DNSSEC pro běžného uživatele

Ondřej Caletka

6. června 2015

Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O sdružení CESNET

edu ID cz

eduroam

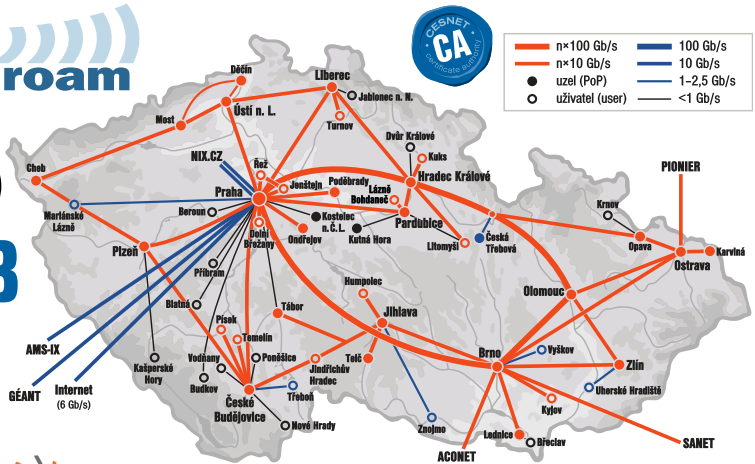
CESNET CSIRTS

CESNET CA

Mentat

LAB

Warden



CESNET DataCare

MetaCentrum

UltraGrid

Mezi uživateli je rozšířeno mnoho **polopravd, omylů a mýtů** o tom, jak funguje systém DNS a jeho rozšíření DNSSEC. Propadají pak mylnému dojmu, že DNSSEC nic neřeší a že se jím nemá cenu zabývat.

Opak je pravdou

- DNS je klíčovým prvkem architektury Internetu, jak ho známe
- na jeho bezchybné funkčnosti závisí všechny[1] internetové služby
- přitom je náchylný k *nedetekovatelné* manipulaci
- jediný úspěšný útok může unést celé části DNS stromu (třeba `.com`)
- šíření malwaru pomocí falešných domén se `pravidelně objevuje`
- DNSSEC **jedinou možností** jak manipulaci detekovat

[1] Skype se nepočítá ☺

Příklady únosů DNS

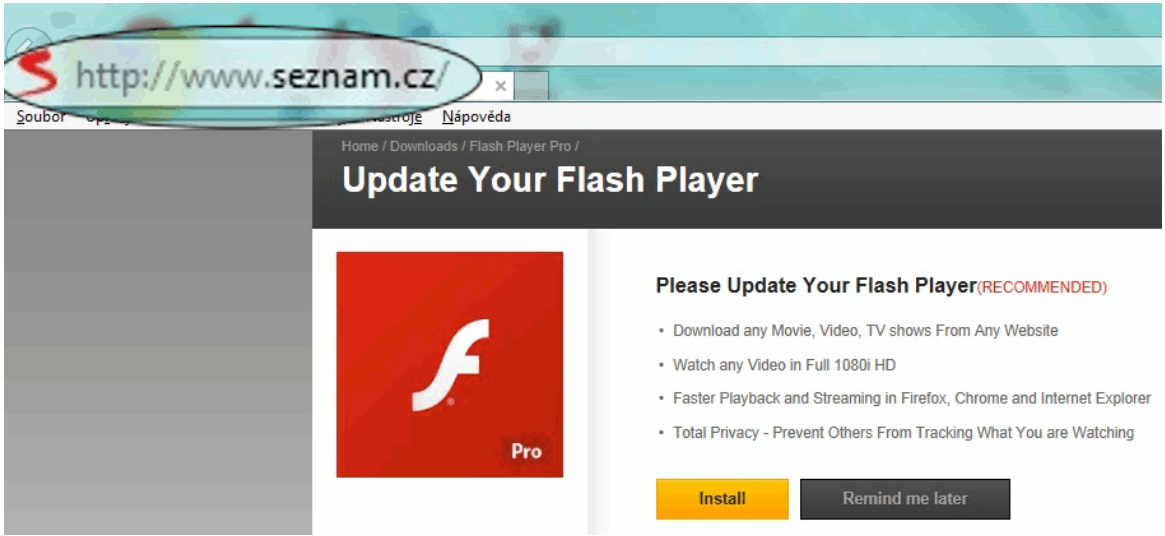
DNSchanger

- trojský kůň pro Windows
- aktivní 2007 – 2011
- změnil nastavení rekurzivních DNS serverů v OS
- přidával reklamy do webových stránek

`rom-0` exploit

- útok na levné domácí routery
- změna adresy rekurzivního DNS serveru v routeru
- náhrada populárních stránek za výzvu k upgradu Flash přehrávače

Oběť změny DNS



Co je vlastně DNSSEC

- systém end-to-end zabezpečení autenticity DNS zpráv
- majitel domény podepisuje, kdokoli může validovat
- hierarchická delegace důvery
  - v nadřazené zóně je umístěn otisk klíče (DS záznam)
  - otisk klíče kořenové zóny je součástí výbavy každého validátoru
- i u nepodepsané domény probíhá validace nadřazených zón
  - až po podepsanou informaci, že další zóny podepsány nejsou

DNSSEC detekuje, ale neopravuje

Součástí specifikace DNSSEC není **křišťálová koule**. Validátory manipulaci detekují, ale nejsou schopny zmanipulovaná data opravit.

Nejčastější příčiny nevalidních DNS dat:

- zastaralé verze rekurzivních DNS serverů
- nevhodné konfigurace firewallů
- captive portály
- chyba na straně držitele domény

Máme přece TLS

- DNSSEC chrání pouze překlad doménového jména na IP adresu, proti odklonění IP provozu je neúčinný
- je tedy nezbytné používat TLS s DNSSECem
- správně implementované TLS dokáže detekovat i únos DNS
- PKI model má však vážné trhliny
- DNSSEC je nezávislý bezpečný kanál
- spolehlivě ochrání přinejmenším proti *vzdálenému* útočníkovi

DNSSEC + TLS = DANE

- důvěryhodnost TLS spojení je dnes výlučně závislá na soustavě certifikačních autorit
- DNSSEC je důvěryhodný nezávislý kanál, kterým může majitel domény publikovat různé informace
- TLSA záznamy umožňují publikovat otisky TLS certifikátů
- výhledově nahradí *Domain Control Validated* TLS certifikáty

Jak validovat

Validace v prohlížeči

- rozšíření DNSSEC a TLSA validátor
- obsahuje kompletní DNSSEC resolver
- kontroluje, zda se prohlížeč připojuje na správnou adresu
- nezasahuje do validace TLS spojení v prohlížeči

Validace na domácím routeru

- stačí aktuální BIND nebo Unbound
- konfigurace je obvykle připravena, stačí vložit klíč kořenové zóny
- režim plné rekurze nebo forwardování na nadřazený DNS server
  - problémy s chybami v nadřazených serverech znemožňující validaci některých jmen
  - režim plné rekurze špatně škáluje, vyžaduje nezasahování ISP do udp/53 provozu

Problém poslední míle

- DNSSEC z principu nechrání před útokem na poslední míli mezi validátorem a konzumentem
- specifikace nařizuje bezpečný kanál
- jsou-li pochybnosti o bezpečnosti kanálu, je nutné kritická data znovu validovat
- validace na vzdáleném serveru hlavně chrání server před otrávením své vlastní cache

Resolver na loopbacku

- snadné pro pevné instalace, obtížné pro přenosná zařízení
  - filtrovaný DNS provoz
  - přesměrování DNS provozu na polofunkční server
  - *captive portály* blokující konektivitu do přihlášení
- experimentální DNSSEC Trigger
  - automatizovaně otestuje použitelnost místního resolveru
  - podle výsledku nastaví lokální unbound na forwardování nebo plnou rekurzi
  - hot spot režim pro přihlášení ke captive portálům
  - nouzové tunelování DNS přes TLS portem `tcp/443`

Problém řetězení resolverů s DNSSEC

- problematická validace žolíkových domén
- chyba v nadřazeném BIND < 9. 9. 0
- automatizovaný test na `http://wildcarddnssec.jdem.cz/`

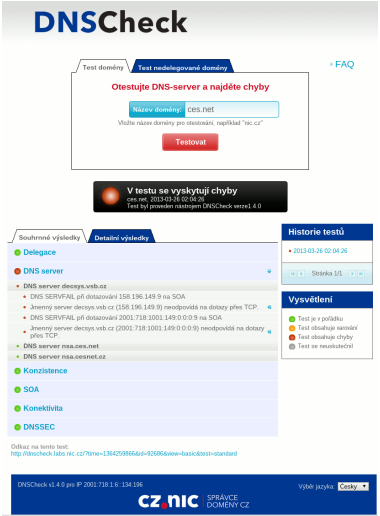
	Test	Výsledek testu
1.	Zabezpečení DNSSEC `*.wilda.rhybar.0skar.cz`	Úspěch. Nedostanete se na doménová jména s neplatným podpisem.
2a.	NSEC zóna s A záznamem `*.wilda.nsec.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *A záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC.
2b.	NSEC zóna s CNAME záznamem `*.wild.nsec.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *CNAME záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC.
3a.	NSEC3 zóna s A záznamem `*.wilda.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *A záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
3b.	NSEC3 zóna s CNAME záznamem `*.wild.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *CNAME záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
4.	NSEC s extra záznamem uvnitř žolíku `www.wilda.nsec.0skar.cz`	Úspěch. Váš DNS server správně validuje *CNAME záznam*, obklopený žolíkovými *A záznamy* na zóně s NSEC.
5.	NSEC3 s extra záznamem uvnitř žolíku `www.wilda.0skar.cz`	Úspěch. Váš DNS server správně validuje *CNAME záznam*, obklopený žolíkovými *A záznamy* na zóně s NSEC3.

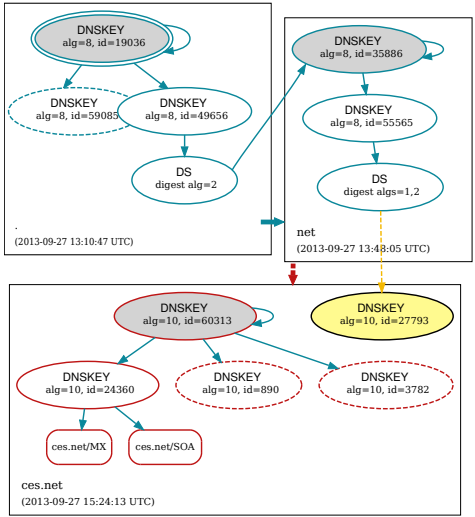
Když něco nefunguje

- selhání validace server signalizuje návratovým kódem SERVFAIL
  - nelze odlišit o ostatních příčin selhání
  - pomocí `dig +cdflag` lze provést dotaz s vypnutou validací
- detailní analýza pomocí `unbound-host`

```
$ unbound-host -C /etc/unbound/unbound.conf \
  rhybar.cz
…
validation failure <rhybar.cz. A IN>: no keys
have a DS with algorithm RSASHA1 from
2001:718::53 for key rhybar.cz. while building
chain of trust
```

Když je problém u zdroje





Závěrem

- DNSSEC je **zralá** technologie se **zcela novým** modelem důvery
- aktivní validace do jisté míry **chrání i nepodepsané subdomény**
- manipulací s provozem **nelze** přesvědčit validátor, že daná zóna není podepsaná
- rozšíření pro validaci v prohlížeči pomůže odhalit zfušovaný internet

Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz