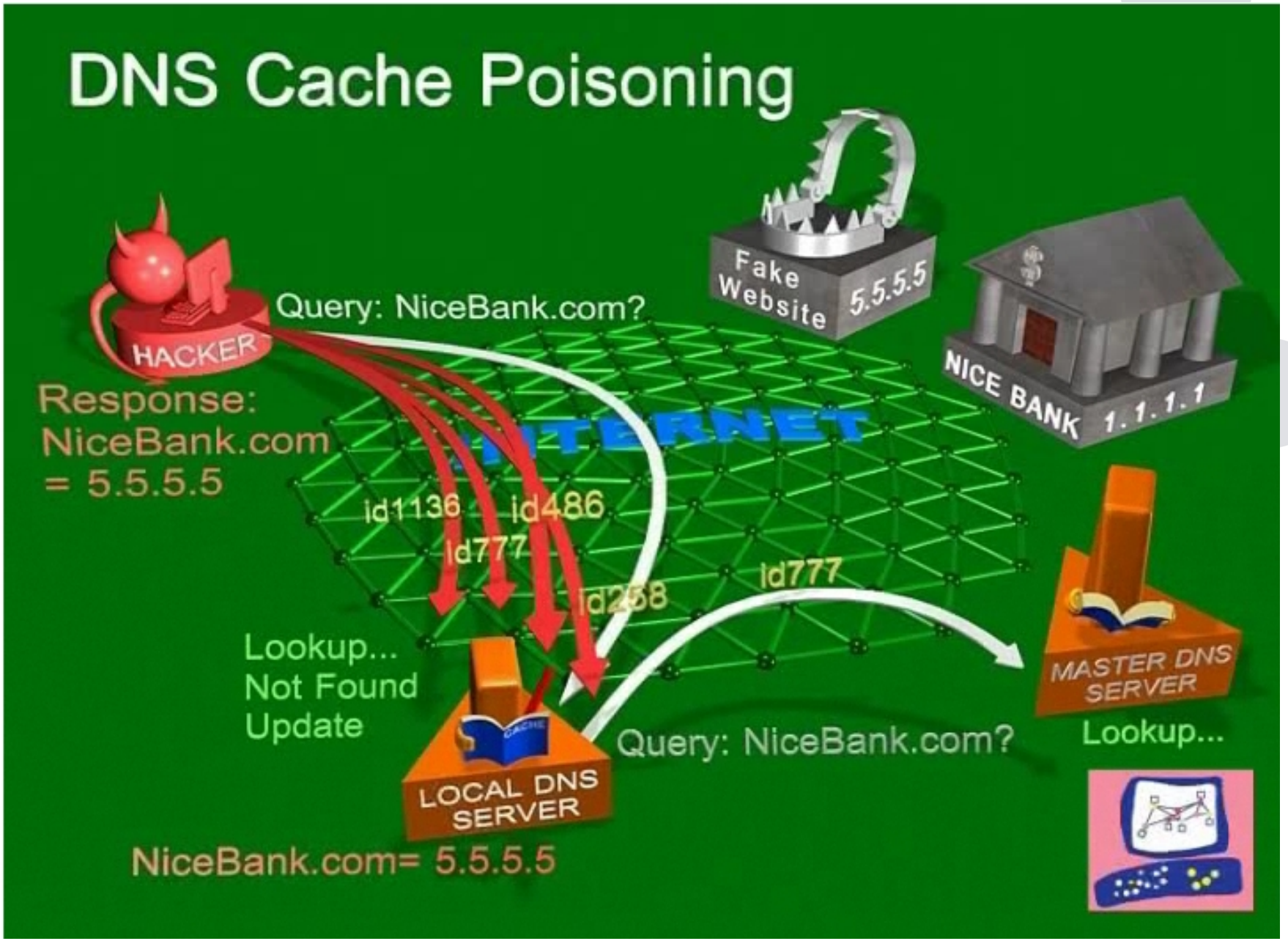
# Útoky na DNS

CZ.NIC Labs

Emanuel Petr <*emanuel.petr@nic.cz*>
7. 6. 2010
IT10, Praha



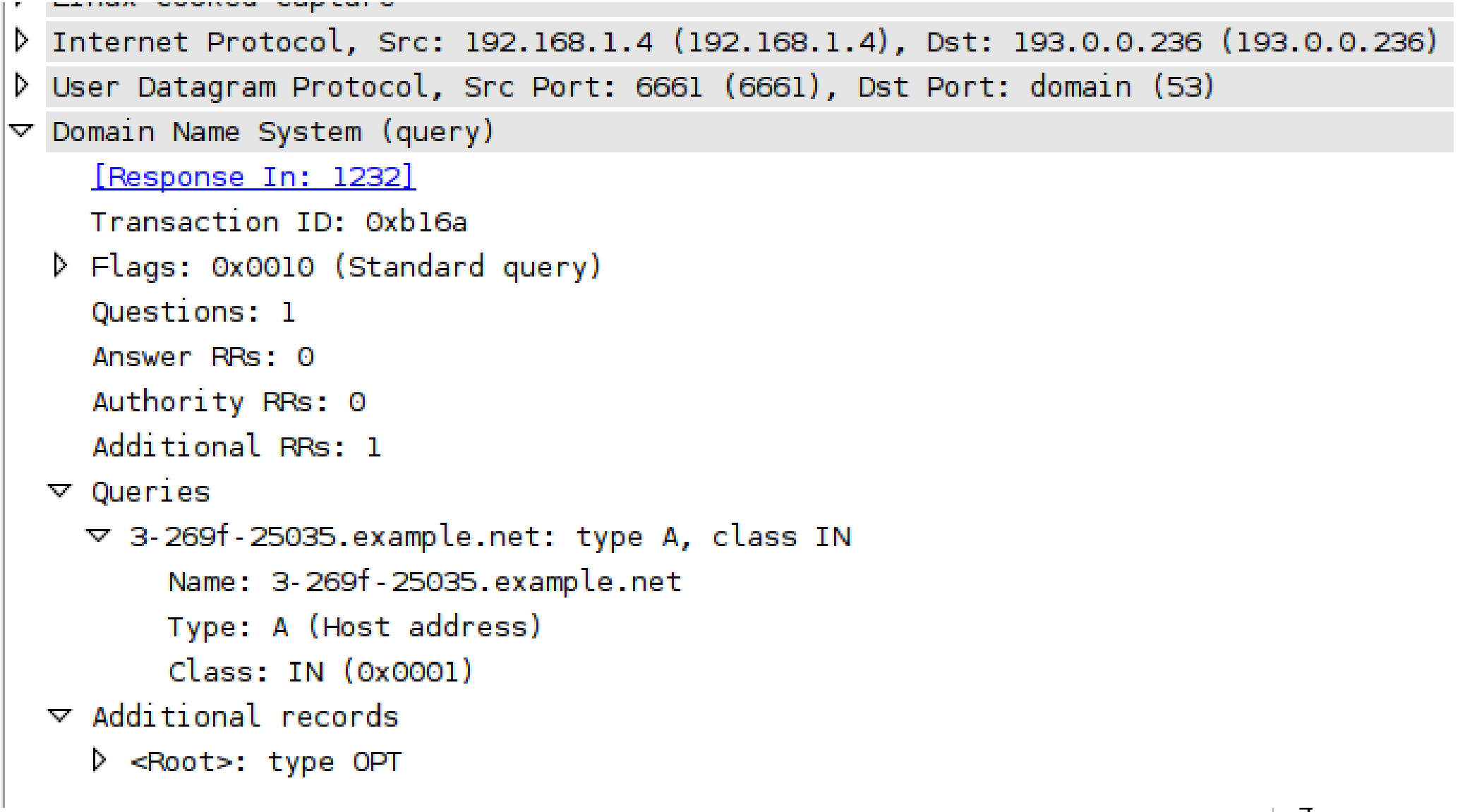

http://www.checkpoint.com/defense/advisories/public/dnsvideo/index.html

# Podvržená odpověď ...

- Doručena dříve než odpověď autoritativního NS
- Obsahovat „Question Section“ z původního dotazu rNS
- Identifikátor odpovědi (ID) roven ID dotazu rNS
- Zdrojová adresa reflektuje adresu autoritativního NS
- Cílový port/adresa se shoduje se zdrojovým portem/adresou dotazu rekurzivního NS

- Pokud splněno → dojde k podvržení údajů nebo-li k otrávení paměti rekurzivního NS

# Dotaz rekurz. NS na autoritativní NS



# Správně vytvořená falešná odpověď

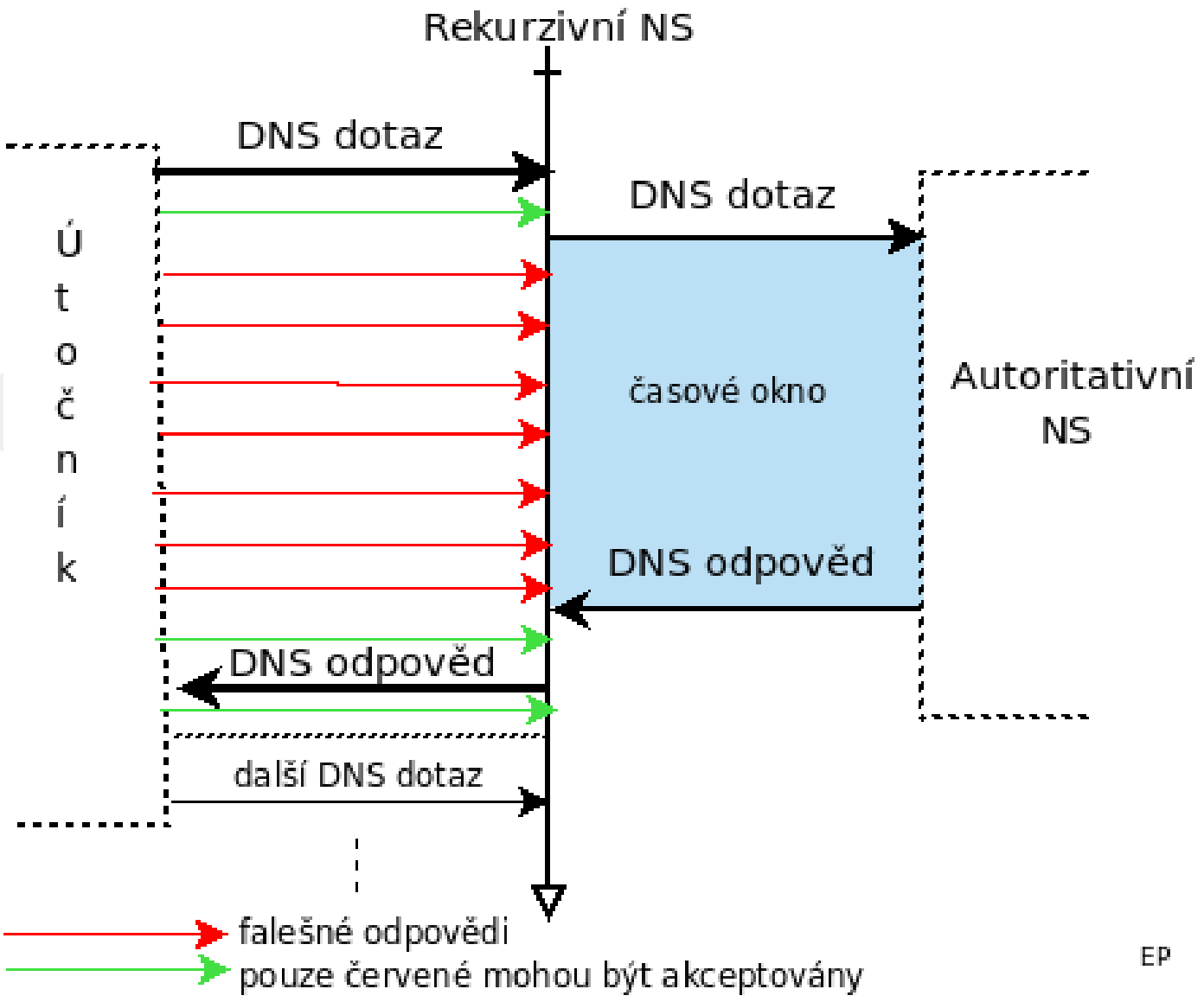
```
▷ Internet Protocol, Src: 193.0.0.236 (193.0.0.236), Dst: 192.168.1.4 (192.168.1.4)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 6661 (6661)
▽ Domain Name System (response)
    Transaction ID: 0xb16a
  ▷ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
  ▽ Queries
    ▽ 3-269f-25035.example.net: type A, class IN
        Name: 3-269f-25035.example.net
        Type: A (Host address)
        Class: IN (0x0001)
  ▽ Answers
    ▷ 3-269f-25035.example.net: type A, class IN, addr 1.2.3.4
  ▽ Authoritative nameservers
    ▷ example.net: type NS, class IN, ns utocnikuv.example.net
  ▽ Additional records
    ▷ utocnikuv.example.net: type A, class IN, addr 1.2.3.4
```

# Zranitelnosti rekurzivních NS - historie (zjednodušeno)

- Sekvenční ID dotazu
  - snadno zjistitelné
- Nedostatečně náhodné ID dotazu
  - ID se dalo předpovědět
- Více souběžných dotazů rNS na shodný záznam
  - 'birthday attack', funkční i při náhodných ID

Výše uvedené zranitelnosti byly opraveny a útoky hrubou silou (odhadnutí ID) nebyly použitelné z důvodu životnosti záznamů v cache rNS.

# Časové okno útoku a životnost záznamu




EP

# Zranitelnost rNS – současnost

- 'Kaminskyho' varianta útoku

  - nemusí se čekat na vypršení životnosti záznamu

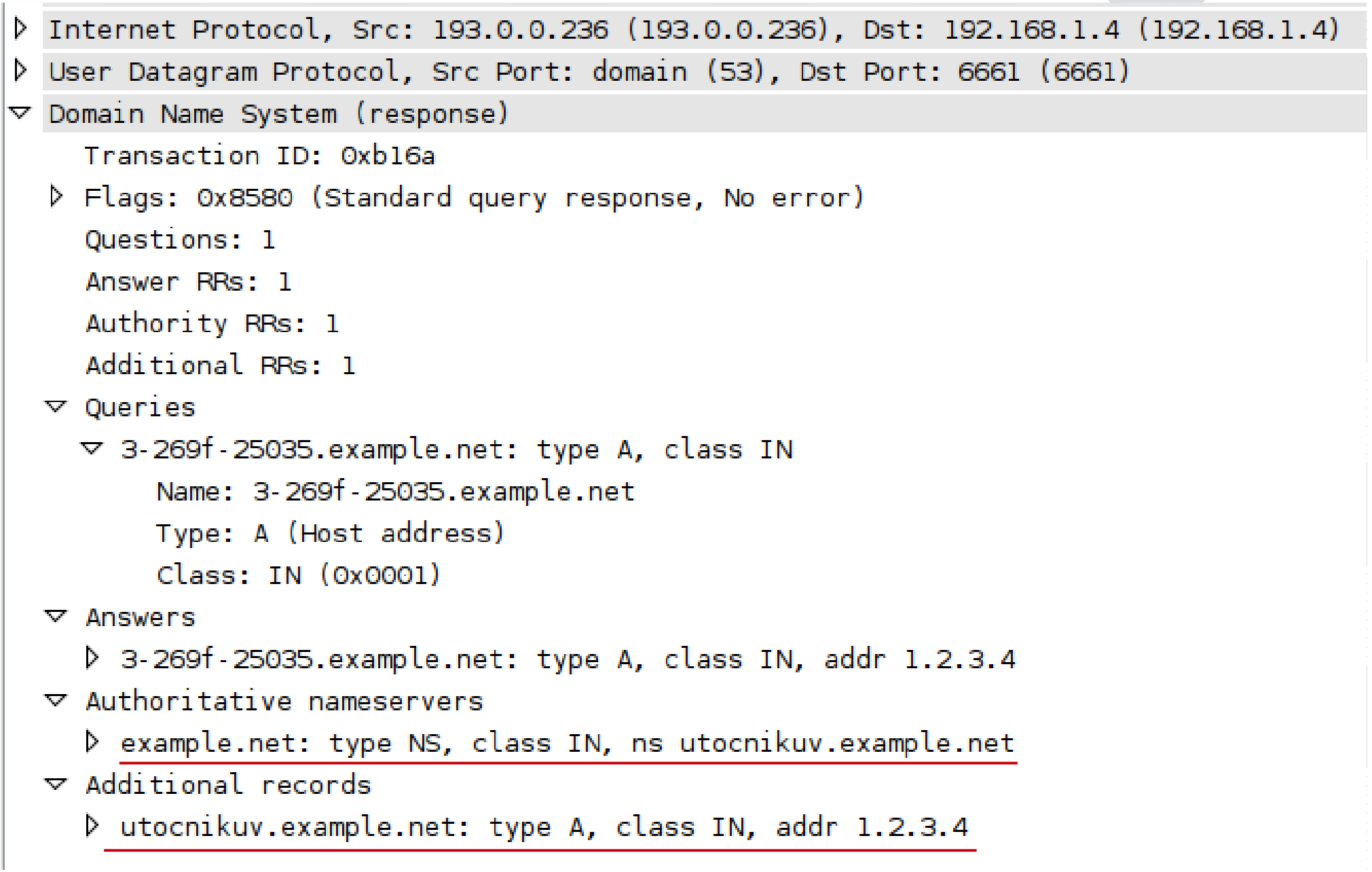
  Jak je to možné ?

- Dotazy se posílají na náhodné poddomény

  např. 'example.net' → 'XYZ.example.net'
  XYZ … je pro každý dotaz unikátní, nebude v cache rNS

- Falešné údaje v 'Authority records' & 'Additional records'

  'Authority records' … FQDN autoritativního NS
  'Additional records' … IP adresa falešného NS


Internet Protocol, Src: 193.0.0.236 (193.0.0.236), Dst: 192.168.1.4 (192.168.1.4)
User Datagram Protocol, Src Port: domain (53), Dst Port: 6661 (6661)
Domain Name System (response)
Transaction ID: 0xb16a
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 1
Queries
3-269f-25035.example.net: type A, class IN
Name: 3-269f-25035.example.net
Type: A (Host address)
Class: IN (0x0001)
Answers
3-269f-25035.example.net: type A, class IN, addr 1.2.3.4
Authoritative nameservers
example.net: type NS, class IN, ns utocnikuv.example.net
Additional records
utocnikuv.example.net: type A, class IN, addr 1.2.3.4

# Zranitelnost rNS – současnost (II)

- Rekurzivní NS: statické zdrojové porty

  napadeny do několika sekund/minut

  útok - nízké nároky na HW a Bandwidth

- Hromadný upgrade na nové verze rekurzivních NS s náhodným zdrojovým portem u dotazů

  Port = 1024 – 65535

# Jaké jsou nyní šance k napadení?

- Falšování **odpovědi** autoritativního NS

  - zdrojová adresa (lze zjistit *)
  - zdrojový port  (fixní, 53)
  - cílová adresa (známé)
  - cílový port (náhodný 1024 – 65535)
  - ID zprávy  (náhodný 0 – 65535)
  - 'Question Section' (známé)

* dvě adres a více

# Čas potřebný k útoku (H)

… při alespoň jedné správné odpovědi útočníka

$$H = \frac{N}{(1000/W)}$$

- *H* … čas útoku v sekundách
- *N* … počet časových oken
- *W* … délka časového okna v ms + režie na další časové okno v ms

# Počet časových oken (N)

… k alespoň jedné správné falešné odpovědi při stanovené pravděpodobnosti (Q)

$$N = \frac{\log(1-Q)}{\log(1-P)}$$

- *Q* … stanovená pravděpodobnost úspěšného útoku
- *P* … pravděpodobnost uhodnutí ID, Portu a IP adresy autoritativní NS

# Pravděpodobnost (P)

… uhodnutí ID, Portu a IP adresy autoritativního NS

$$P = \frac{F}{D * U * S}$$

- *F* … počet falešných odpovědí přijatých v časovém okně
- *D* … počet možných ID
- *U …* počet možných Portů
- *S* … počet možných adres autoritativních NS

# Kompletní vzorec pro výpočet času útoku v sekundách

$$H = \frac{\log(1-Q)}{\log\left(1-\frac{F}{D*U*S}\right)} \Big/ 1000/W$$

- Pravděpodobnost **Q** je stanovena
- Hodnoty **D** a **U** jsou známé
- **S** lze zjistit
- **F** a **W** je měřitelné

- Vzorec je platný za podmínek:
  - ID a zdrojový port dotazů rNS jsou náhodné
  - ID a zdrojové porty falešných dotazů generovány systematicky náhodně

# Testy DNS cache poisoning útoku (I)

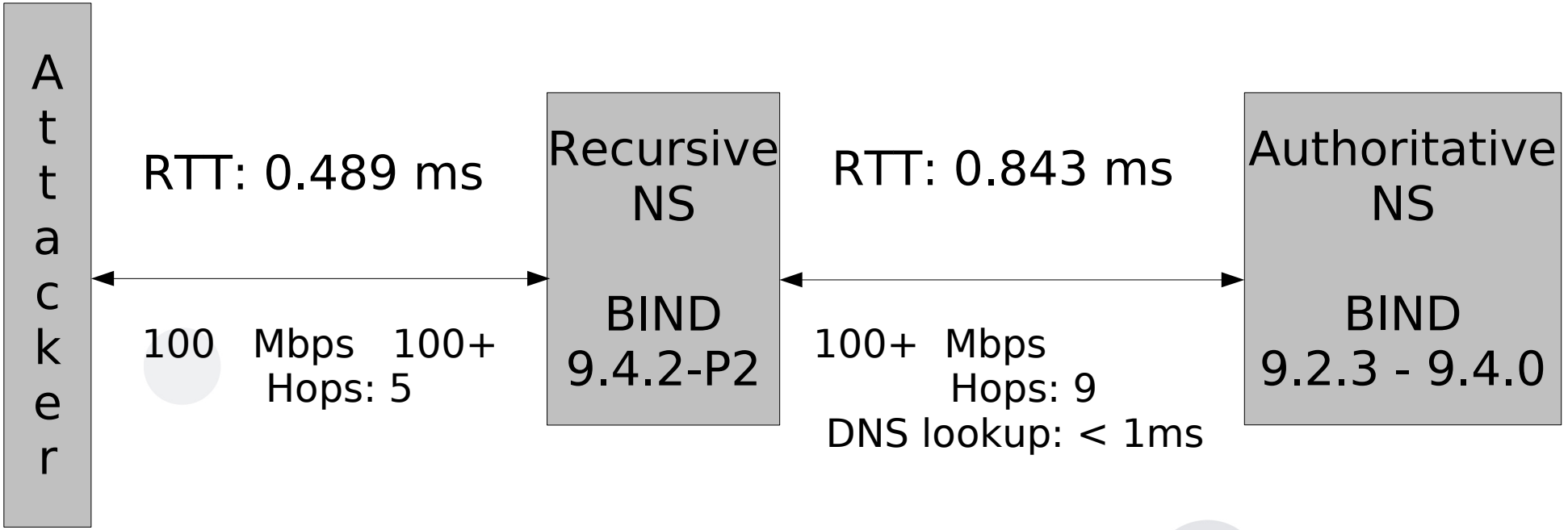
- Tři lokality propojeny v NIX.CZ
- Útočník, rekurzivní NS a autoritativní v samostatné lokalitě
- Podvrhovaná doména dva autoritativní NS
- Autoritativní NS s jednou adresou (bez IPv6)
- Dotazy rekurzivního NS rovnoměrně rozloženy mezi oba autoritativní NS
- Falešné odpovědi posílány pouze pro jeden autoritativní NS
- BIND9 verze 9.4.2 a novější

# Testy DNS cache poisoning útoku (II)

- Průměrná velikost falešné DNS zprávy 125 B
- ID a zdrojový port náhodné
  ID = 0 – 65535
  Port = 1024 – 65535
- Evgeniy Polyakov implementace útoku

  http://www.ioremap.net/archive/dns/

# Testovací scénář I.



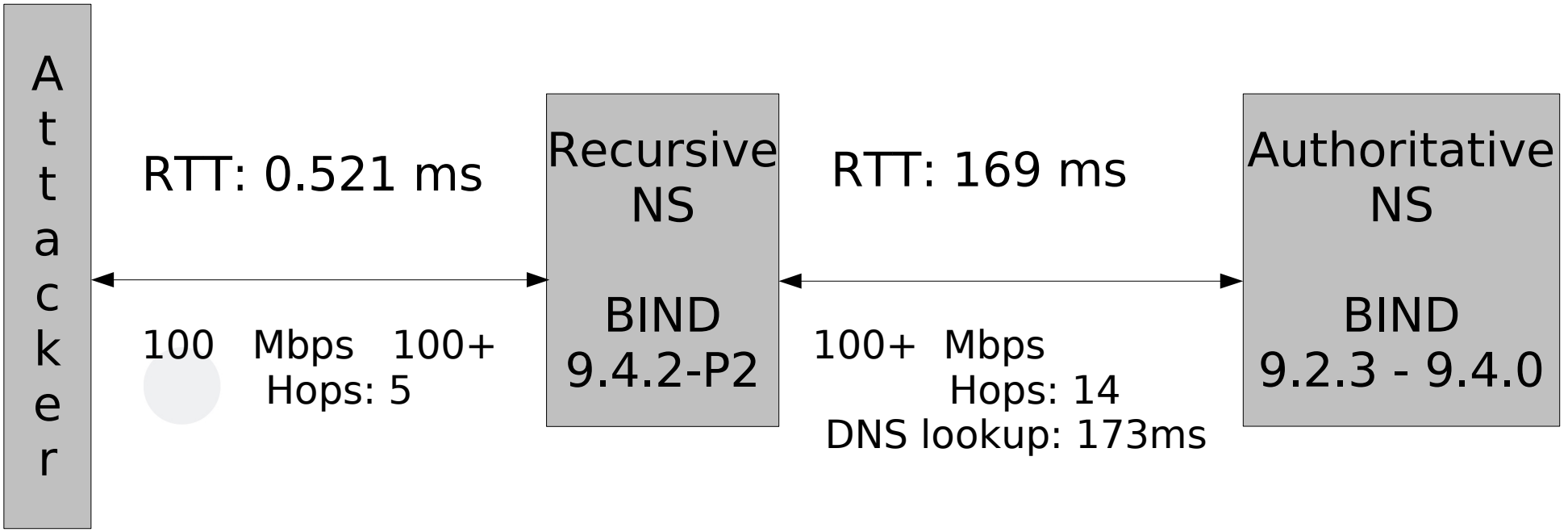

- round-trip časy a DNS překlad pod 1 ms
- krátké časové okno k útoku (1.041 ms)

# Testovací scénář I.

| Testovací scénář 1 | Průměr | Směrodatná odchylka |
|---|---|---|
| Časové okno útoku | 1.041 ms | 0.096 |
| Počet falešných odpovědí na jedno časové okno | 57 | 6 |
| Provoz přijatých falešných odpovědí | 55.05 Mbps | 3.86 |
| Režie na časové okno | 10.451 ms | 1.599 |
| Režie na jednu vteřinu útoku | 909.41 ms | |

| Pravděpodobnost úspěšného útoku | |
|---|---|
| 99 % | 2 169 hodin (~ 90 dnů) |
| 95 % | 1 411 hodin (~ 59 dnů) |
| 90 % | 1 084 hodin (~ 45 dnů) |

# Testovací scénář II.



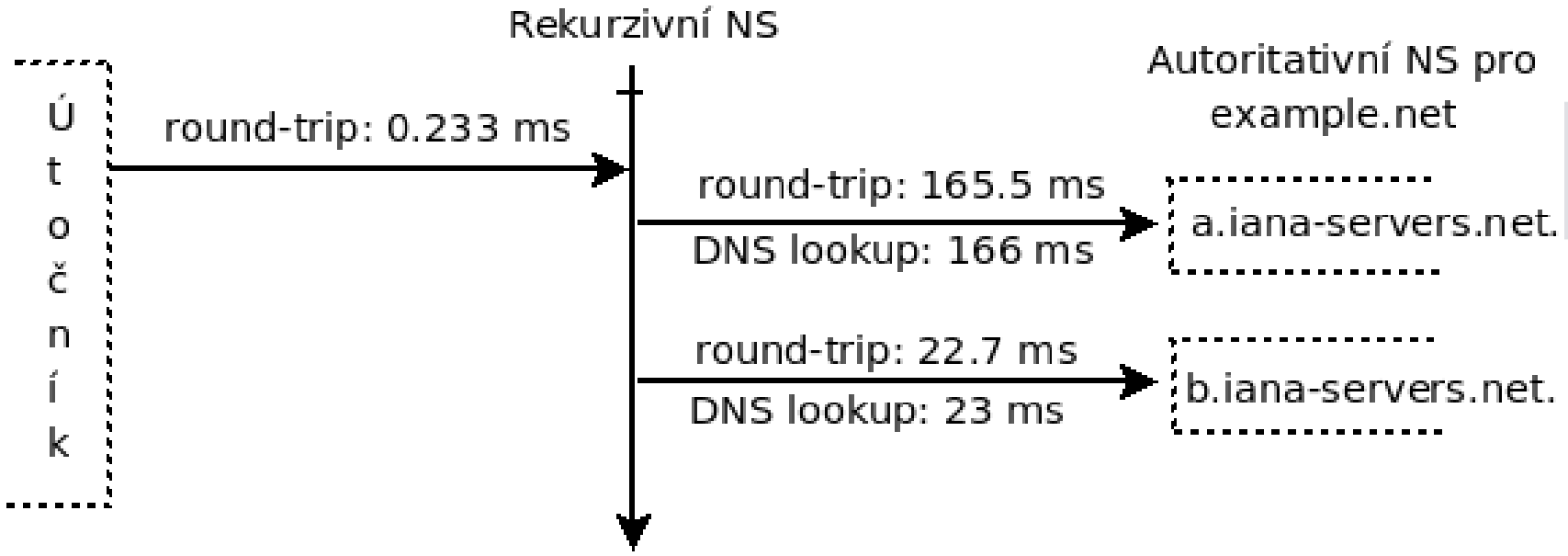

- Autoritativní NS má horší dostupnost a pomalé odezvy
- Časové okno útoku 163 ms

# Testovací scénář II.

| Testovací scénář 2 | Průměr | Směrodatná odchylka |
|---|---|---|
| Časové okno útoku | 163.678 ms | 13.965 |
| Počet falešných odpovědí na jedno časové okno | 8 560 | 761 |
| Provoz přijatých falešných odpovědí | 52.30 Mbps | 2.00 |
| Režie na časové okno | 3.650 ms | 0.592 |
| Režie na jednu vteřinu útoku | 21.81 ms | |

| Pravděpodobnost úspěšného útoku | |
|---|---|
| 99 % | 211 hodin (~ 9 dnů) |
| 95 % | 138 hodin (~ 6 dnů) |
| 90 % | 106 hodin (~ 4 dny) |

# Útok na rNS - statický zdrojový port




- Útok na doménu 'example.net'
- Rekurzivní NS upřednostňuje **b.iana-servers.net**

# Útok na rNS - statický zdrojový port

| Provoz falešných odpovědí (Mbps) | Časové okno (ms) | Falešné odpovědi doručené na jedno časové okno | Délka útoku (vteřiny) | | | |
|---|---|---|---|---|---|---|
| | | | test1 | test2 | test3 | test4 |
| 34.16 | 23 - 27 | 746 - 865 | 2 | 1 | 3 | 6 |
| 10.72 | 19 - 32 | 202 - 335 | 3 | 18 | 9 | 8 |
| 1.68 | 25 - 26 | 41 - 42 | 34 | 32 | 7 | 5 |
| 0.56 | 27 - 28 | 13 - 14 | 193 | 76 | 601 | 152 |

# Útok na rNS - náhodný zdrojový port

| Test | Vygenerovaný provoz falešných odpovědí | Časové okno ms | Falešné odpovědi doručené na jedno časové okno | Trvání útoku ( odpovídající pravděpobnost ) |
|---|---|---|---|---|
| 1. | 85.31 Mbps | 45.491 | 3 820 | 25 h 40 min (59 %) |
| 2. | 64.08 Mbps | 18.501 | 1 171 | 93 h 41 min (88 %) |
| 3. | 14.34 Mbps | 102.241 | 1 466 | 64 h 3 min (32 %) |
| 4. | 14.80 Mbps | 684.982 | 10 139 | 25 h 0 min (15 %) |
| 5. | 14.80 Mbps | 597.701 | 8 845 | 95 h 52 min (45 %) |
| 6. | 14.15 Mbps | 650.851 | 9 207 | 50 h 41 min (26 %) |
| 7. | 14.47 Mbps | 504.132 | 7 293 | 248h 30 min (78%) |

# BIND9 rekurzivní NS a výběr autoritativního DNS serveru

- Udržuje si přehled o dostupnosti autoritativních NS
- Dostupnost reprezentuje prostřednictvím SRTT (Smoothed Round Trip Time)

- Sledovat změny SRTT lze příkazem:
- ```
  $ watch -n 0.5 'sudo rndc dumpdb -cache; sleep 0.5;  \
   grep -E "((192\.0\.34\.43)|(193\.0\.0\.236)).*srtt" \
  /var/cache/bind/named_dump.db'
  ```
- Ukázka výstupu

```
;   192.0.34.43 [srtt 39866] [flags 00000000] [ttl 1711]
;   193.0.0.236 [srtt 21929] [flags 00000000] [ttl 1711]
```
```

# BIND9 rekurzivní NS a výběr autoritativního DNS serveru

- `$ dig example.net @192.0.34.43 | grep "Query time"`
  `;; Query time: **158 msec**`

- `$ dig example.net @193.0.0.236 | grep "Query time"`
  `;; Query time: **25 msec**`

- čtyři testy, tisíc žádostí na překlad domény example.net

| Preference autoritativního NS | | | | |
|---|---|---|---|---|
| **193.0.0.236** | **98.1 %** | **98.1 %** | **98.1 %** | **98.1 %** |
| 192.0.34.43 | 1.9 % | 1.9 % | 1.9 % | 1.9 % |

# Omezující faktory útoku (neúplné)

| | | |
|---|---|---|
| Kontrola zdrojové adresy | Útok není možný | Směrovač mezi útočníkem a rekurzivním NS blokuje pakety s falešnou zdrojovou adresou |
| DNSSEC na rekurzivním a autoritativním NS | Útok není možný | DNS Security Extensions chrání proti DNS cache poisoning útokům |
| Rekurzivní NS s filtrací dotazů | Omezuje útok z povolených sítí | NS akceptuje rekurzivní dotazy pouze ze seznamu povolených sítí |
| Náhodné ID a zdrojové porty | Snižuje účinnost útoku | Rekurzivní NS pro své dotazy používá náhodně generované ID a zdrojové porty |
| Více autoritativních NS pro doménu | Snižuje účinnost útoku | Každý nový autoritativní NS snižuje odhadnutí zdrojové adresy |
| IPv6 adresa na autoritativním a rekurzivním NS | Snižuje účinnost útoku | Zavedení IPv6 adresy na autoritativním a rekurzivním NS redukuje odhadnutí zdrojové adresy odpovědi autoritativ. NS |
| Rychlá odezva / vysokokapacitní šířka pásma autoritativn.NS | Snižuje účinnost útoku | Rychlá odezva zkracuje časové okno útoku a dostatečná šířka pásma znesnadňuje DoS útoky na autoritativ.NS |
| ... | ... | ... |

# Otevřené rekurzivní NS & statické zdrojové porty

- Rekurzivní NS z dotazů na autoritativní NS .cz TLD (jednodenní provoz)
  - celkem k analýze: 79 963
  - otevřené rekurzivní NS: 10 219 (v4) + 1 762 (v6)
  - statický port: 2651 +

- Autoritativní NS českých domén (.cz zóna)
  - celkem k analýze: 18 854
  - otevřené rekurzivní NS: 2 927
  - statický port: 745

# Závěr

- Útok na rekurzivní NS s náhodnými zdrojovými porty
  - mnohem složitější, ale stále možný
  - dny až týdny při provozu desítek Mbps
  - technicky realizovatelné
  - asi největší překážkou monitoring sítě a správci sítě
  - monitoring i lidský faktor však může selhat
  - integritu údajů a jistotu, že byly poskytnuty správným zdrojem zajistí pouze …

DNSSEC → Implementujte ;)

# Děkuji vám za pozornost

Emanuel Petr

*emanuel.petr@nic.cz*

Kde získat informace o dalších aktivitách sdružení CZ.NIC?

| | |
|---|---|
| **Web** | **www.nic.cz** |
| **Blog** | **blog.nic.cz** |
| **Email** | **kontakt@nic.cz** |
| **Konference** | **nic-news@nic.cz** |