RNIDS

DNS kao bezbednosni servis

Registar nacionalnog internet domena Srbije

DATUM
22 novembar 202

GOVORI
Žarko Kecić

MANIFESTACIJA
TELFOR 2023

RNIDS

Koliko smo zaista bezbedni?

- Firewall uređaji
- SIEM sistemi
- Proxy serveri
- Antivirusni programi
- …

RNIDS

Šta je DNS?

Zamišljen kao protokol koji nazive domena uparuje sa odgovarajućim IP adresama (telefonski imenik interneta).

Nakon oko 300 RFC-ova, DNS pre može da se definiše kao usluga nego kao protokol.

RNIDS

Karakteristike DNS-a

Dostupnost – Svi internet ser[illegible]d DNS-a. Ako e-pošta ne radi, sve ostalo će raditi, ali ako DNS stane ništ[illegible]

Pouzdanost i integritet – K[illegible]eBay-u? Šaljete i primate važne i-mejl poruke? Ako neko zlo[illegible]s preusmeriti gde god želi.

Brzina – učitavanje jedn[illegible]e, pa i stotine DNS upita (zamislite kada bi odgovor na svak[illegible]

Prilagodljivost – Koris[illegible]bavlja mnoge druge zadatke (DMARC i DKIM, SPF, DANE, CAA, ...).

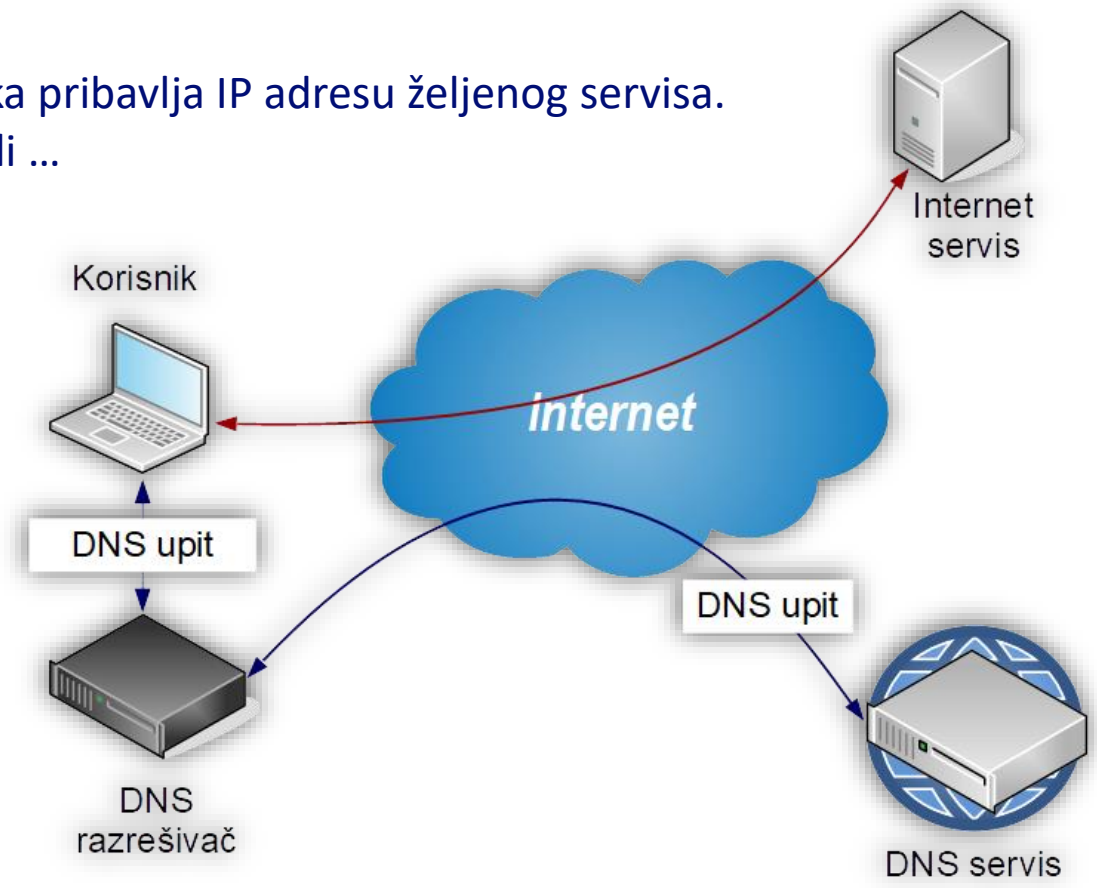
DNS je osnovni servis bez koga internet ne bi funkcionisao!

RNIDS

Razrešavanje DNS upita

DNS razrešivač?

Servis koji na osnovu zahteva korisnika pribavlja IP adresu željenog servisa.
Najčešće je kompanijski ili kod ISP-a ili …



RNIDS

Zloupotreba DNS-a

Zlonamerni korisnici registruju novi naziv domena (naziv domena koji nema lošu reputaciju).

- Takvi domeni se najčešće upotrebljavaju odmah, mada…

- Phishing kampanje
- Širenje malvera
- Varanje korisnika na neki drugi način (npr. homografi, typosquatting, …)
- Širenje neprikladnog sadržaja

RNIDS

Komunikacija malvera sa C&C serverom

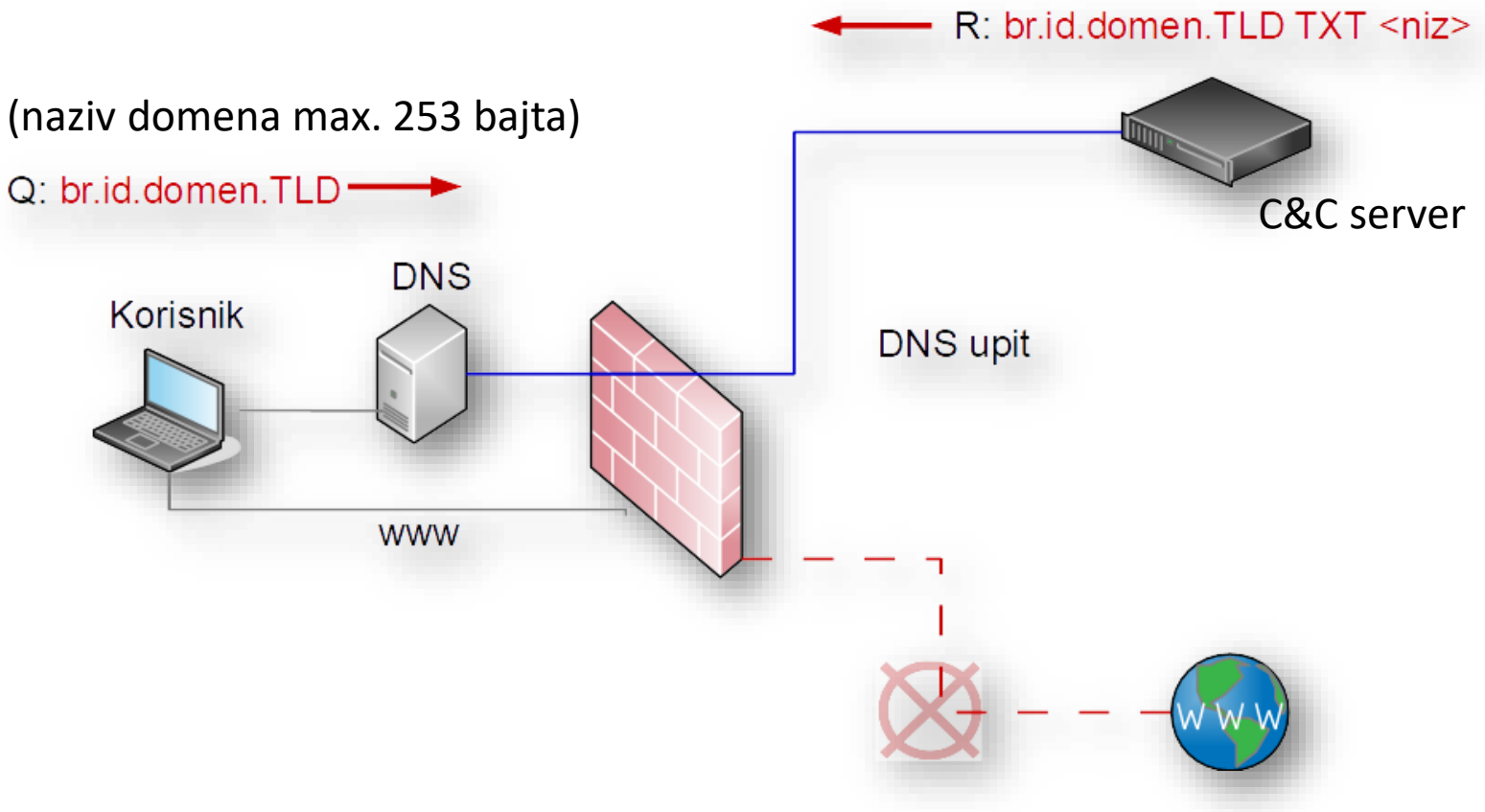
Kada se nađe unutar zaštićenog sistema, malver pokušava da komunicira sa C&C serverom.

a) Pokušava da uspostavi direktnu komunikaciju
b) Šalje DNS upite sa predefinisane liste domena - DGA (Domain Generation Algorithm)

… dok ne uspostavi komunikaciju.

RNIDS

DNS tunel



RNIDS

Kroz DNS tunel može da se pošalje…

… mnogo podataka!

- Naziv domena može da ima najviše 253 karaktera (63 karaktera po segmentu)
- Maksimalna veličina DNS poruke je 64kb preko TCP konekcije

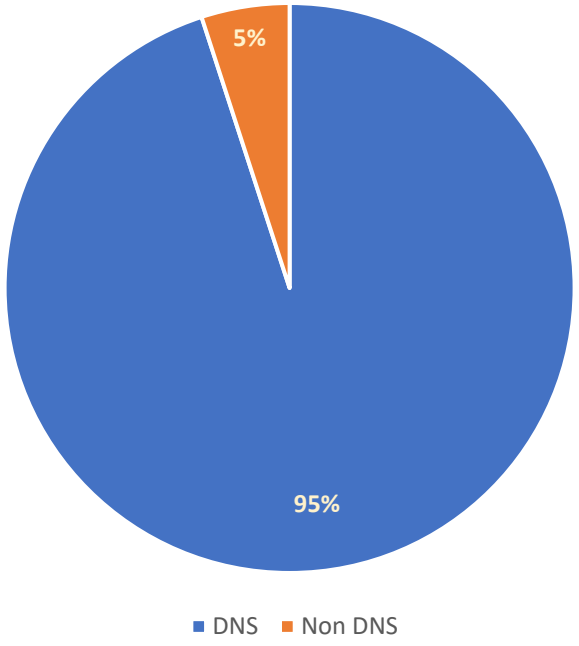
Da bi se prenela velika količina podataka DNS upit se ponavlja sa novim blokom podataka.

```
0.podaci.id.domen.TLD
1.podaci.id.domen.TLD
2.podaci.id.domen.TLD
…
```

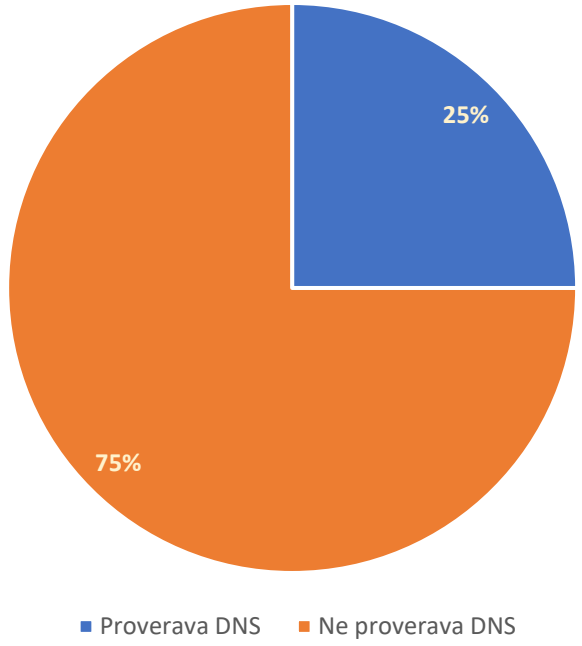
RNIDS

Šta možemo saznati uz pomoć DNS-a?

Malver koji koristi DNS



Korisnici koji proveravaju DNS



RNIDS

Savremeni DNS

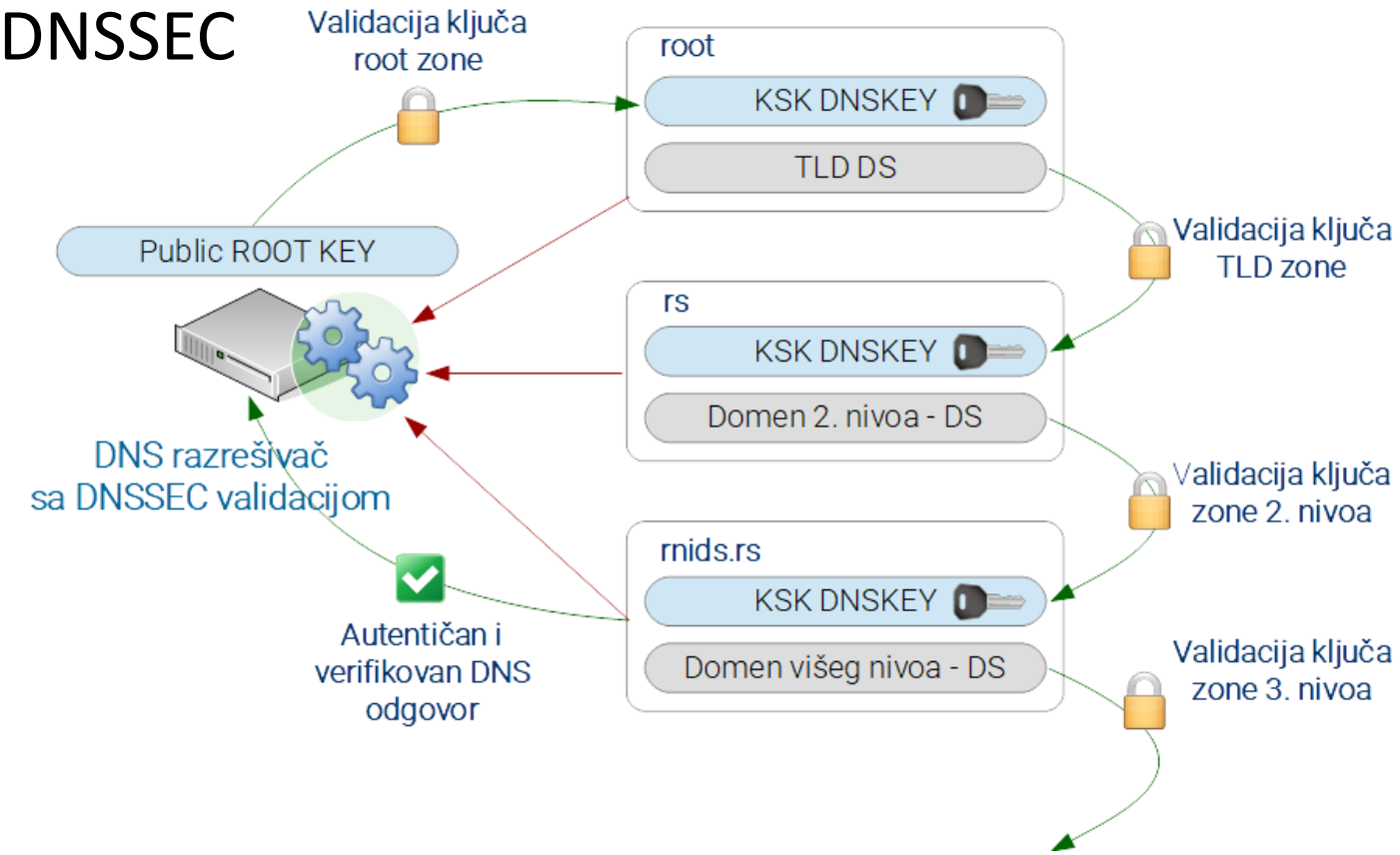
Poslednjih 20tak godina urađeno je mnogo na unapređenju DNS bezbednosti i uvedena proširenja koja povećavaju bezbednost drugih servisa (DMARC i DKIM, SPF, DANE, CAA, ...).

Jedan od najznačajnijih je DNSSEC koji potvrđuje autentičnost izvora i integritet DNS podataka.

RNIDS

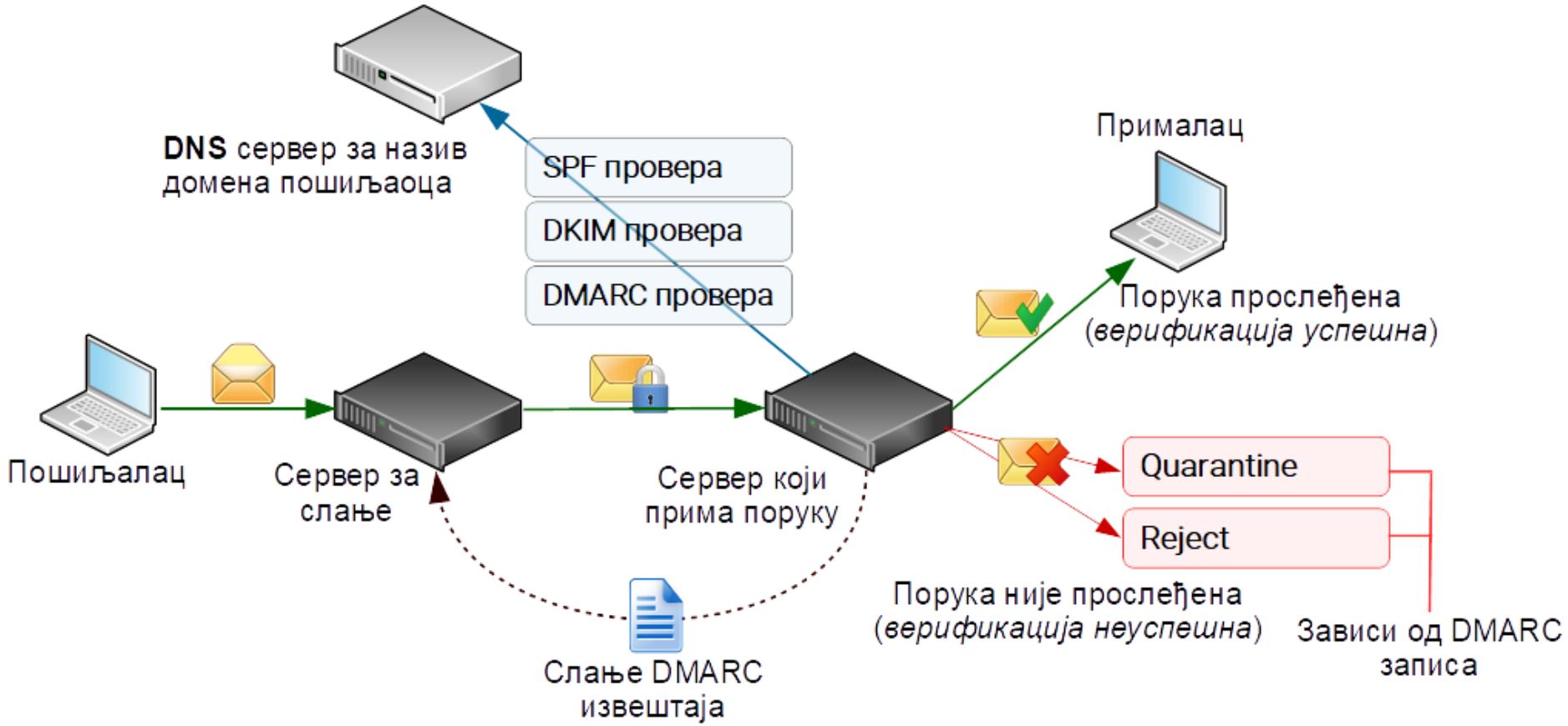
Autentičnost i integritet

DNSSEC



RNIDS

Zaštita servisa e-pošte



RNIDS

Zaštita privatnosti

Standardni DNS upiti i odgovori šalju se u tekstualnim porukama.

- DoT (DNS over TLS) koristi port 853
- DoH (DNS over https) koristi port 443

RNIDS

…ali DNS i dalje razrešava zlonamerne nazive domena

Poslednjih nekoliko godina veliki je pritisak na TLD operatere i registrare da suspednuju (ne publikuju DNS podatke) za zlonamerne domene, ali…

… ccTLD operateri nemaju legalan osnov da ukidaju uslugu koja im je plaćena

… to samo privremeno rešava problem jer je sadržaj i dalje dostupan preko nekog drugog naziva domena

RNIDS

Zaštita korisnika

Sa druge strane, operateri DNS razrešivača mogu da koriste liste zlonamernih naziva domena i u cilju zaštite svojih korisnika ne razrešavaju takve upite.

Response Policy Zone (RPZ) – omogućava uspostavljanje pravila za filtriranje DNS upita za zlonamerne (ili na drugi način štetne) nazive domena.

RNIDS

Baza zlonamernih naziva domena

- Preuzimanje podataka od kompanija koje se bave bezbednošću: Spamhouse, Phishtank, McAfee, Kaspersky, Symantec…
- Analiza DNS upita i odgovora (na svojim rekurzivnim serverima ili preuzimanje podataka od kompanija koje rade pasivnu analizu DNS-a)

Međutim, veliki broj kompanija koje imaju podatke o zlonamernim domenima tu uslugu preuzimanja tih podataka skupo naplaćuju.

RNIDS

Da li DNS filteri moraju da koštaju?

Neki operateri javnih/besplatnih rekurzivnih DNS servera imaju implementirane DNS filtere za maliciozne nazive domena (Quad9, CleanBrowsing, dns0.eu…)

Google (8.8.8.8) nema filtere, a Cloudflare (1.1.1.1) filtrira nazive domena koji šire malver.

RNIDS

Šta možemo sami da uradimo?

- Redovno praćenje i analiza DNS saobraćaja na rekurzivnim serverima koje kontrolišemo.
- Pravljenje sopstvenih RPZ pravila i liste nepoželjnih domena (zaštita dece, zaštita korporativne mreže, …).
- Upotreba javih rekurzora koji rade filtriranje malicioznih naziva domena.

RNIDS

Pitanja?

www.rnids.rs
рнидс.срб

www.domen.rs
домен.срб