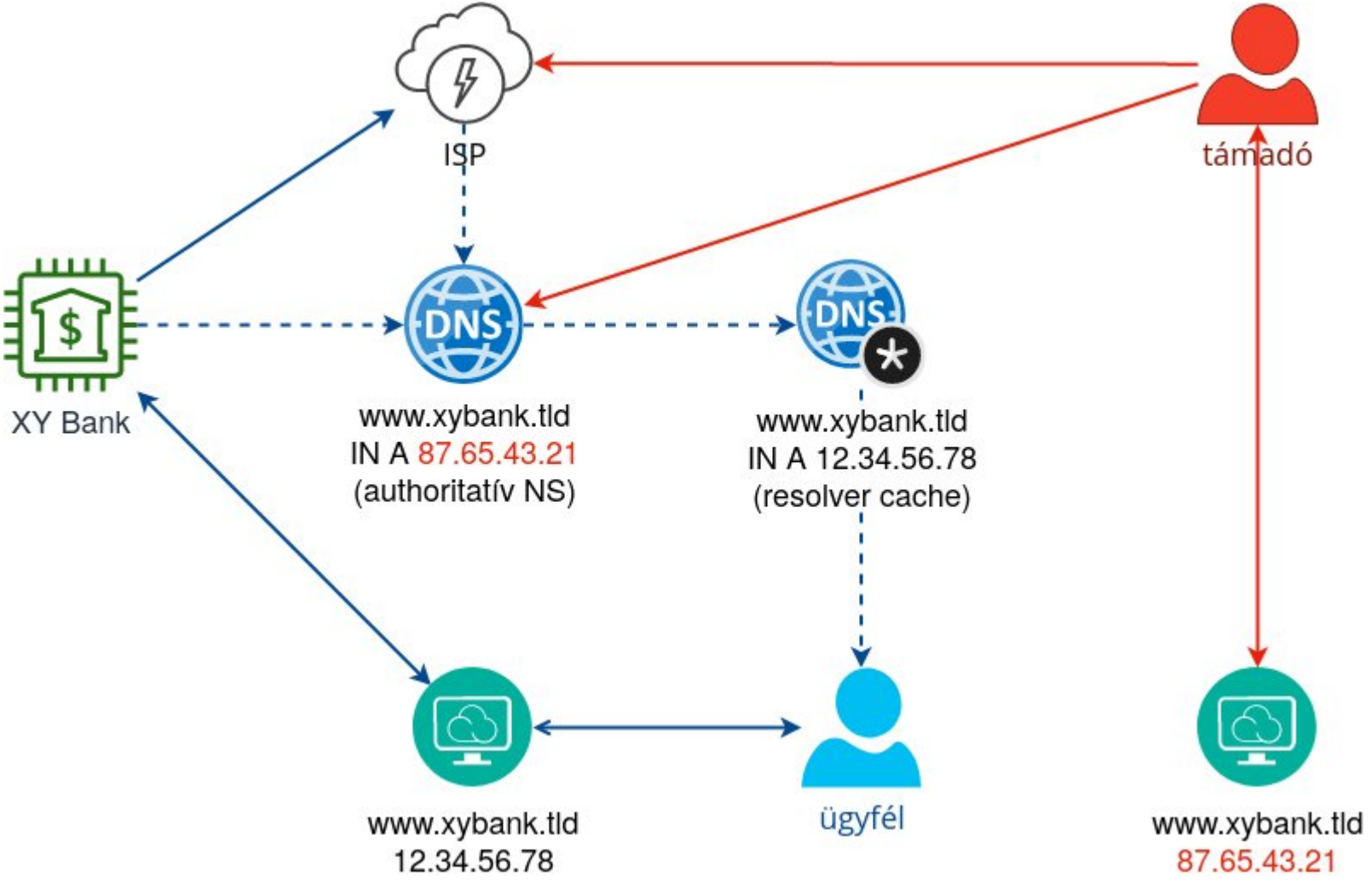

XY Bank
www.xybank.tld
12.34.56.78
ügyfél

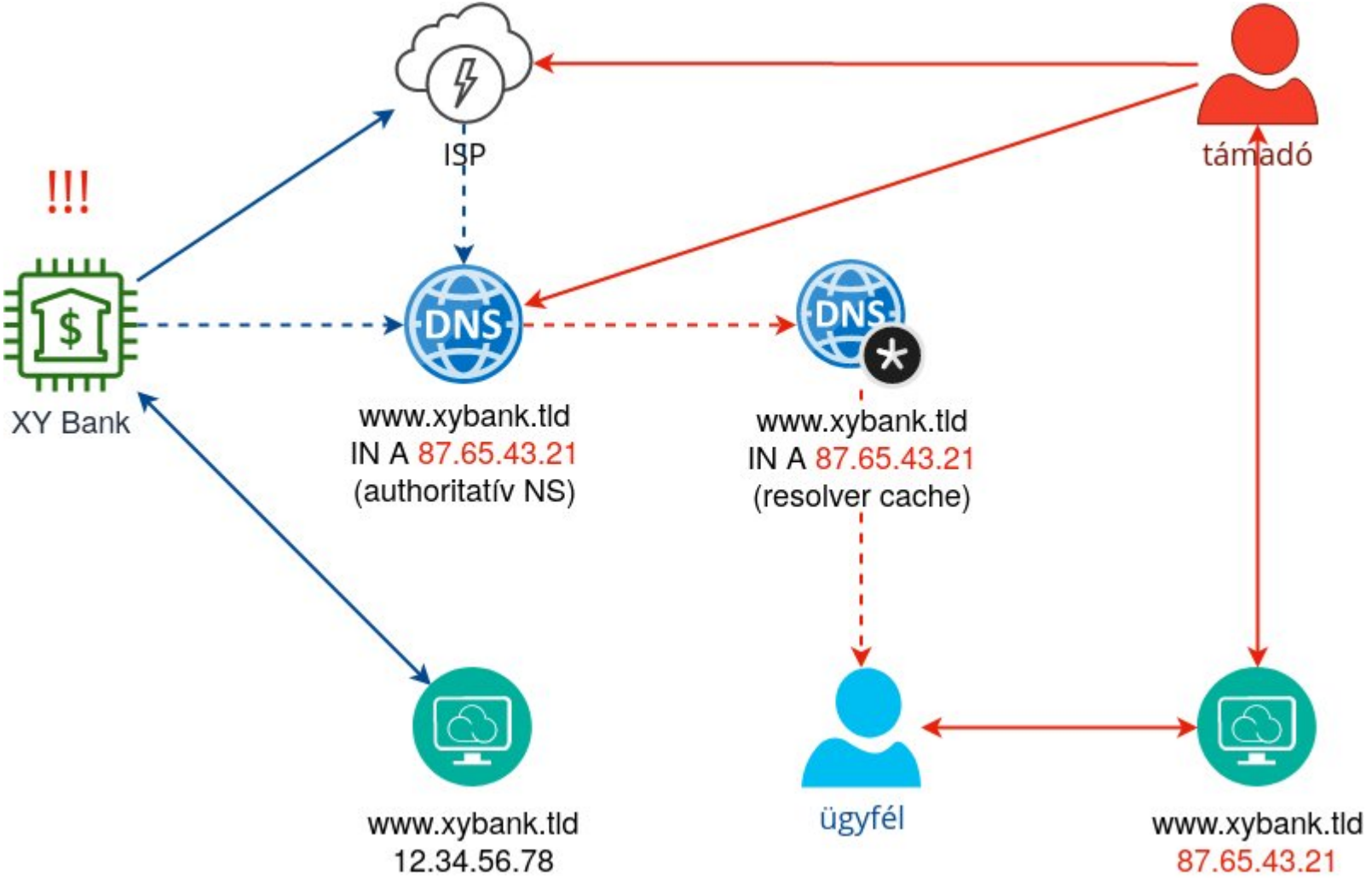

XY Bank
DNS
www.xybank.tld
IN A 12.34.56.78
www.xybank.tld
12.34.56.78
ügyfél

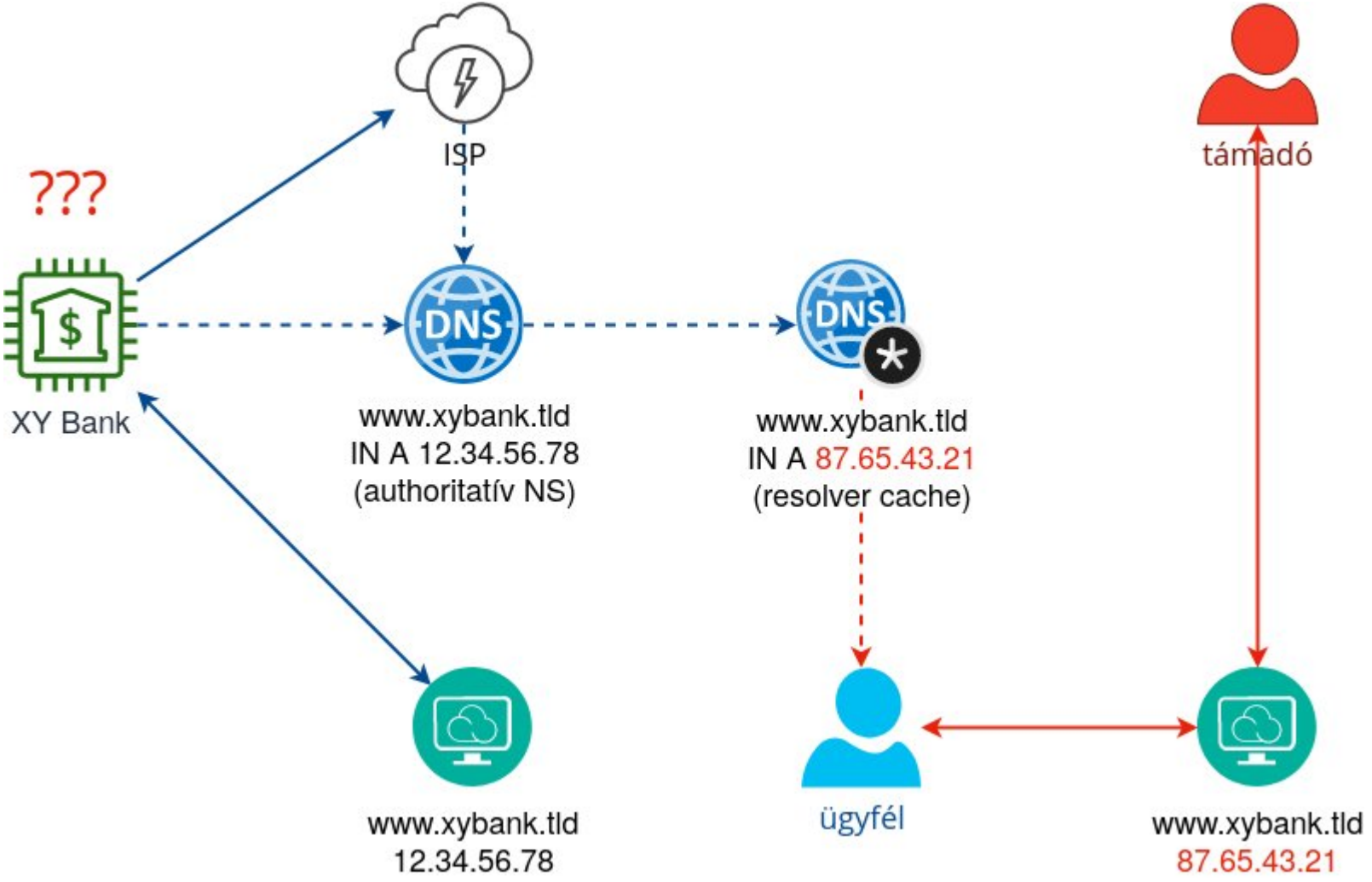

XY Bank
DNS
www.xybank.tld
IN A 12.34.56.78
(authoritatív NS)
DNS
www.xybank.tld
IN A 12.34.56.78
(resolver cache)
www.xybank.tld
12.34.56.78
ügyfél


ISP
XY Bank
DNS
www.xybank.tld
IN A 12.34.56.78
(authoritatív NS)
DNS
www.xybank.tld
IN A 12.34.56.78
(resolver cache)
www.xybank.tld
12.34.56.78
ügyfél


ISP
támadó
XY Bank
DNS
DNS
www.xybank.tld
IN A 12.34.56.78
(authoritatív NS)
www.xybank.tld
IN A 12.34.56.78
(resolver cache)
www.xybank.tld
12.34.56.78
ügyfél
www.xybank.tld
87.65.43.21


ISP
támadó
XY Bank
DNS
DNS
www.xybank.tld
IN A 87.65.43.21
(authoritatív NS)
www.xybank.tld
IN A 12.34.56.78
(resolver cache)
www.xybank.tld
12.34.56.78
ügyfél
www.xybank.tld
87.65.43.21


ISP
támadó
!!!
DNS
DNS
XY Bank
www.xybank.tld
IN A 87.65.43.21
(authoritatív NS)
www.xybank.tld
IN A 87.65.43.21
(resolver cache)
www.xybank.tld
12.34.56.78
ügyfél
www.xybank.tld
87.65.43.21


???
ISP
támadó
DNS
DNS
XY Bank
www.xybank.tld
IN A 12.34.56.78
(authoritatív NS)
www.xybank.tld
IN A 87.65.43.21
(resolver cache)
www.xybank.tld
12.34.56.78
ügyfél
www.xybank.tld
87.65.43.21

Háttér

DNS Time To Live (TTL)

- DNS rekordok érvényességi ideje
- A hiteles névszerver a resolvert ***tájékoztatja***
- Értéke változatos
  - Általános RIPE ajánlás: 1-24 óra
  - Dinamikus DNS, HA, DoS védelem: 1-15 perc
  - Maximális érték: 2^{31}-1 másodperc, vagyis 68.096 év

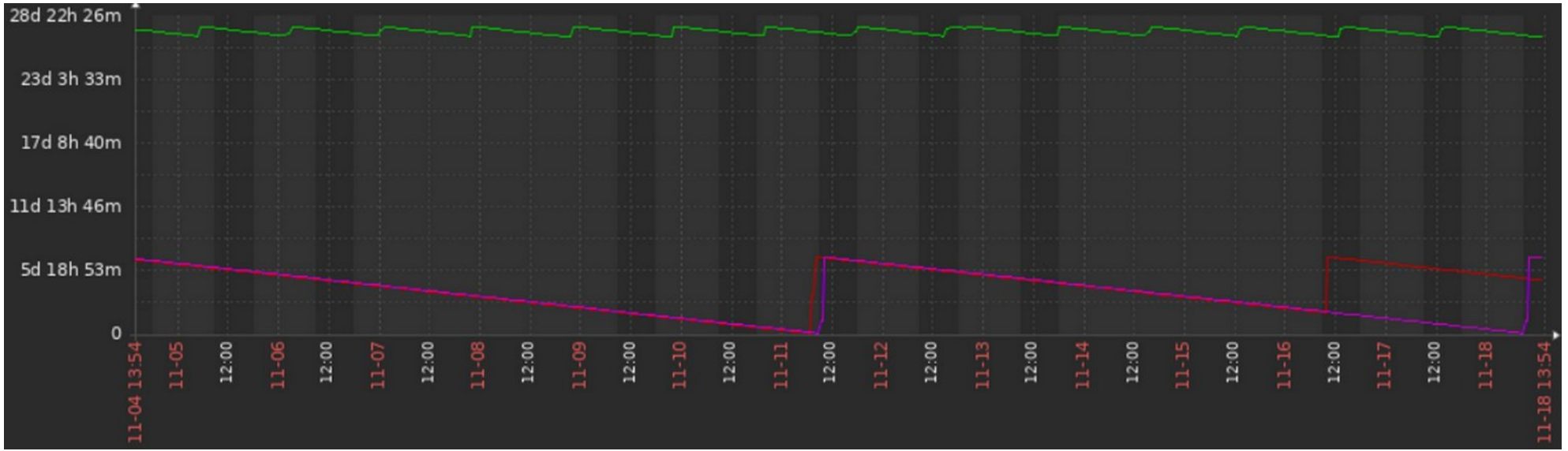
DNS resolver üzemeltetése

- ISP-k számára „kötelező”
- Nyílt (open) resolverek
  - DNS amplification attack (DDoS)
  - Konfigurációs hiba
- Nyilvános (public) resolverek
  - Privacy kérdések
  - Értéknövelt szolgáltatások
  - Mobilitás

Nyilvános DNS resolverek

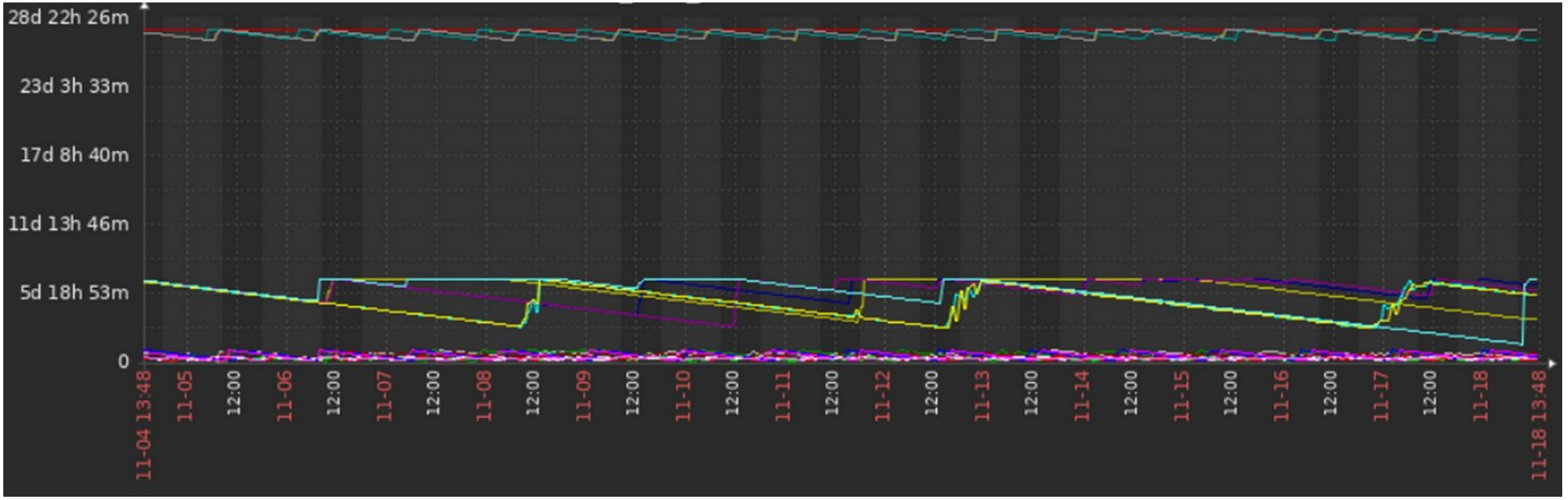
- Önkiszolgáló cache törlő szolgáltatás
  - OpenDNS
    - resolver1.opendns.com, resolver2.opendns.com
    - https://cachecheck.opendns.com/
  - Google
    - 8.8.8.8, 8.8.4.4
    - https://developers.google.com/speed/public-dns/cache
  - CloudFlare
    - 1.1.1.1, 1.0.0.1
    - https://1.1.1.1/purge-cache/
  - Verisign, Neustar
    - recpubns1.nstld.net, recpubns2.nstld.net
    - rdns1.ultradns.net, rdns2.ultradns.net
    - https://www.verisign.com/en_US/security-services/public-dns/dns-cache/index.xhtml
- Abuse contact űrlap vagy e-mail cím
  - Comodo
    - ns1.recursive.dnsbycomodo.com, ns2.recursive.dnsbycomodo.com
    - support@comodo.com
  - Quad9
    - 9.9.9.9, rpz-public-resolver1.rrdns.pch.net, rpz-public-resolver2.rrdns.pch.net
    - support@quad9.net
  - UncensoredDNS
    - anycast.censurfridns.dk, unicast.censurfridns.dk
  - Yandex
    - dns.yandex.ru
  - AdGuard
    - dns.adguard.com
  - Alternate DNS
    - dns1.alternate-dns.com, dns2.alternate-dns.com
    - support@alternate-dns.com
  - CleanBrowsing
    - dns.cleanbrowsing.org

TTL privát / ISP resolverekben



- Forrás TTL: 28 nap (teszt rekord)
- Resolver válaszban megjelenő TTL: 7 nap - 28 nap
- Gyakorlati TTL: 1 nap – 7 nap

TTL nyilvános resolverekben



- Forrás TTL: 28 nap (teszt rekord)
- Resolver válaszban megjelenő TTL: 1 nap – 28 nap
- Gyakorlati TTL: 5 perc – 7 nap

11 hazai bank gyakorlata

- DNS szerverek külső szolgáltatóknál
  - 7 bank 2 hazai „nagy” szolgáltatónál
  - 2 bank 2 hazai „kis” szolgáltatónál (ISO 27001 nélkül)
  - 1 bank külföldi szolgáltatónál
- Egyéb DNS szerverek
  - 7 bank csak külső szolgáltató osztott DNS szerverét használja
  - 4 banknak saját dedikált DNS szervere IS van
  - 1 banknak CSAK saját dedikált DNS szerverei vannak

Értékelés

Értékelés

- Támadás összetettsége
- Bekövetkezési valószínűség
- Megelőzési lehetőségek
- Mitigációs lehetőségek

Köszönöm a figyelmet!