possible.lv

IT security services

DNS on steroids

SECURITY EXPERT

CyberChess 2024 | Riga | 03.10.2024. | Kirils Solovjovs

Kirils Solovjovs

SECURITY EXPERT

- Mg.sc.comp., Mg.phys.
- CEO at *Possible Security*
- Background
  - Live network forensics
  - Social engineering
- Somehow keeps breaking stuff

SECURITY

INSECURITY

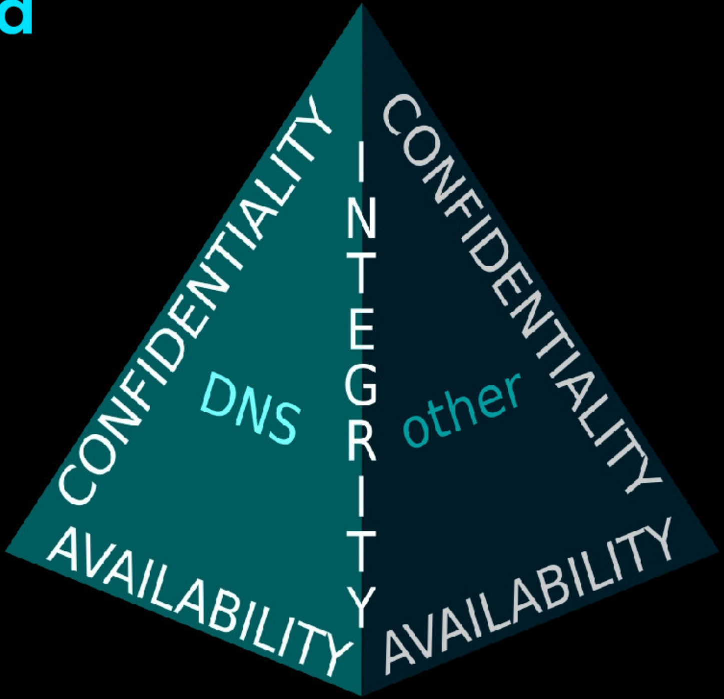
INSECURITY

Architectural vulnerabilities

Implementation weaknesses

Human errors

The CIA pyramid

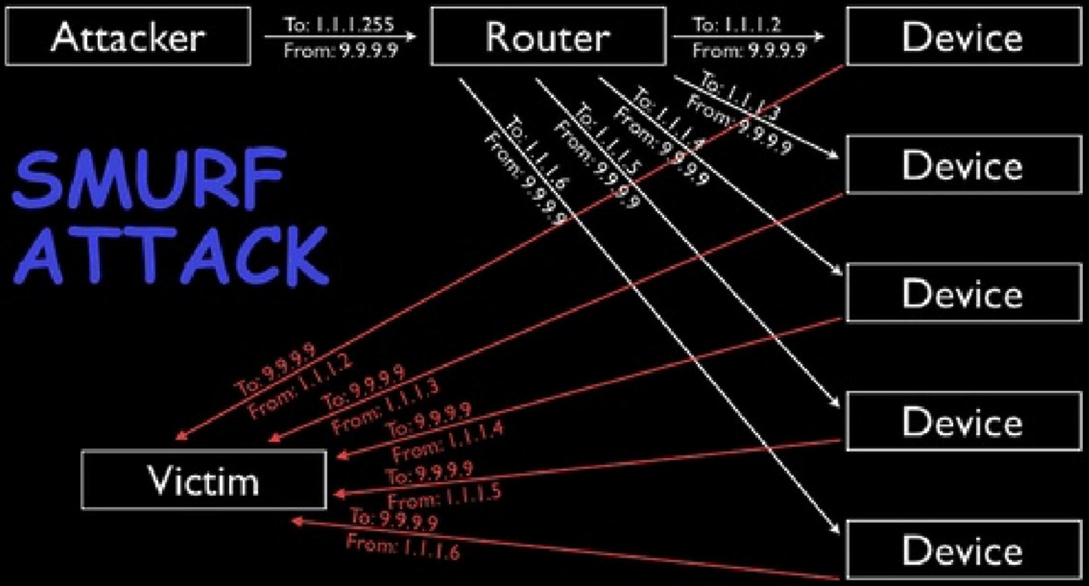


Impact of DNS attacks; scope duality (left – unchanged, right - changed)

Source: Possible Security

Architectural vulnerabilities

DNS reflection & amplification

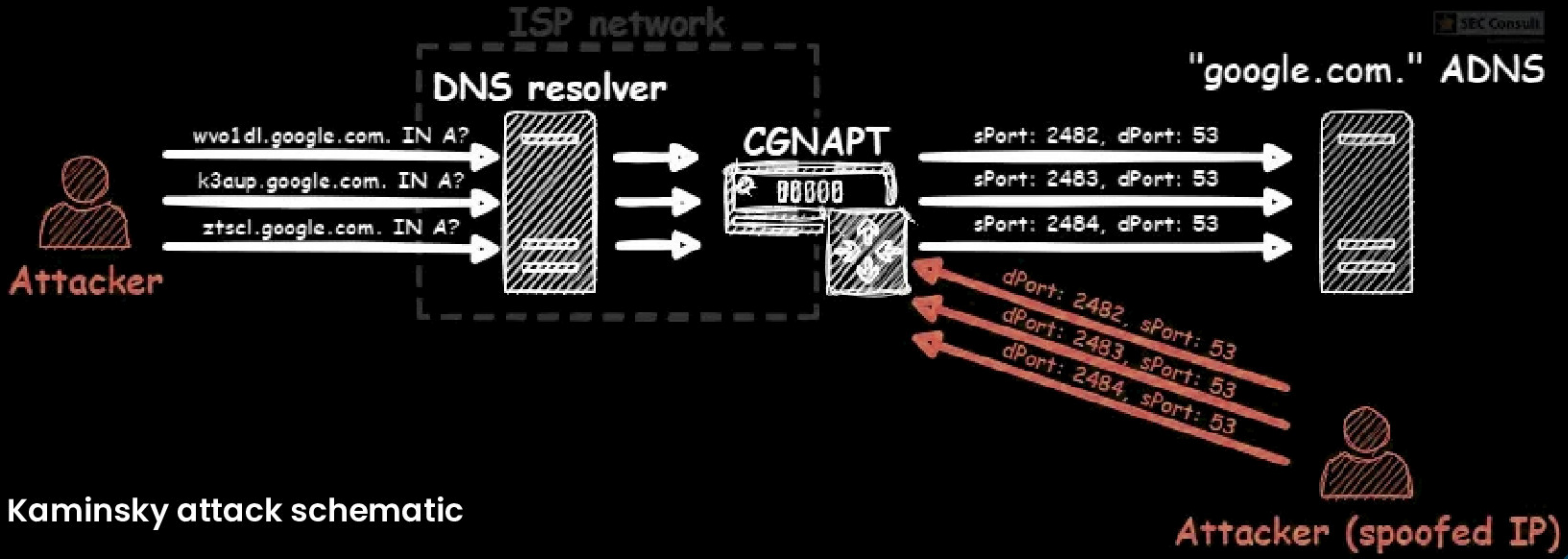


**The lack of 3way handshake in UDP enables reflection;
size ratio between DNS query and response enables amplification**

Source: Cloudflare

DNS spoofing / cache poisoning

- Can be used against systems sending e-mails on demand



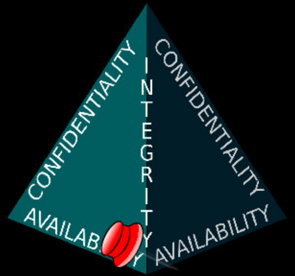
Kaminsky attack schematic

Source: SEC Consult

DDoS attacks on root nameservers

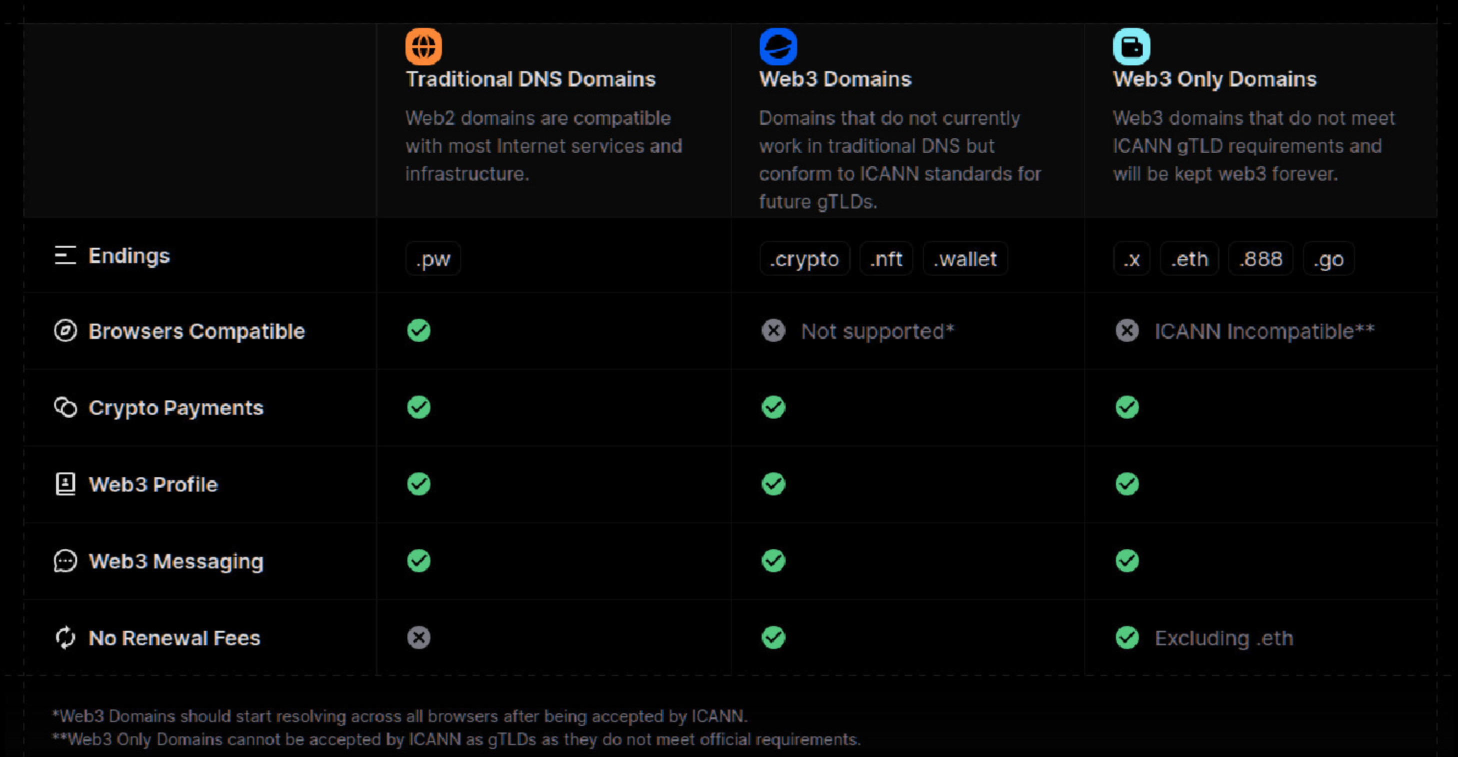
- Is there a center to the internet?
  - If there is, it’s the root nameservers
  - Makes sense to attack!
- Attempted in 2002, 2007, 2012, 2015
- Never panned out → Theoretical threat

Root conflicts with altDNS



- RFC 2826
  - To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority.

Root conflicts vs DNS-on-a-blockchain



	Traditional DNS Domains Web2 domains are compatible with most Internet services and infrastructure.	**Web3 Domains** Domains that do not currently work in traditional DNS but conform to ICANN standards for future gTLDs.	**Web3 Only Domains** Web3 domains that do not meet ICANN gTLD requirements and will be kept web3 forever.
Endings	.pw	.crypto .nft .wallet	.x .eth .888 .go
Browsers Compatible	✓	✗ Not supported*	✗ ICANN Incompatible**
Crypto Payments	✓	✓	✓
Web3 Profile	✓	✓	✓
Web3 Messaging	✓	✓	✓
No Renewal Fees	✗	✓	✓ Excluding .eth

*Web3 Domains should start resolving across all browsers after being accepted by ICANN.

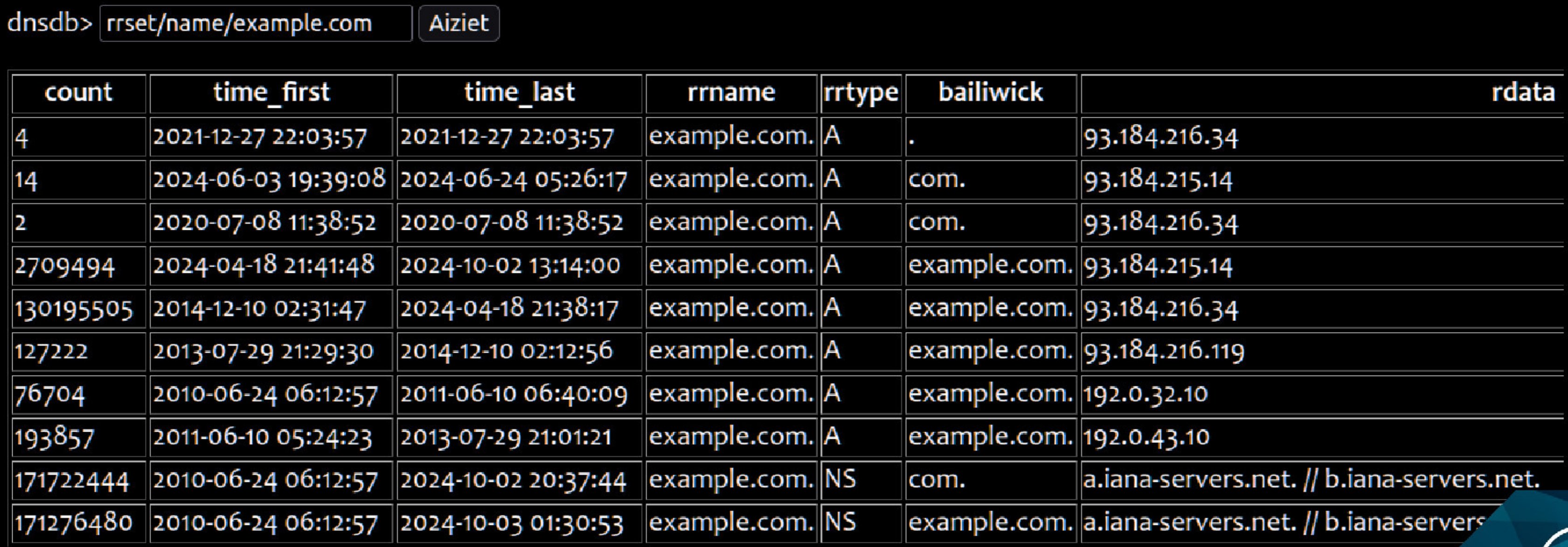
**Web3 Only Domains cannot be accepted by ICANN as gTLDs as they do not meet official requirements.

Web2 vs Web3 domains

Source: unstoppable domains

Passive DNS

- Can be used to work around DDoS protection

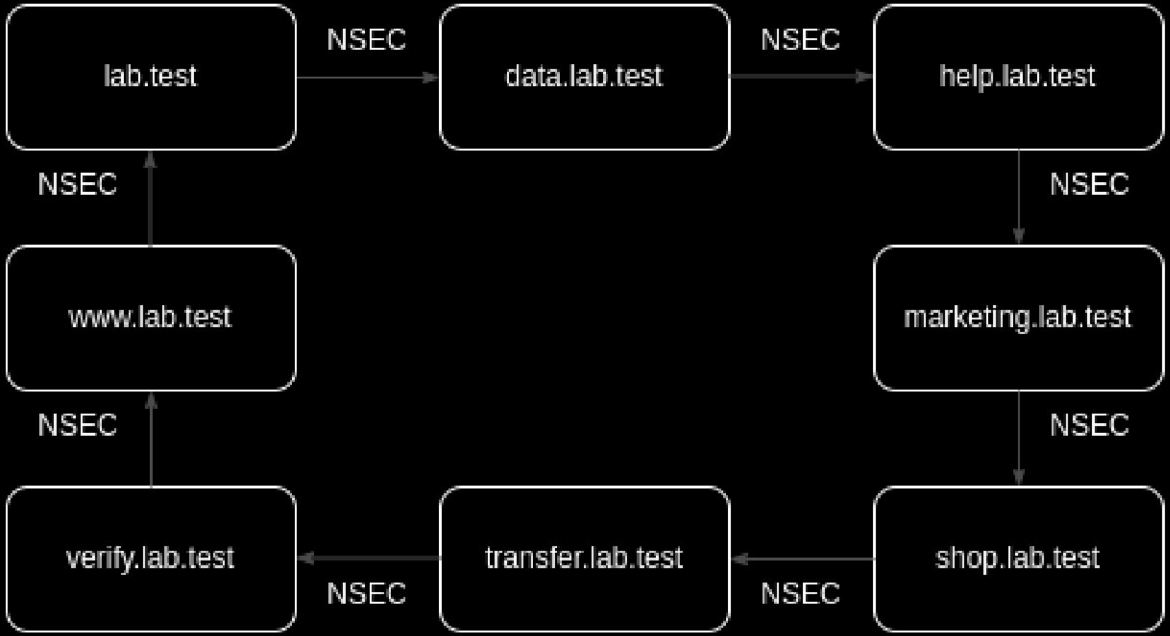


count	time_first	time_last	rrname	rrtype	bailiwick	rdata
4	2021-12-27 22:03:57	2021-12-27 22:03:57	example.com.	A	.	93.184.216.34
14	2024-06-03 19:39:08	2024-06-24 05:26:17	example.com.	A	com.	93.184.215.14
2	2020-07-08 11:38:52	2020-07-08 11:38:52	example.com.	A	com.	93.184.216.34
2709494	2024-04-18 21:41:48	2024-10-02 13:14:00	example.com.	A	example.com.	93.184.215.14
130195505	2014-12-10 02:31:47	2024-04-18 21:38:17	example.com.	A	example.com.	93.184.216.34
127222	2013-07-29 21:29:30	2014-12-10 02:12:56	example.com.	A	example.com.	93.184.216.119
76704	2010-06-24 06:12:57	2011-06-10 06:40:09	example.com.	A	example.com.	192.0.32.10
193857	2011-06-10 05:24:23	2013-07-29 21:01:21	example.com.	A	example.com.	192.0.43.10
171722444	2010-06-24 06:12:57	2024-10-02 20:37:44	example.com.	NS	com.	a.iana-servers.net. // b.iana-servers.net.
171276480	2010-06-24 06:12:57	2024-10-03 01:30:53	example.com.	NS	example.com.	a.iana-servers.net. // b.iana-servers

Historical NS and SOA records for example.com. rrname (via pDNS)

Source: net.02.lv

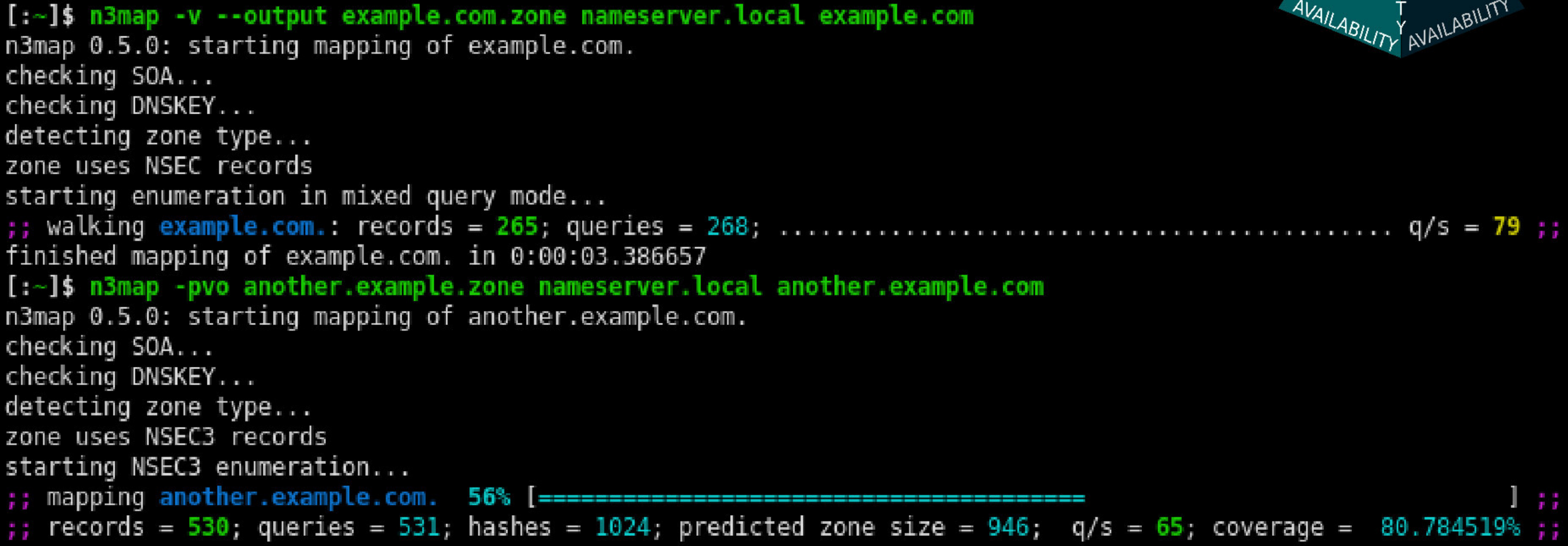
NSEC



Linked list of chained NSEC records

Source: SECURE SYSTEMS ENGINEERING GMBH

NSEC3



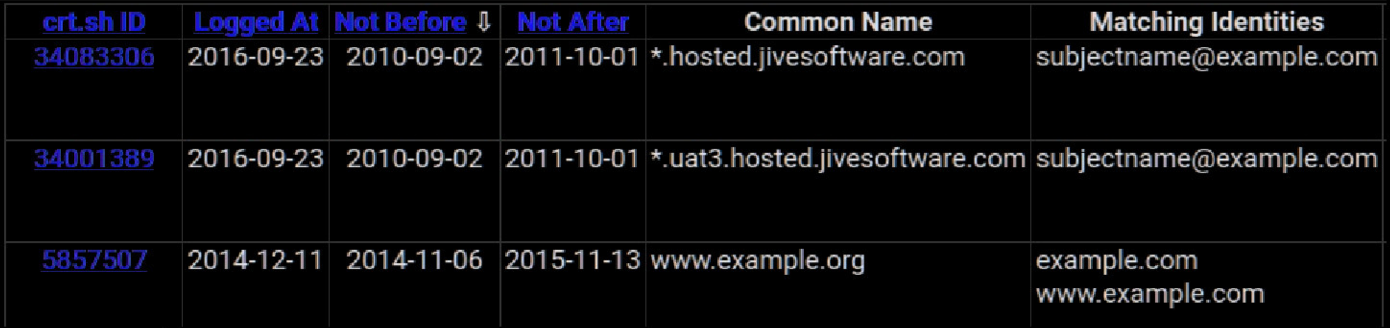
```
[:~]$ n3map -v --output example.com.zone nameserver.local example.com
n3map 0.5.0: starting mapping of example.com.
checking SOA...
checking DNSKEY...
detecting zone type...
zone uses NSEC records
starting enumeration in mixed query mode...
;; walking example.com.: records = 265; queries = 268; ............................................ q/s = 79 ;;
finished mapping of example.com. in 0:00:03.386657
[:~]$ n3map -pvo another.example.zone nameserver.local another.example.com
n3map 0.5.0: starting mapping of another.example.com.
checking SOA...
checking DNSKEY...
detecting zone type...
zone uses NSEC3 records
starting NSEC3 enumeration...
;; mapping another.example.com.  56% [=======================================                              ] ;;
;; records = 530; queries = 531; hashes = 1024; predicted zone size = 946;  q/s = 65; coverage =  80.784519% ;;
```

DNSSEC Zone Enumerator at work

Source: github

Certificate Transparency

- Symantec, Comodo, and others are doing bad stuff[1]
  - We try to fix it with HPKP
    - *shooting_yourself_in_the_foot.gif*
  - CT promises to solve it all



crt.sh ID	Logged At	Not Before ⇩	Not After	Common Name	Matching Identities
34083306	2016-09-23	2010-09-02	2011-10-01	*.hosted.jivesoftware.com	subjectname@example.com
34001389	2016-09-23	2010-09-02	2011-10-01	*.uat3.hosted.jivesoftware.com	subjectname@example.com
5857507	2014-12-11	2014-11-06	2015-11-13	www.example.org	example.com www.example.com

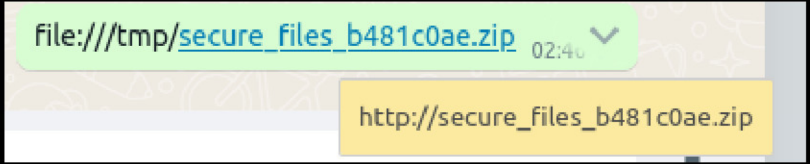
CT log for example.com

Source: crt.sh

[1] https://sslmate.com/resources/certificate_authority_failures

Dangerous gTLDs

- .zip
- .mov
- and more to come



file:///tmp/secure_files_b481c0ae.zip 02:4

http://secure_files_b481c0ae.zip

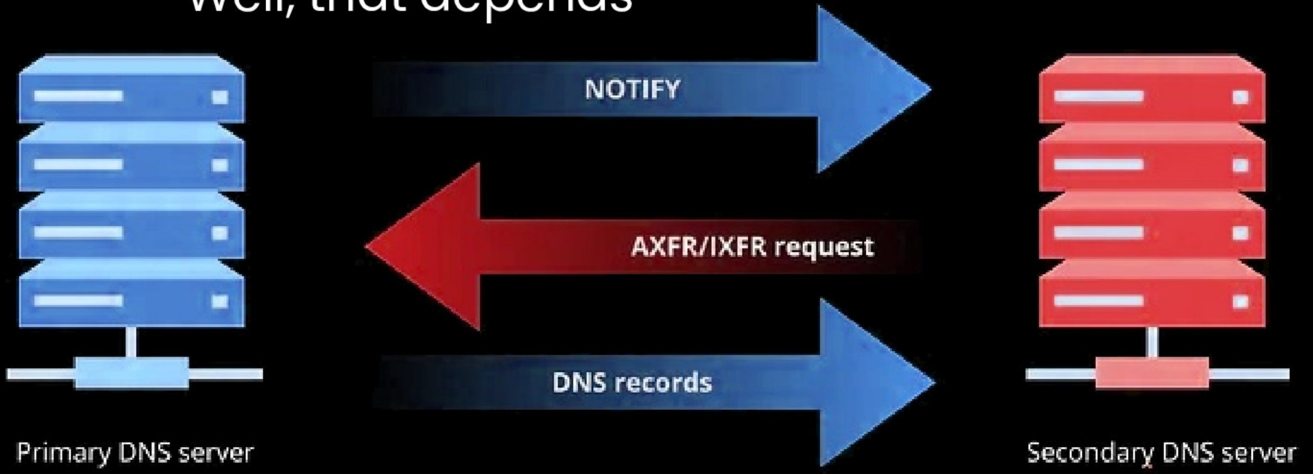
An older version of Meta's WhatsApp Web parsing a non-domain as a domain

Source: Possible Security

Implementation weaknesses

AXFR

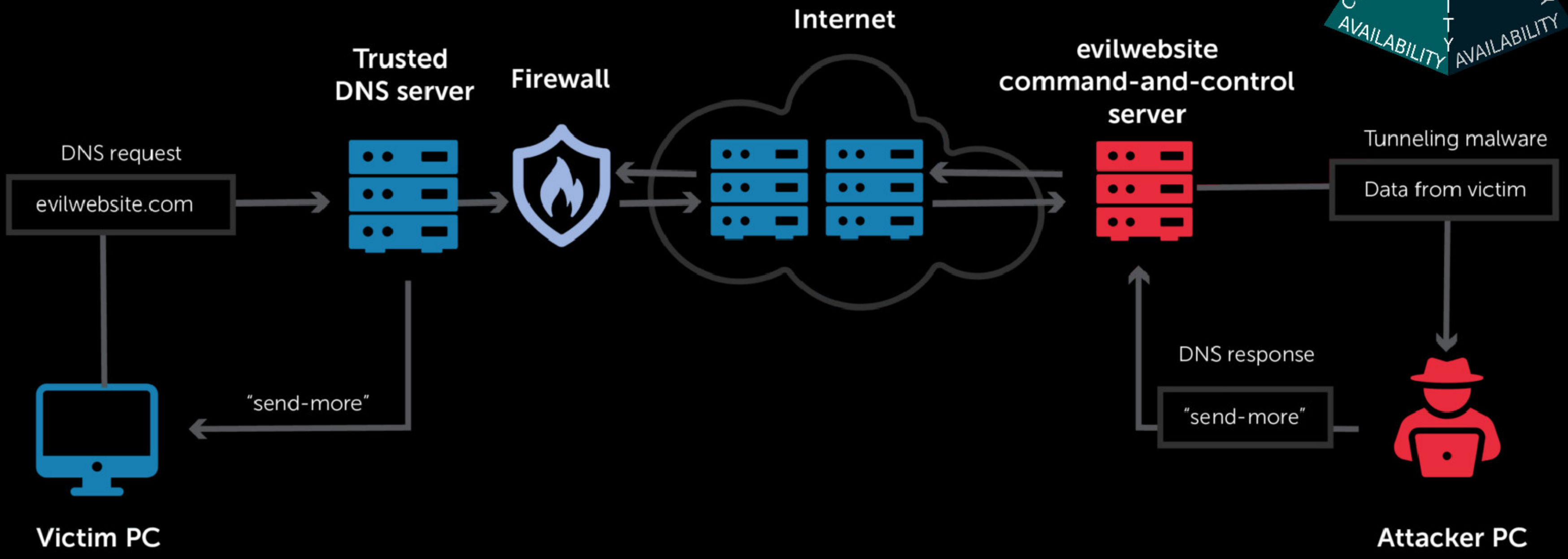
- Who can request an AXFR?
  - Well, that depends



DNS zone transfer

Source: Raghuveer Singh Chouhan

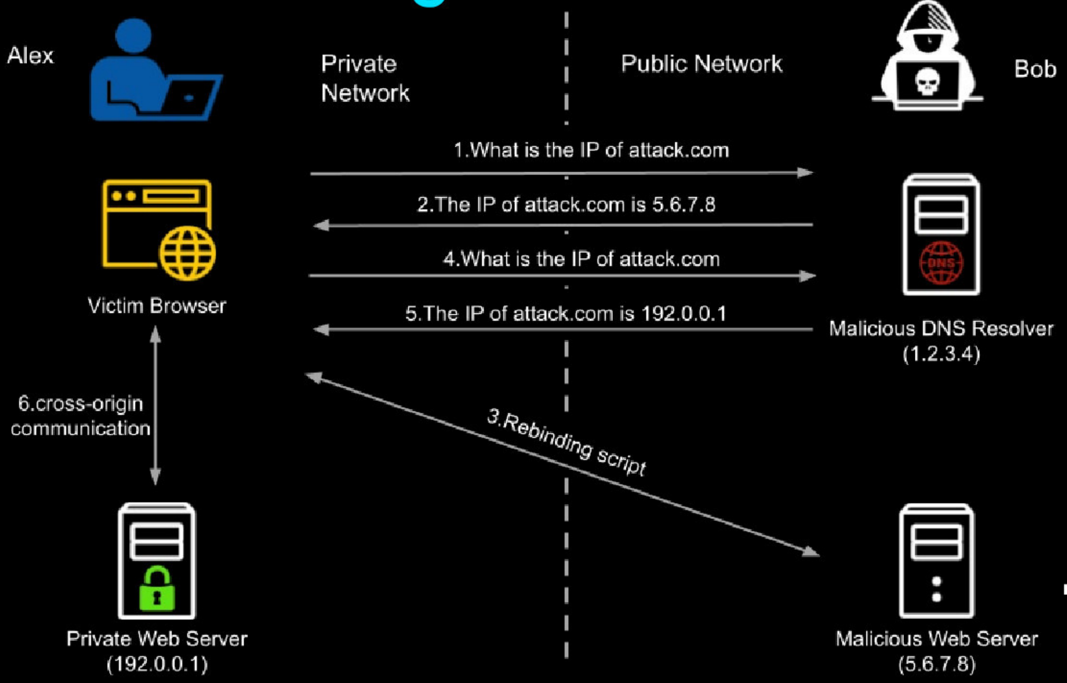
DNS tunnelling



DNS tunnelling

Source: Bluecat

DNS rebinding


Alex
Private Network
Public Network
Bob
1.What is the IP of attack.com
2.The IP of attack.com is 5.6.7.8
4.What is the IP of attack.com
5.The IP of attack.com is 192.0.0.1
Victim Browser
Malicious DNS Resolver (1.2.3.4)
6.cross-origin communication
3.Rebinding script
Private Web Server (192.0.0.1)
Malicious Web Server (5.6.7.8)

DNS rebinding attack schematic

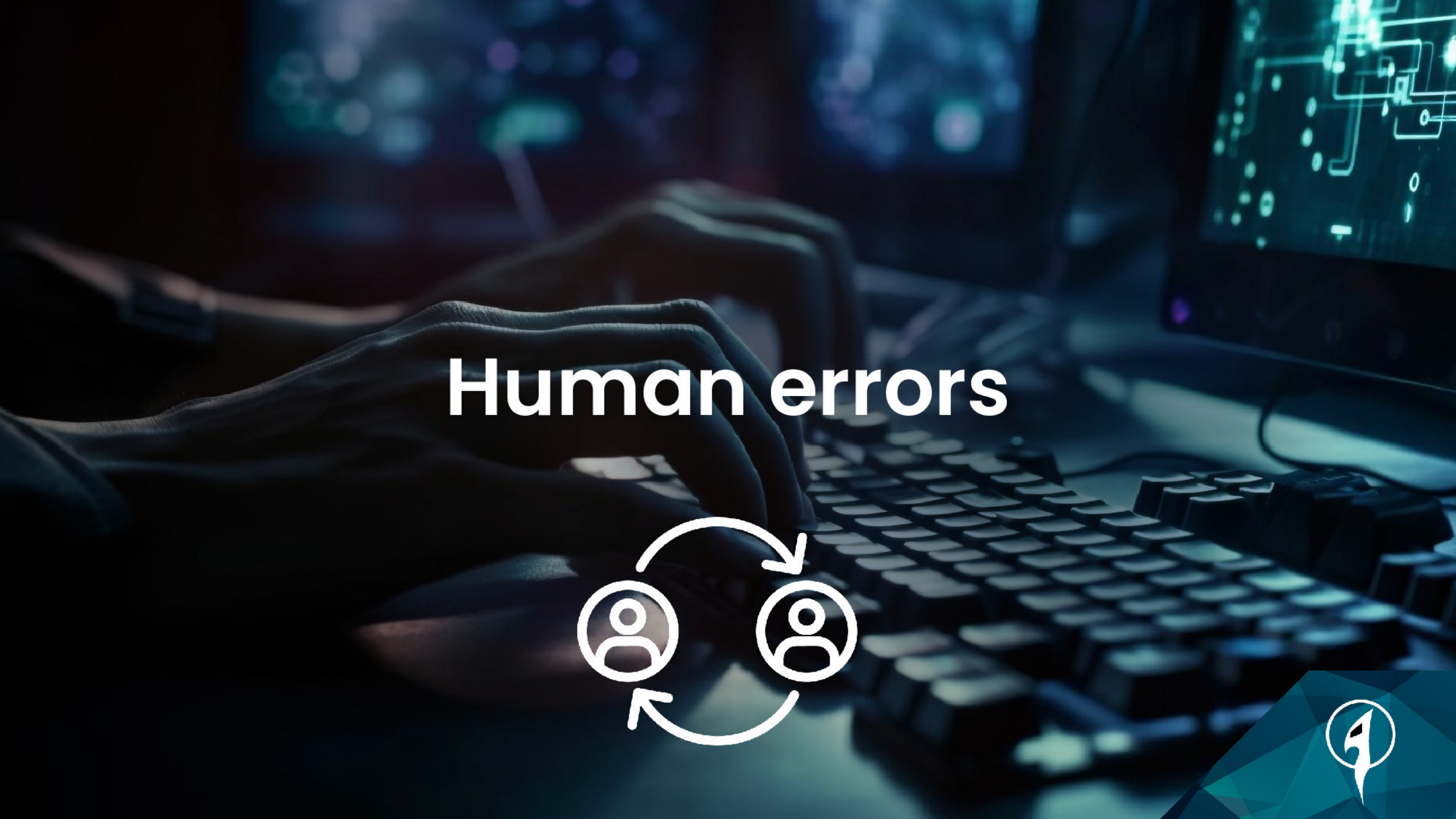
Source: Palo Alto Networks

- It's a type of timing attack

Exposure via DNS as a Service (managed DNS)

- **What we found was that registering certain "special" domains, specifically the name of the name server itself, has unexpected consequences** on all other customers using the name server. It breaks the isolation between tenants. We successfully registered one type of special domain, but we suspect there are many others.
  - Shir Tamari & Ami Luttwak, 2021

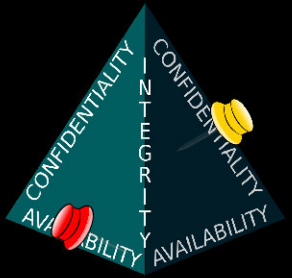
Human errors



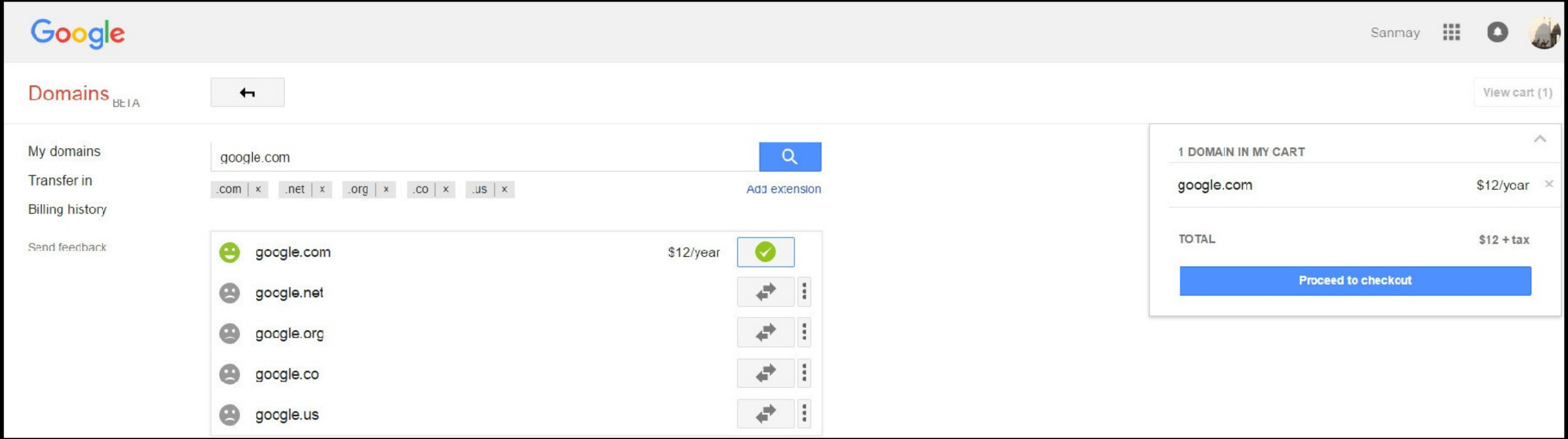
Typo-squatting

- registering misspelled domain names
- example.com <-> exampla.com

Drop-catching



- re-registering a freshly expired domain name



google.com

.com × .net × .org × .co × .us ×

google.com	$12/year	✓
google.net		
google.org		
google.co		
google.us		

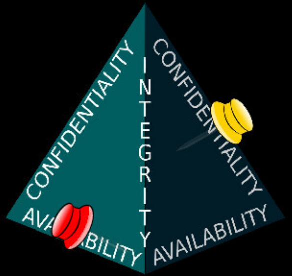
1 DOMAIN IN MY CART

google.com	$12/year
TOTAL	$12 + tax

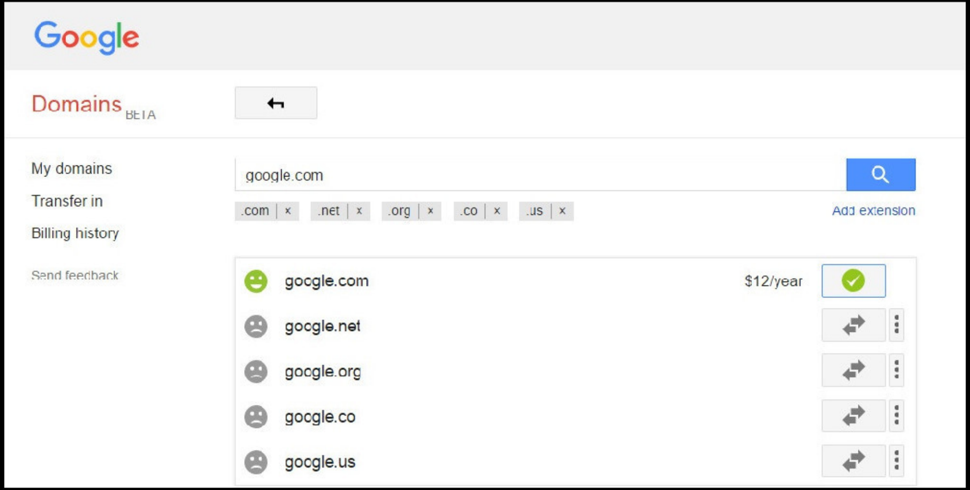
In 2015 Google sold the freshly expired google.com for $12

Source: Sanmay Ved

Drop-catching



- re-registering a freshly expired domain name



Google

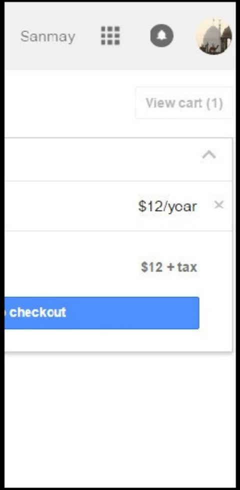
Domains BETA

My domains
Transfer in
Billing history
Send feedback

google.com

.com × .net × .org × .co × .us × Add extension

google.com	$12/year	✓
google.net		
google.org		
google.co		
google.us		



Sanmay

View cart (1)

$12/year ×

$12 + tax

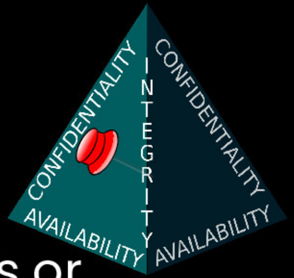
checkout

In 2015 Google sold the freshly expired google.com for $12

https://www.linkedin.com/pulse/i-purchased-domain-googlecom-via-google-domains-sanmay-ved

Source: Sanmay Ved

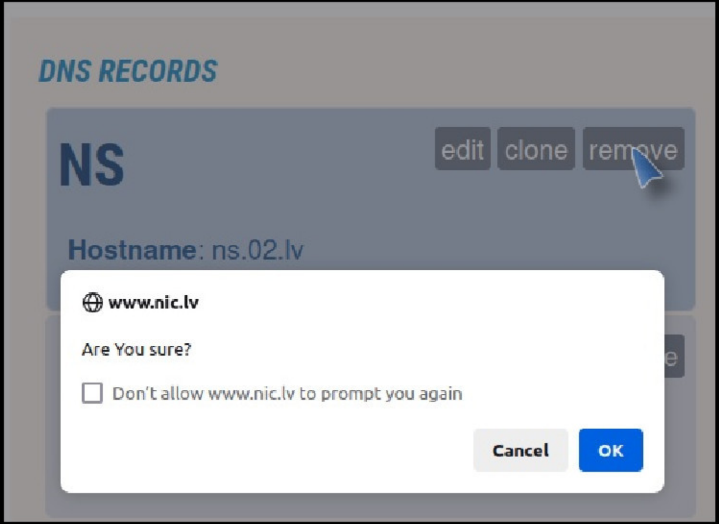
Domain hijacking / takeover



- Changing the owner of the domain by abusing registrars or registrant’s credentials

NS reclamation

1) Domain zone is delegated to NS of external trusted party ζ
2) [*decades pass*]
3) Domain changes ownership
4) NS records are deleted and replaced with A records / new NS records
5) ζ is not informed of this and does not destroy the zone
6) Users using ζ's authoritative and slave NSs as recursive servers are provided stale responses, potentially in perpetuum



DNS RECORDS

NS

Hostname: ns.02.lv

www.nic.lv

Are You sure?

☐ Don't allow www.nic.lv to prompt you again

Removal of zone delegation record on nic.lv

Source: Possible Security

Loss of DNSSEC root keys

**Historic photo of the 1st Root Key Signing Key Ceremony
16 June 2010**

Source: IANA

- Unlikely, bordering on impossible

Overview of DNS insecurity

Architectural vulnerabilities		Implementation weaknesses	Human errors
DRDoS	pDNS	AXFR	typo-squatting
Kaminsky	NSEC	DNS tunneling	drop-catching
root NS	NSEC3	DNS rebinding	domain hijacking
altDNS	CT	DNSaaS	NS reclamation
web3 DNS	.zip, …		DNSSEC root keys

Source: Possible Security

Thank you for your attention!

Any questions?

Content curated by Kirils Solovjovs
@k@chaos.social | https://kirils.org

possible.lv
IT security services

possible@possible.lv
+371 26036916