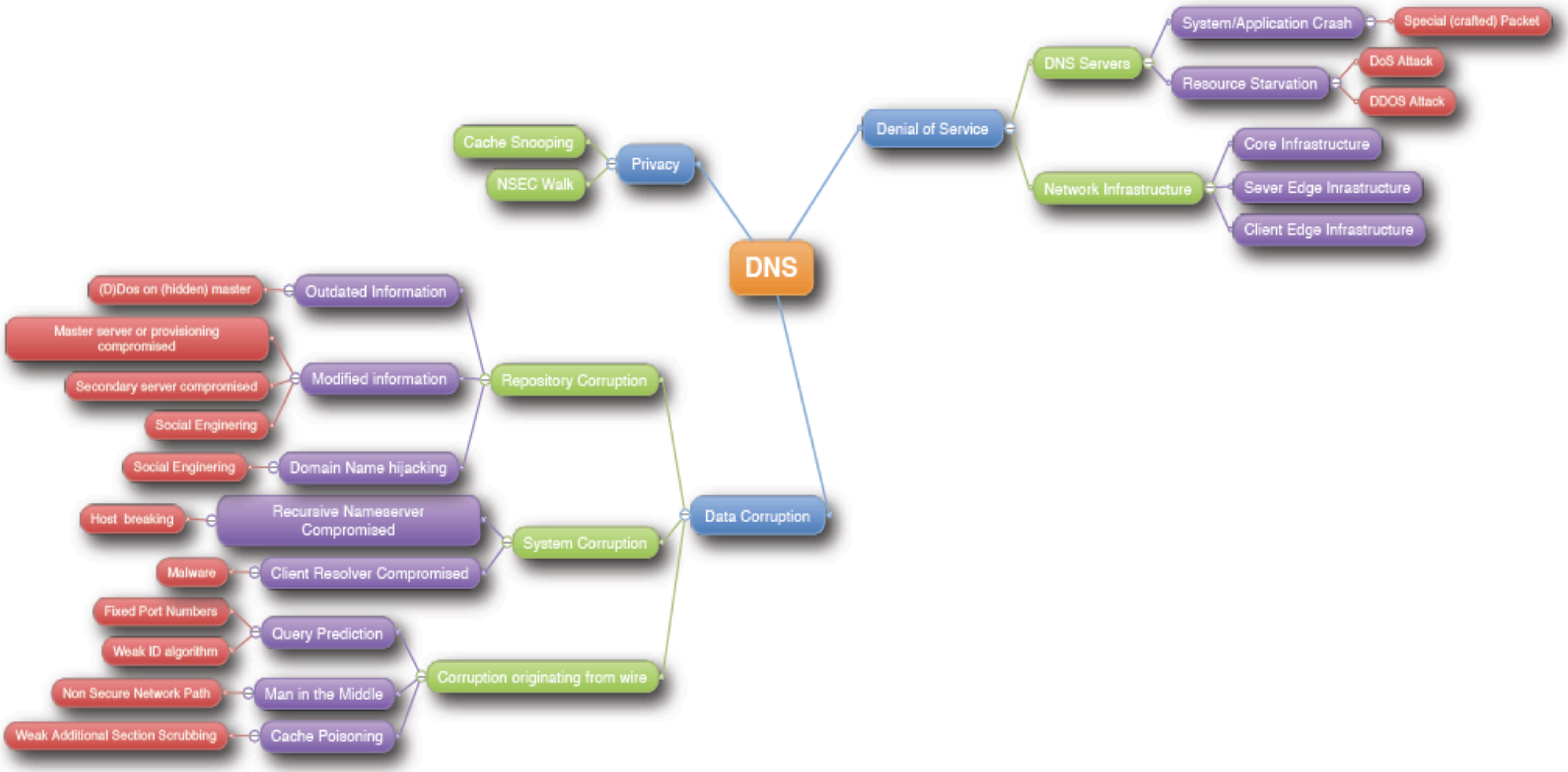
DNSSEC: Kā? un Kāpēc?

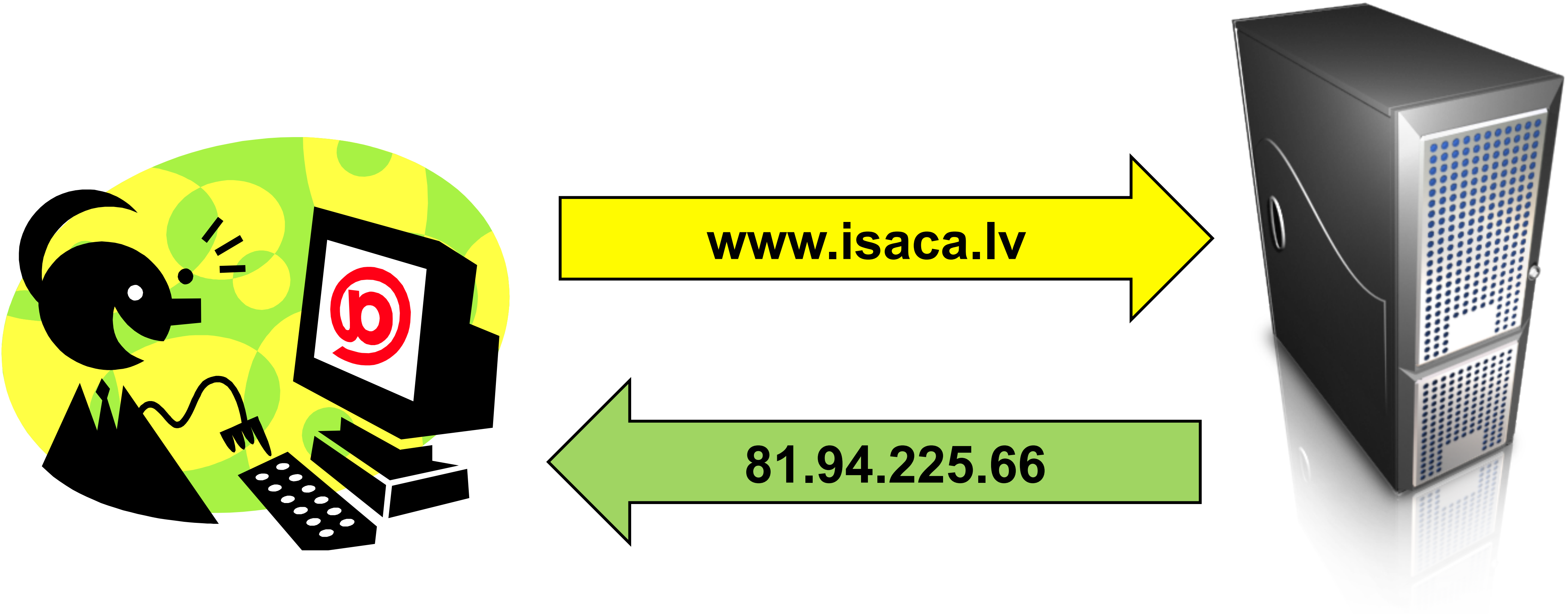
Ivo Ķutts, Katrina Sataki, NIC.LV

ISACA konference, 2012.gada 8.novembrī

DNS ievainojamības

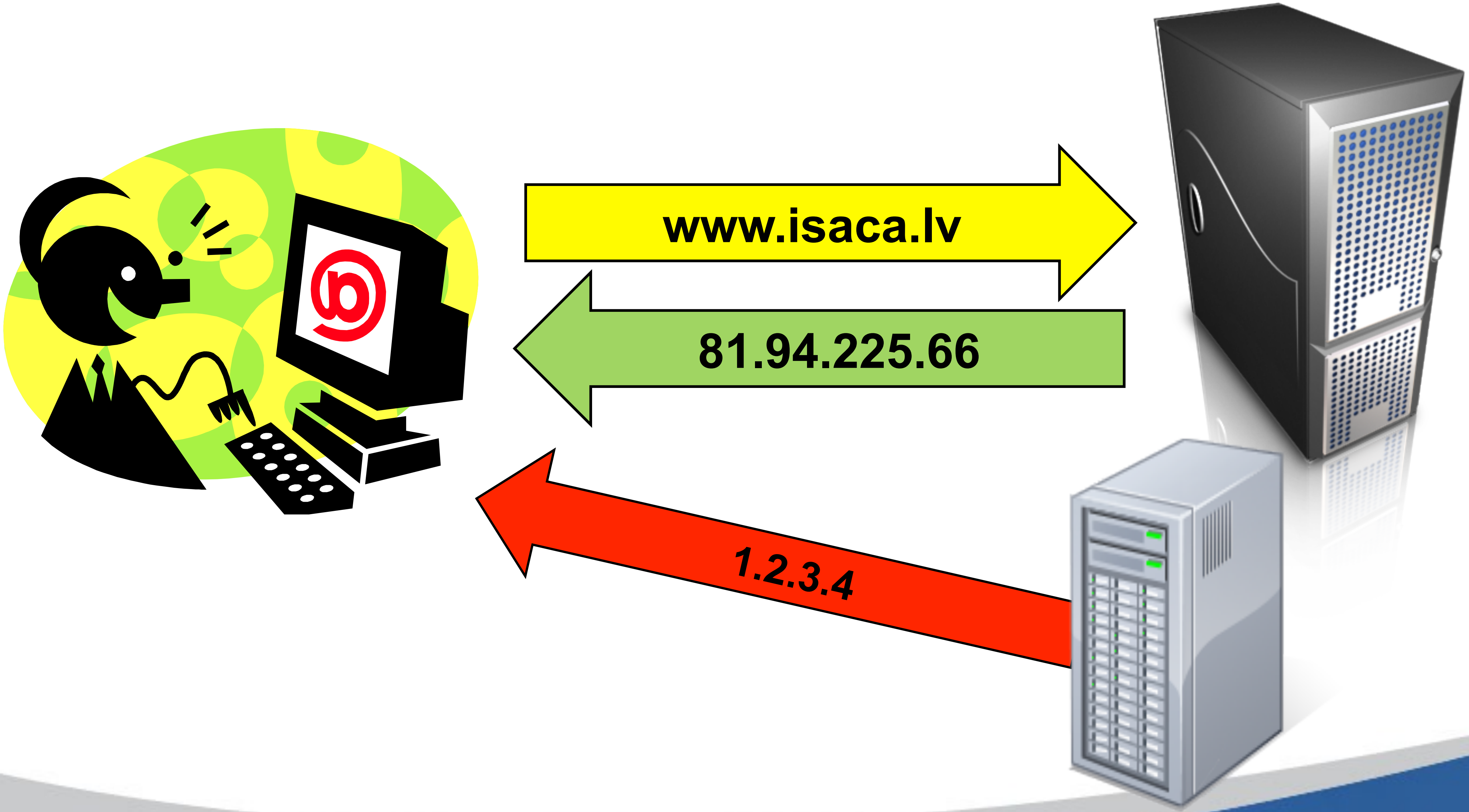


- DNS
  - Privacy
    - Cache Snooping
    - NSEC Walk
  - Denial of Service
    - DNS Servers
      - System/Application Crash
        - Special (crafted) Packet
      - Resource Starvation
        - DoS Attack
        - DDOS Attack
    - Network Infrastructure
      - Core Infrastructure
      - Sever Edge Inrastructure
      - Client Edge Infrastructure
  - Data Corruption
    - Repository Corruption
      - Outdated Information
        - (D)Dos on (hidden) master
      - Modified information
        - Master server or provisioning compromised
        - Secondary server compromised
        - Social Enginering
      - Domain Name hijacking
        - Social Enginering
    - System Corruption
      - Recursive Nameserver Compromised
        - Host breaking
      - Client Resolver Compromised
        - Malware
    - Corruption originating from wire
      - Query Prediction
        - Fixed Port Numbers
        - Weak ID algorithm
      - Man in the Middle
        - Non Secure Network Path
      - Cache Poisoning
        - Weak Additional Section Scrubbing



www.isaca.lv

81.94.225.66



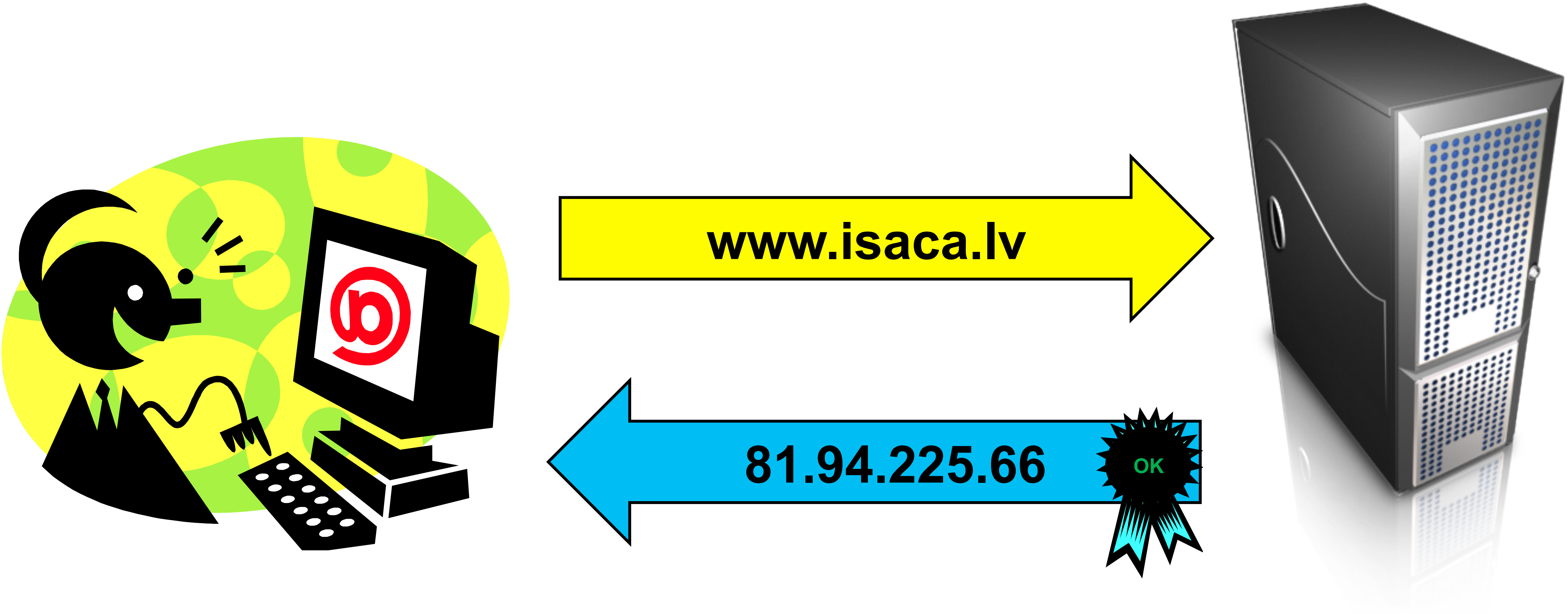
www.isaca.lv

81.94.225.66

1.2.3.4

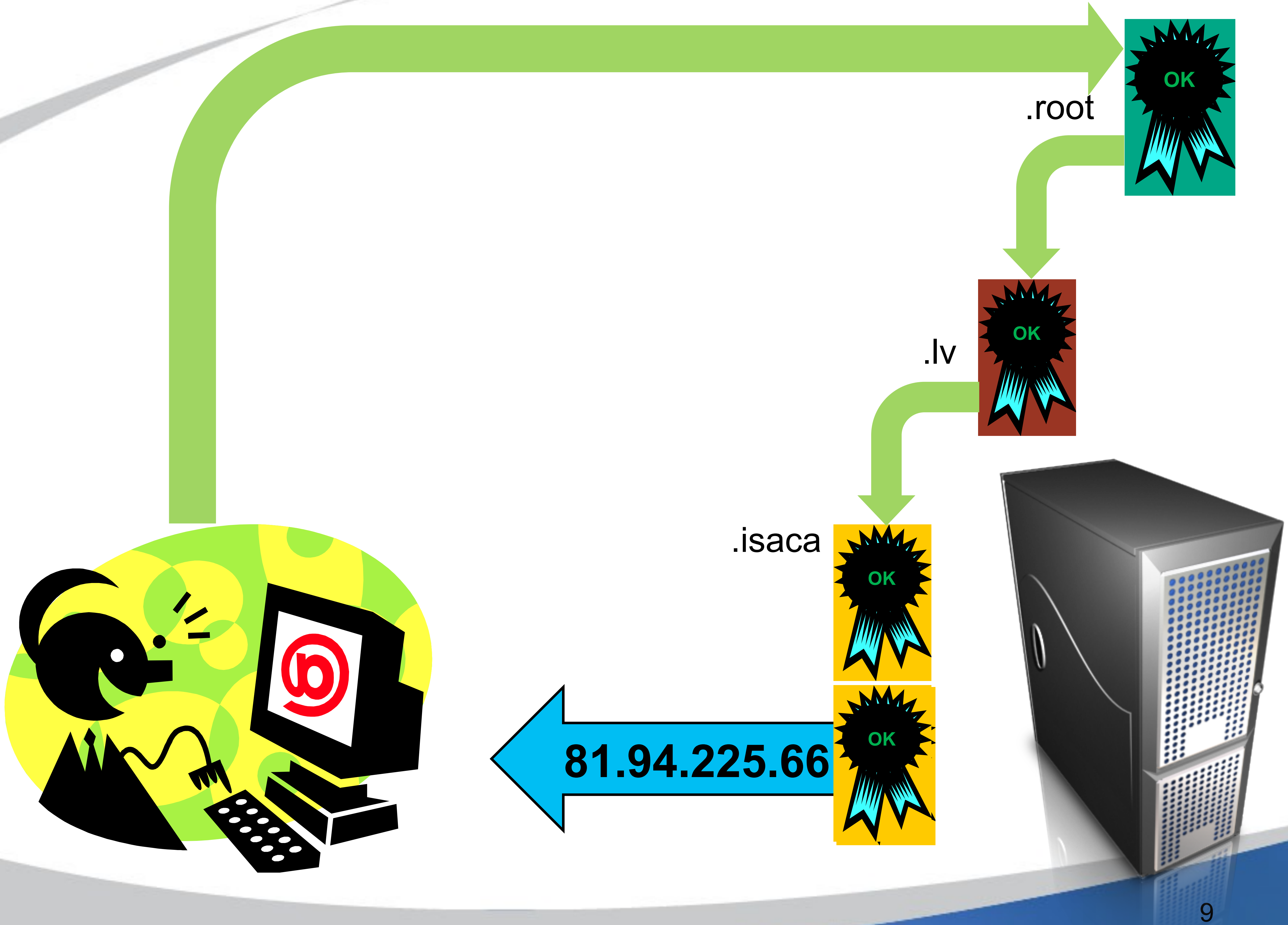
Kas ir un ko dara DNSSEC?

DNS Security Extensions



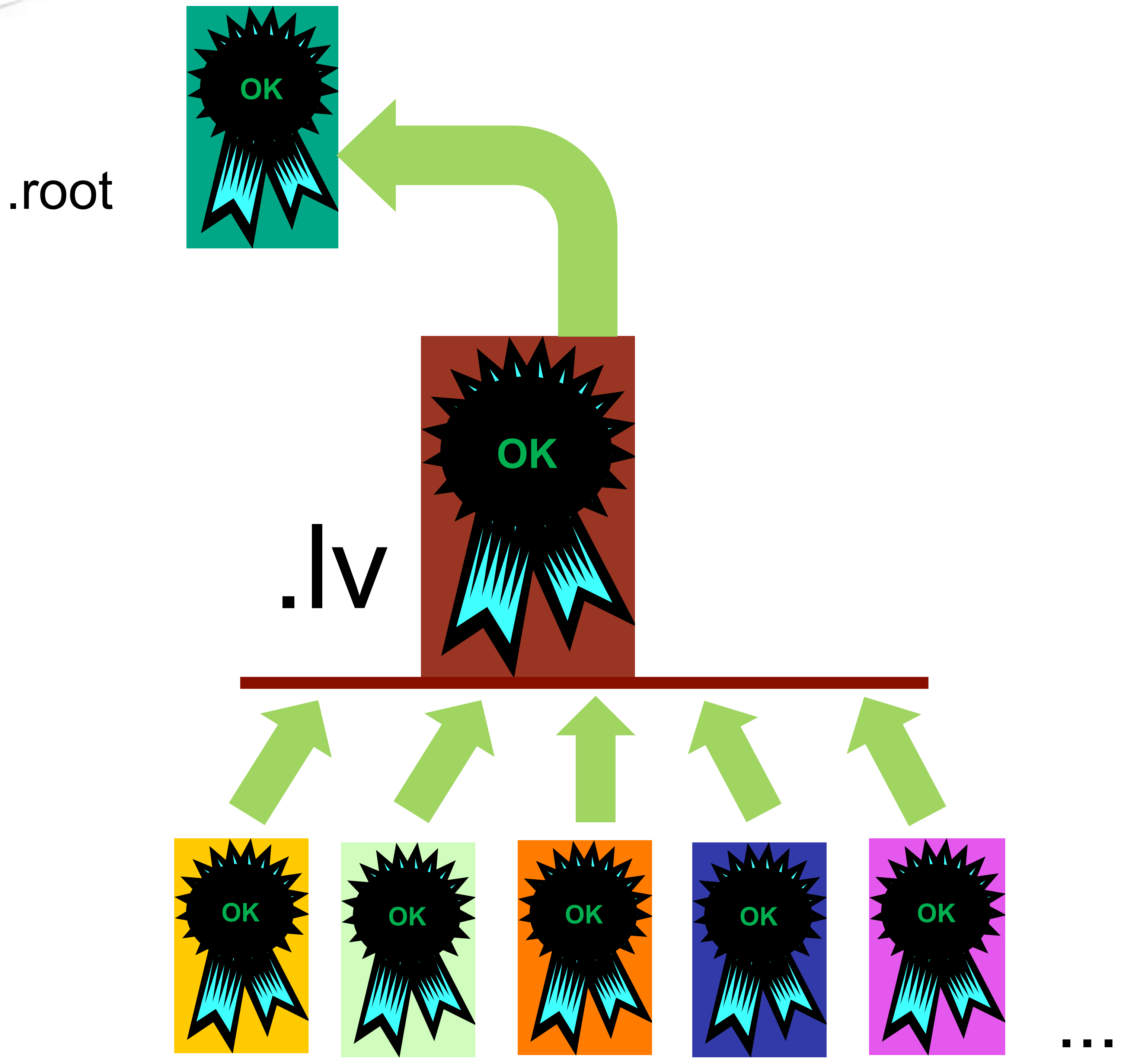
www.isaca.lv

81.94.225.66


OK
.root
OK
.lv
.isaca
OK
OK
81.94.225.66

DNSEC ≠ PKI

DNSSEC darbībā



.root

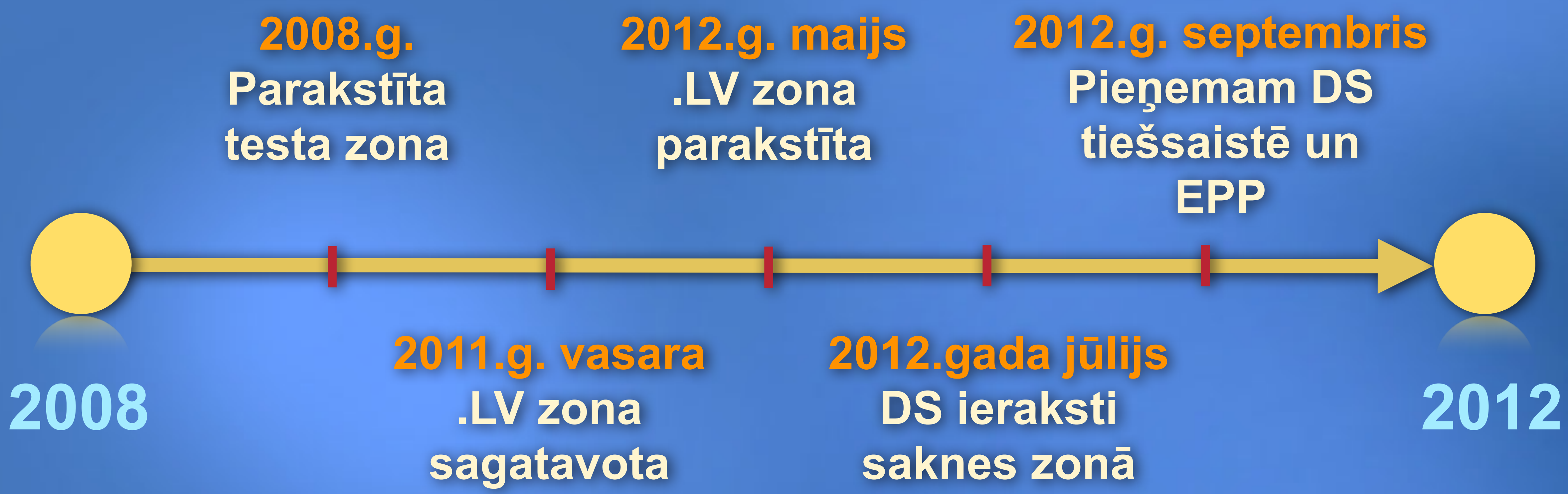
.lv

...

316 domēni saknes zonā

103 parakstīti

96 DS ieraksti saknes zonā



2008

2008.g.
Parakstīta
testa zona

2011.g. vasara
.LV zona
sagatavota

2012.g. maijs
.LV zona
parakstīta

2012.gada jūlijs
DS ieraksti
saknes zonā

2012.g. septembris
Pieņemam DS
tiešsaistē un
EPP

2012

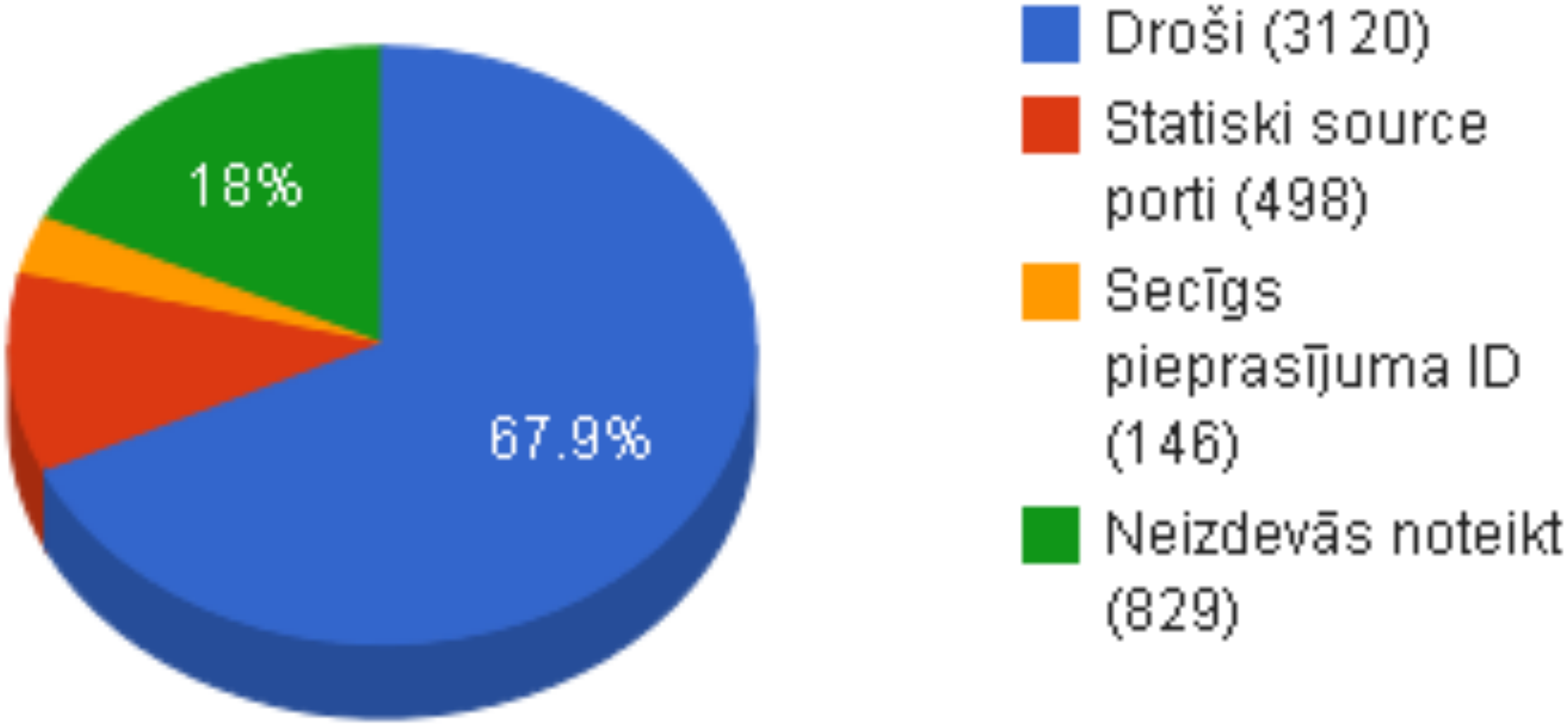
Vai DNSSEC tiešām ir vajadzīgs?

~ 4500 kešdarbes atrisinātāji

~13% potenciāli ievainojami

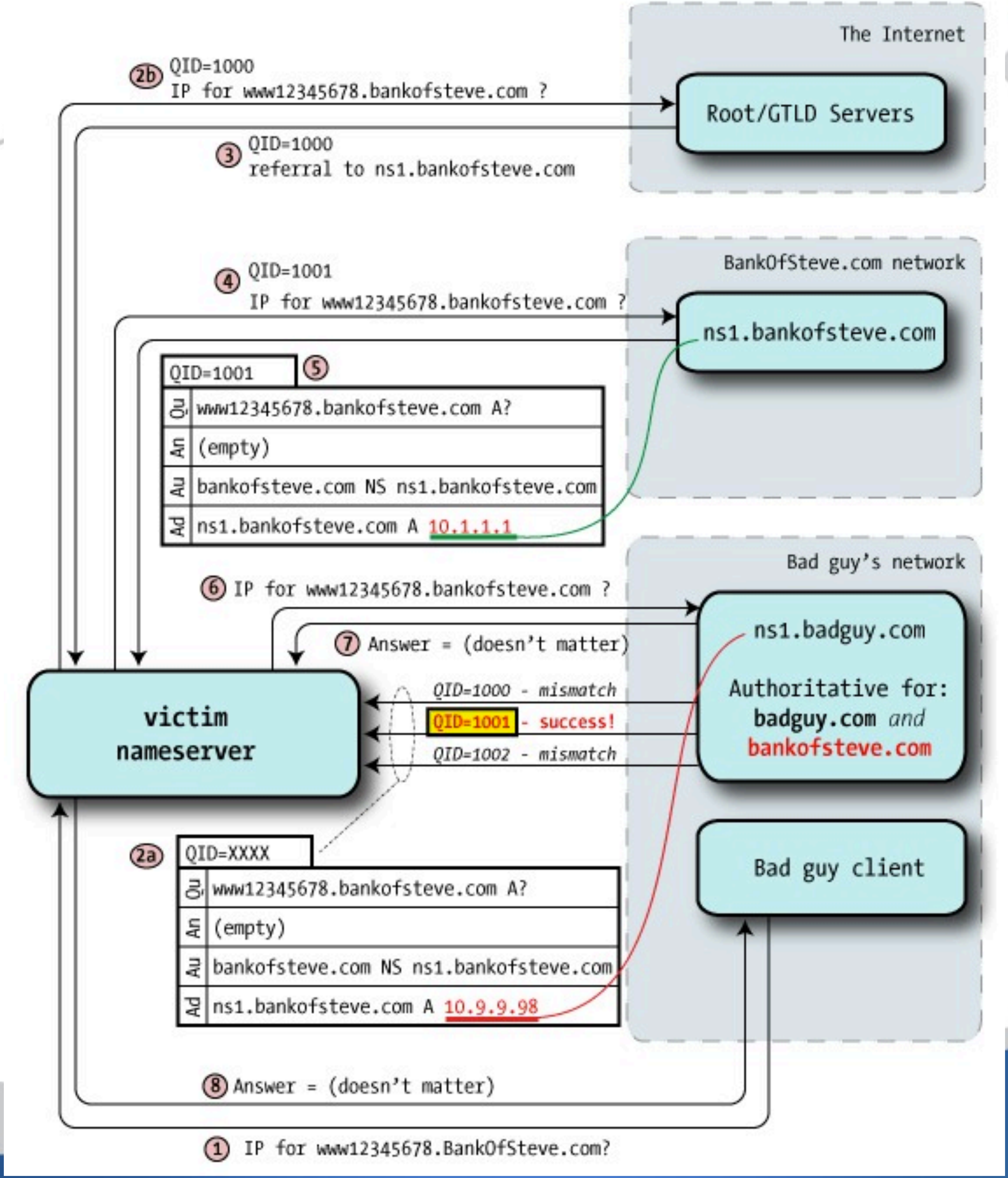
177 atvērti

Drošu un potenciāli nedrošu DNS serveru īpatsvars



DNS pakešu viltošana

- DNS *cache* informācijas viltošana, paredzot DNS paketes elementus:
  - secīgs DNS pieprasījuma ID (query id)
  - secīgs DNS *source* ports



The Internet

Root/GTLD Servers

(2b) QID=1000
IP for www12345678.bankofsteve.com ?

(3) QID=1000
referral to ns1.bankofsteve.com

BankOfSteve.com network

ns1.bankofsteve.com

(4) QID=1001
IP for www12345678.bankofsteve.com ?

(5)

QID=1001	
Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.1.1.1

Bad guy's network

(6) IP for www12345678.bankofsteve.com ?

(7) Answer = (doesn't matter)

ns1.badguy.com

Authoritative for:
badguy.com *and*
bankofsteve.com

victim
nameserver

QID=1000 - mismatch

QID=1001 - success!

QID=1002 - mismatch

Bad guy client

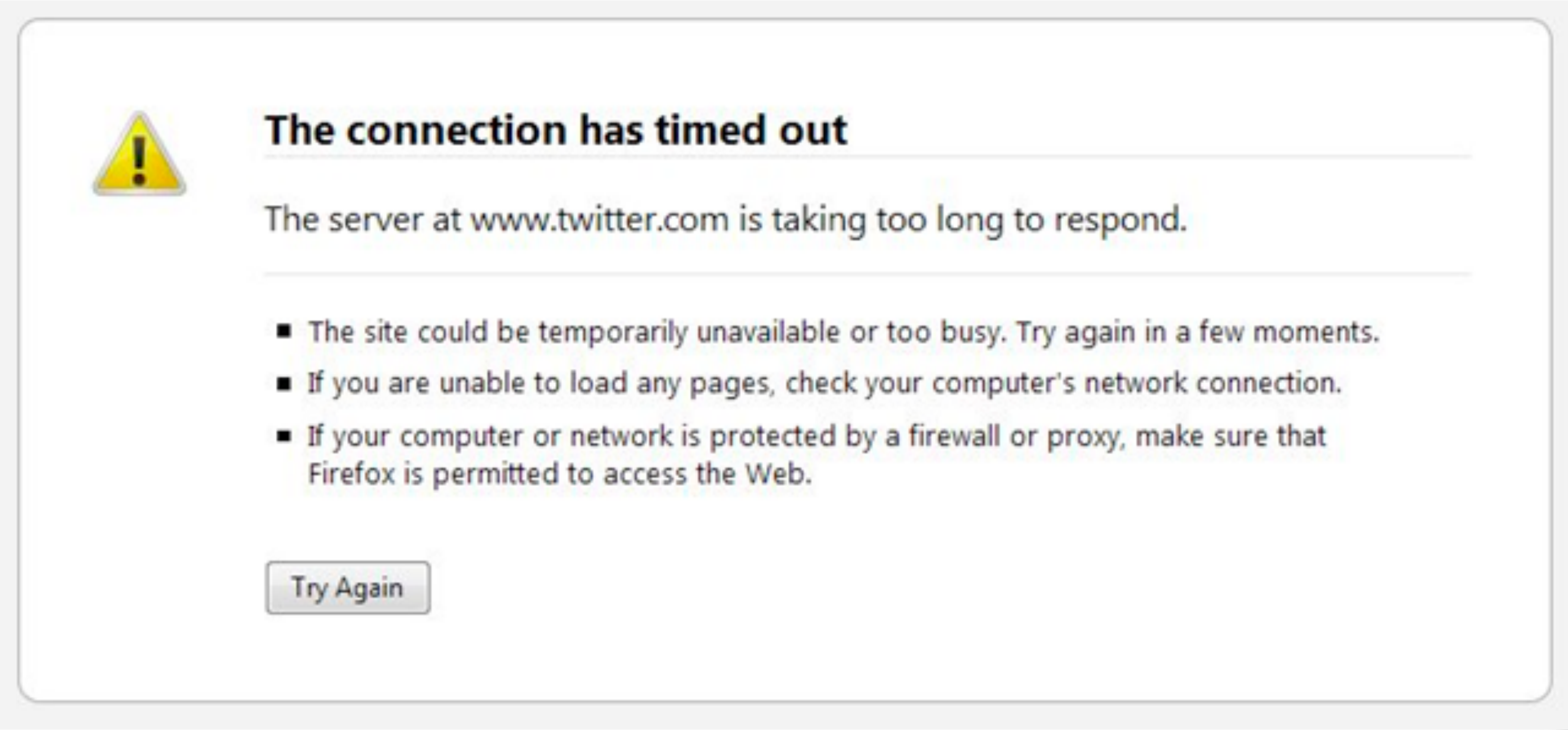
(2a)

QID=XXXX	
Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.9.9.98

(8) Answer = (doesn't matter)

(1) IP for www12345678.BankOfSteve.com?

Twitter



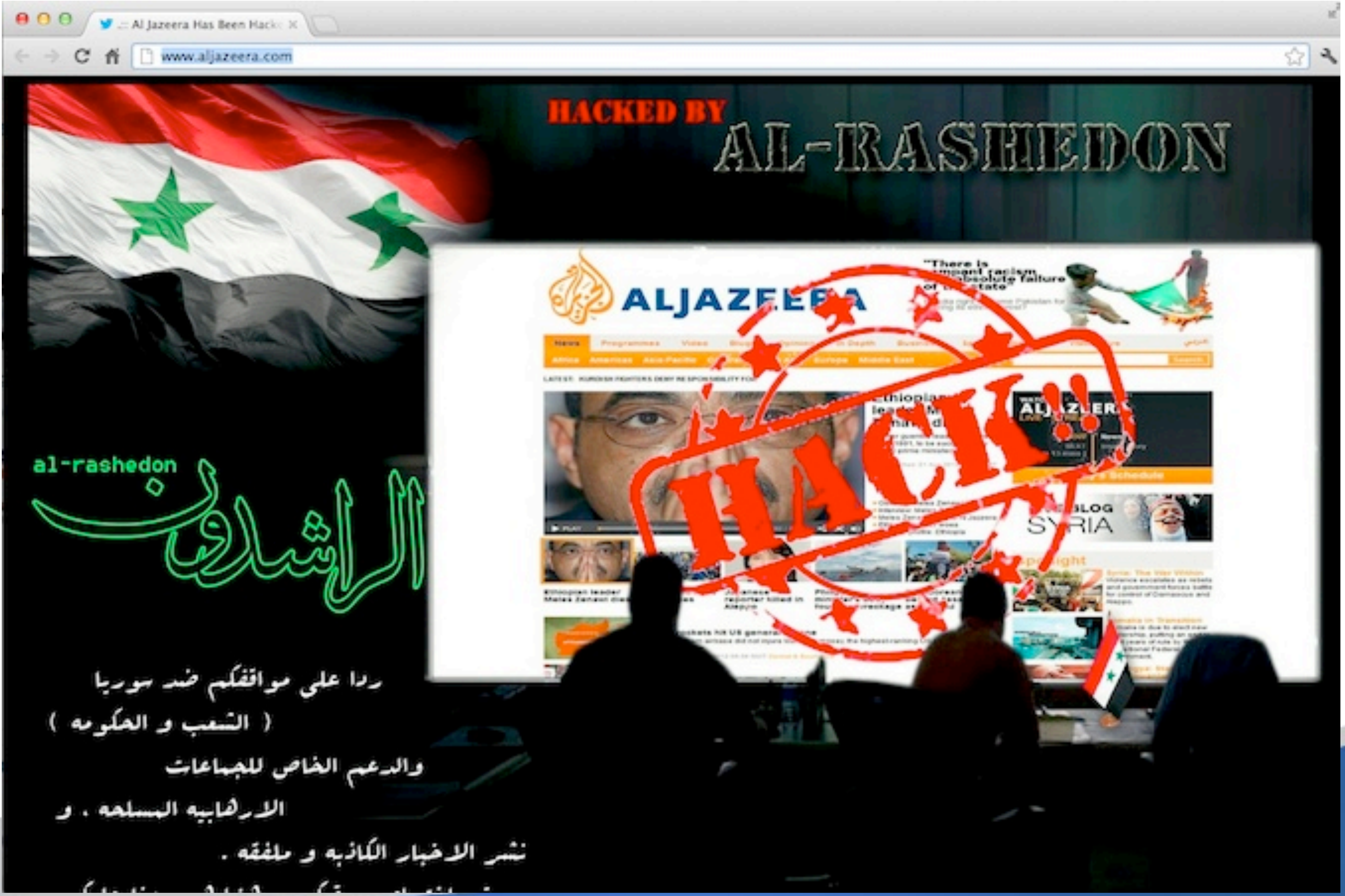
The connection has timed out

The server at www.twitter.com is taking too long to respond.

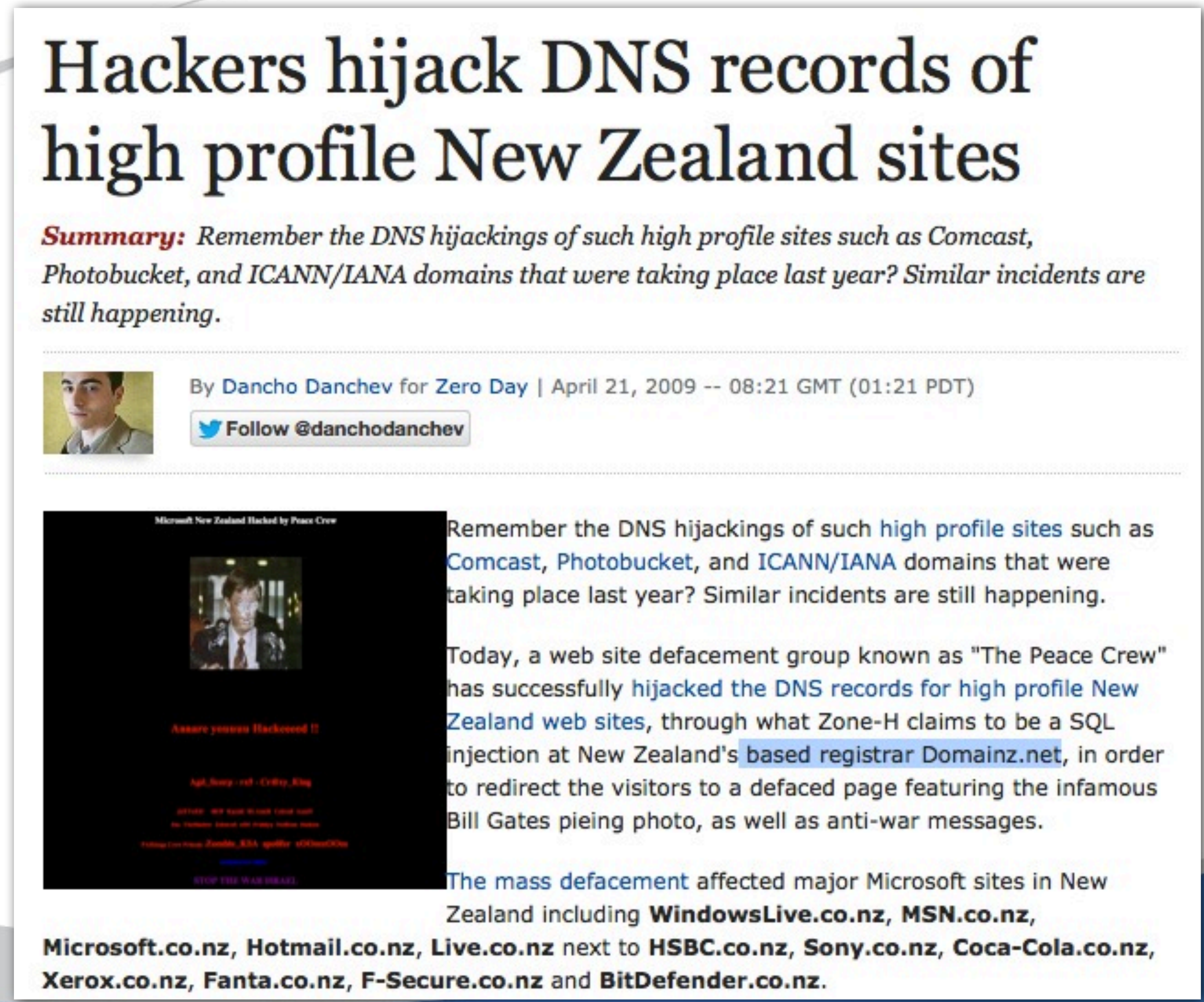
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Google

Al Jazeera



ردا على موافقكم ضد سوريا
(الشعب و الحكومه)
والدعم الخاص للجماعات
الارهابيه المسلحه . و
نشر الاخبار الكاذبه و ملفقه .



Hackers hijack DNS records of high profile New Zealand sites

Summary: Remember the DNS hijackings of such high profile sites such as Comcast, Photobucket, and ICANN/IANA domains that were taking place last year? Similar incidents are still happening.

By Dancho Danchev for Zero Day | April 21, 2009 -- 08:21 GMT (01:21 PDT)

Follow @danchodanchev

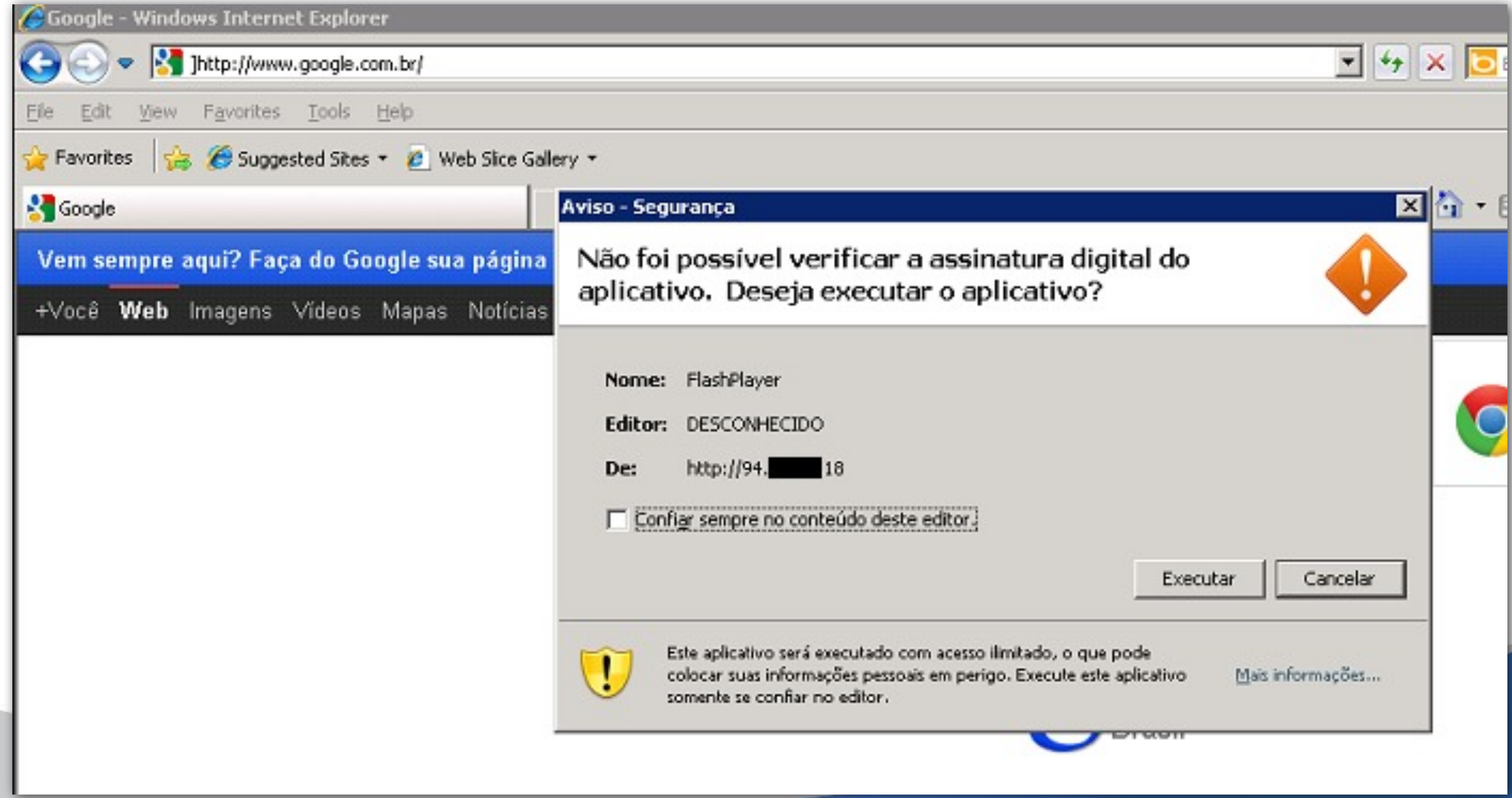
Microsoft New Zealand Hacked by Peace Crew
Aaaare youuuu Hackeeeed !!
Agd_Scorp - cr0 - Cr4zy_King
STOP THE WAR ISRAEL

Remember the DNS hijackings of such high profile sites such as Comcast, Photobucket, and ICANN/IANA domains that were taking place last year? Similar incidents are still happening.

Today, a web site defacement group known as "The Peace Crew" has successfully hijacked the DNS records for high profile New Zealand web sites, through what Zone-H claims to be a SQL injection at New Zealand's based registrar Domainz.net, in order to redirect the visitors to a defaced page featuring the infamous Bill Gates pieing photo, as well as anti-war messages.

The mass defacement affected major Microsoft sites in New Zealand including **WindowsLive.co.nz**, **MSN.co.nz**, **Microsoft.co.nz**, **Hotmail.co.nz**, **Live.co.nz** next to **HSBC.co.nz**, **Sony.co.nz**, **Coca-Cola.co.nz**, **Xerox.co.nz**, **Fanta.co.nz**, **F-Secure.co.nz** and **BitDefender.co.nz**.

Brazīlijas IPS DNS



Aviso - Segurança

Não foi possível verificar a assinatura digital do aplicativo. Deseja executar o aplicativo?

Nome: FlashPlayer

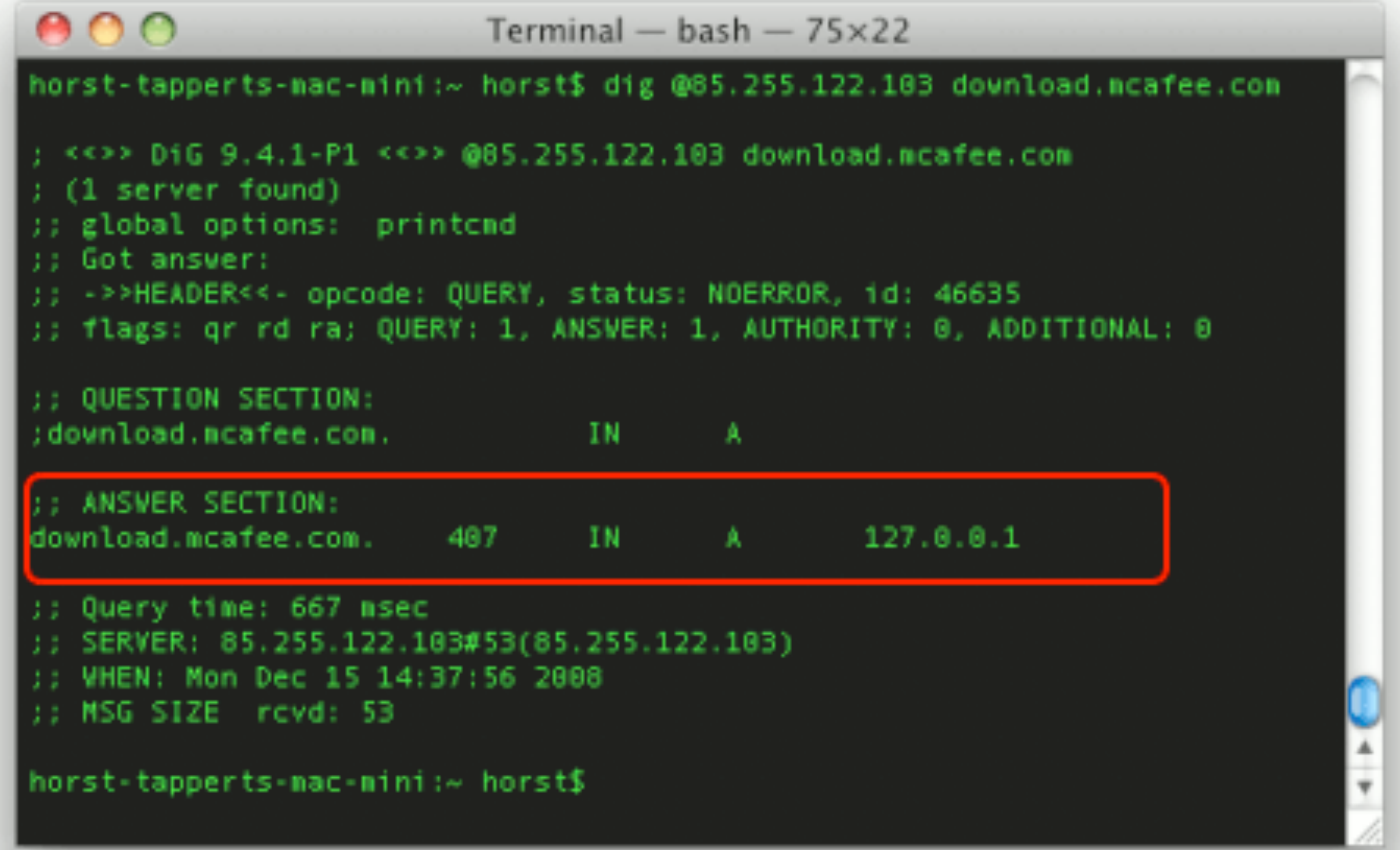
Editor: DESCONHECIDO

De: http://94.[redacted]18

□ Confiar sempre no conteúdo deste editor.

Este aplicativo será executado com acesso ilimitado, o que pode colocar suas informações pessoais em perigo. Execute este aplicativo somente se confiar no editor.

Vai DNSSEC palīdzētu pret DNSChanger?



Terminal — bash — 75×22

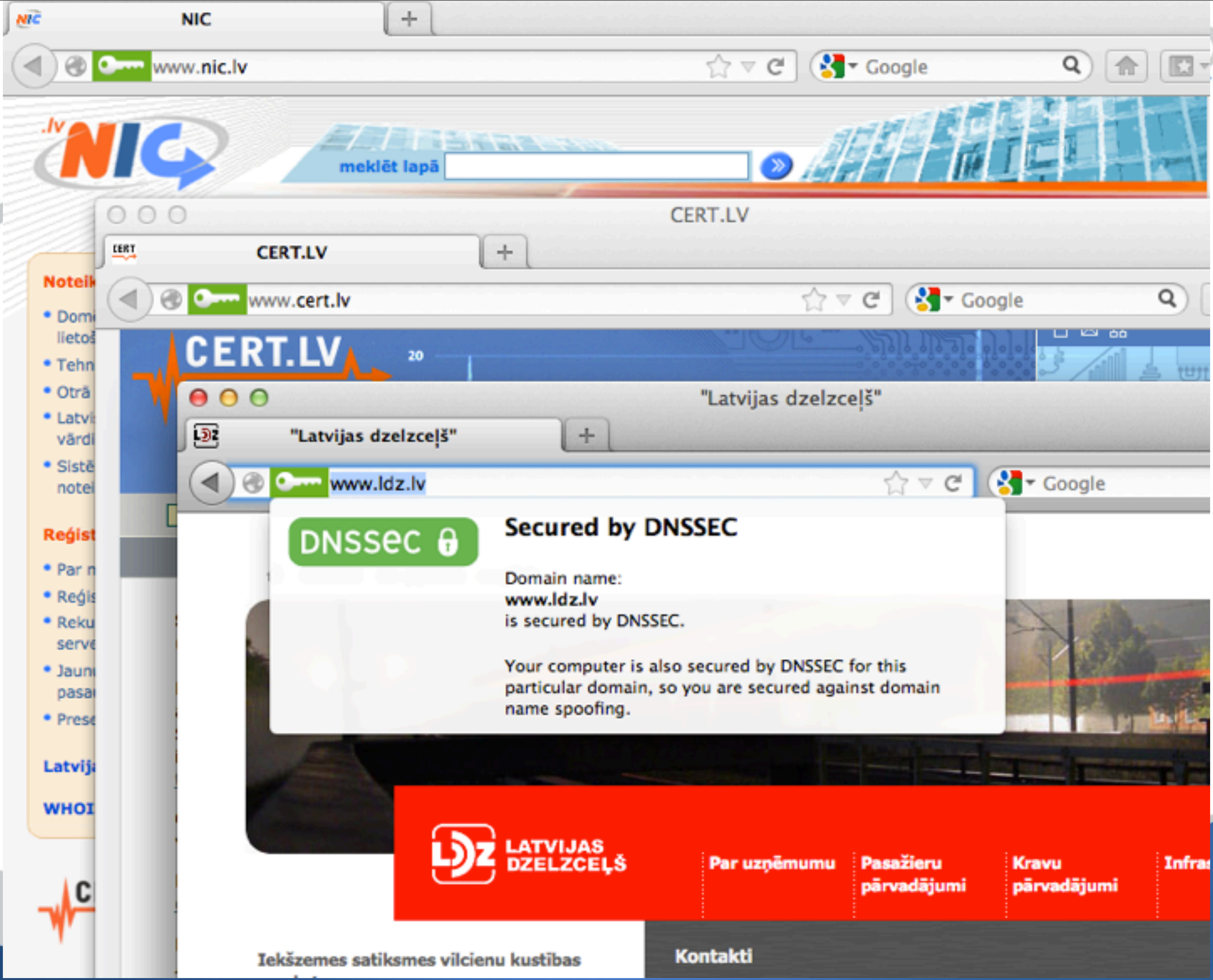
```
horst-tapperts-mac-mini:~ horst$ dig @85.255.122.103 download.mcafee.com

; <<>> DiG 9.4.1-P1 <<>> @85.255.122.103 download.mcafee.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46635
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;download.mcafee.com.           IN      A

;; ANSWER SECTION:
download.mcafee.com.    407     IN      A       127.0.0.1

;; Query time: 667 msec
;; SERVER: 85.255.122.103#53(85.255.122.103)
;; WHEN: Mon Dec 15 14:37:56 2008
;; MSG SIZE  rcvd: 53

horst-tapperts-mac-mini:~ horst$
```

Aizsardzība

- Servera source porta un DNS transakcijas ID randomizācija
- Nejauši lielie burti domēna vārdā, 0x20
- DNSSEC

Citi labumi

- DANE - TLSA
- SSHFP
- DKIM
- IPSECKEY



Secured by DNSSEC

Domain name:
www.ldz.lv
is secured by DNSSEC.

Your computer is also secured by DNSSEC for this particular domain, so you are secured against domain name spoofing.

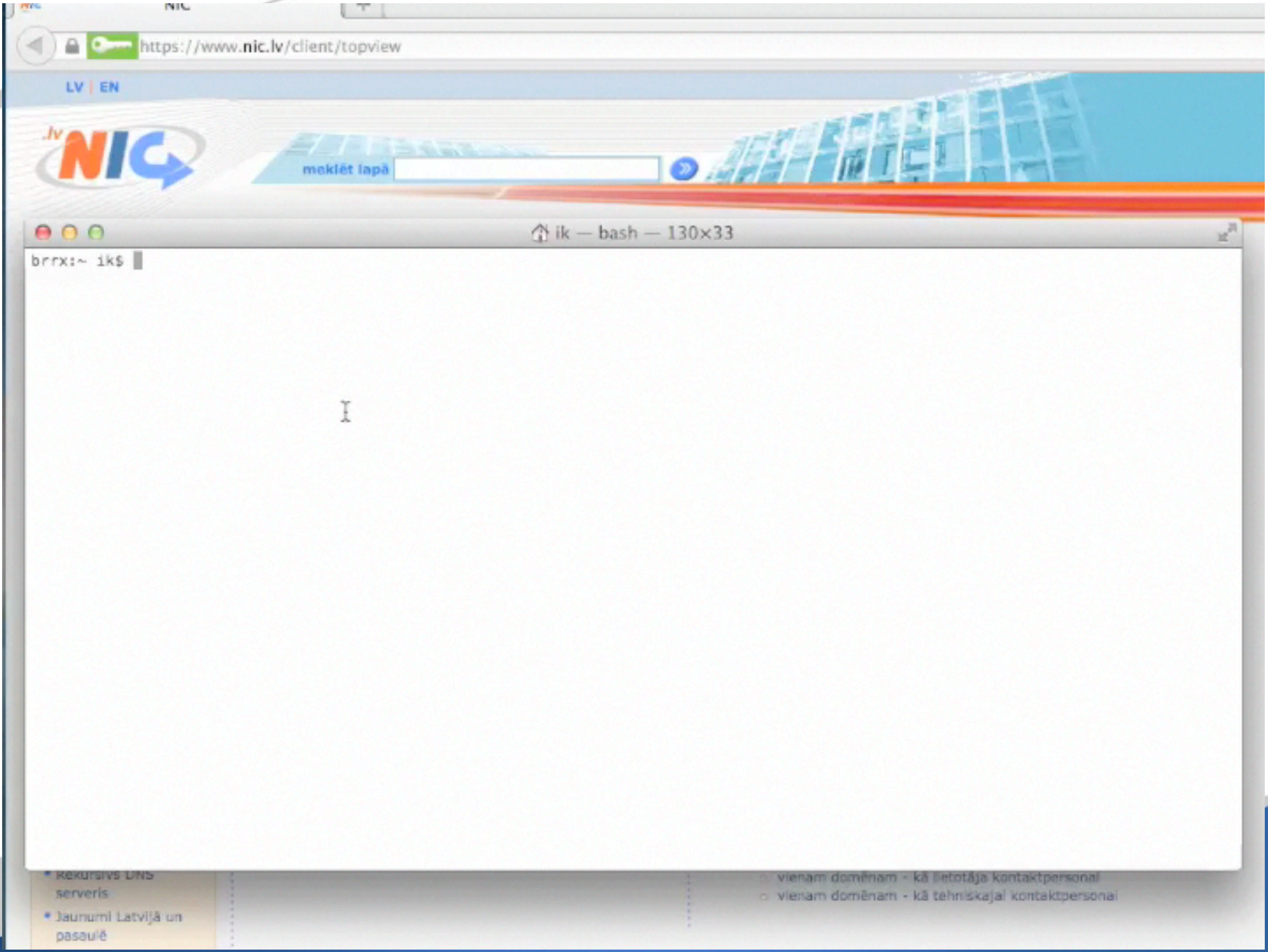
DNSSEC rīki

DNSSEC risinājumi: bezmaksas

- Bind > 9.7 + *(www.isc.org)*
- NSD + ldns-tools *(www.nlnetlabs.nl)*
- Yadifa (Eurid)
- Knot DNS (.cz)
- PowerDNS *(www.powerdns.com)*
- OpenDNSSEC + SoftHSM *(www.opendnssec.org)*
- ZKT *(http://www.hznet.de/dns/zkt/)*
- Dnssec-tools *(www.dnssec-tools.org)*

DNSSEC risinājumi: komerciālie

- BlueCoat,
- Infoblox,
- Secure64,
- Xelerance,
- MS Windows 2008 R2

NIC
https://www.nic.lv/client/topview
LV | EN
meklēt lapā
ik — bash — 130×33

```
brrx:~ ik$ 
```

Rekursīvs DNS serveris
Jaunumi Latvijā un pasaulē
vienam domēnam - kā lietotāja kontaktpersonai
vienam domēnam - kā tehniskajai kontaktpersonai

Papildus nepieciešams

- regulāri atjaunot RRSIG
- mainīt un glabāt KSK un ZSK

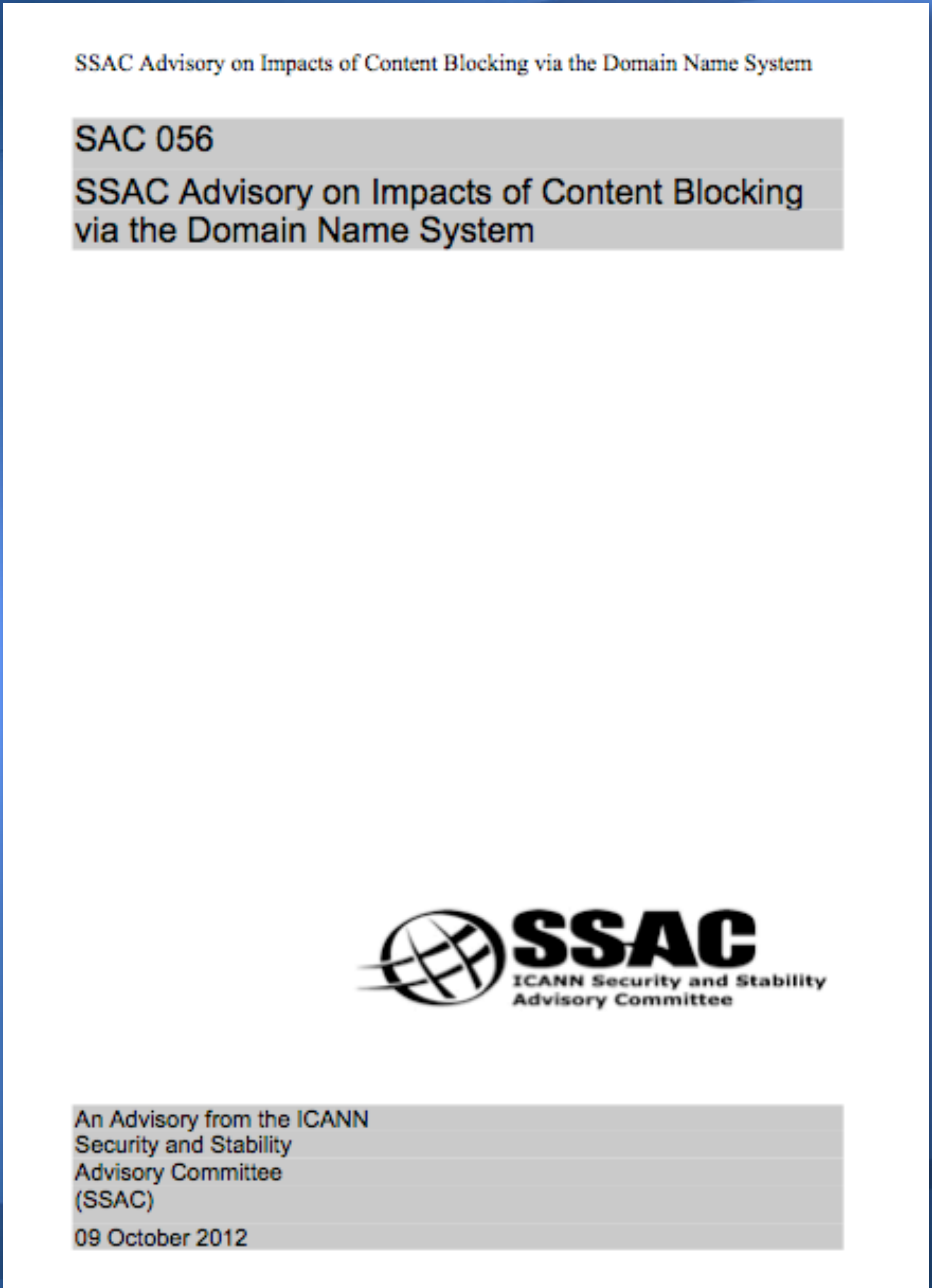
DNSSEC rīki: tiešsaiste

- http://dnsviz.net - dnssec saišu un problēmu vizualizēšanai
- http://dnscog.com – vispārējs DNS tests, kas iekļauj arī DNSSEC pārbaudi
- http://dnssec-debugger.verisignlabs.com
- http://www.dnssecmonitor.org

DNSSEC rīki

- http://www.nlnetlabs.nl/projects/ldns/ - ldns-verify-zone – pārbauda parakstīto zonas failu
- http://www.opendnssec.org - auditor modulis (ruby)
- http://www.verisignlabs.com/dnssec-tools/ - (DNSjava)
- https://github.com/dotse/dnssec-monitor - (perl)
- http://yazvs.verisignlabs.com - šo Verisign lietojot savu zonu pārbaudēm pirms publicēšanas (perl)
- http://www.vantage-points.org/index.html - Monitorē DS un dnskey atbilstību atslēgu rotēšanas procesā (c++)
- https://github.com/bortzmeyer/key-checker - key rollover monitorēšanas skripts (python)
- https://github.com/jpmens/nagval - nagios spraudnis (c)

Un vēl...



SAC 056

SSAC Advisory on Impacts of Content Blocking via the Domain Name System

SSAC
ICANN Security and Stability Advisory Committee

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)

09 October 2012

Paldies par uzmanību!

Jautājumi?

ivo@nic.lv, katrina@nic.lv