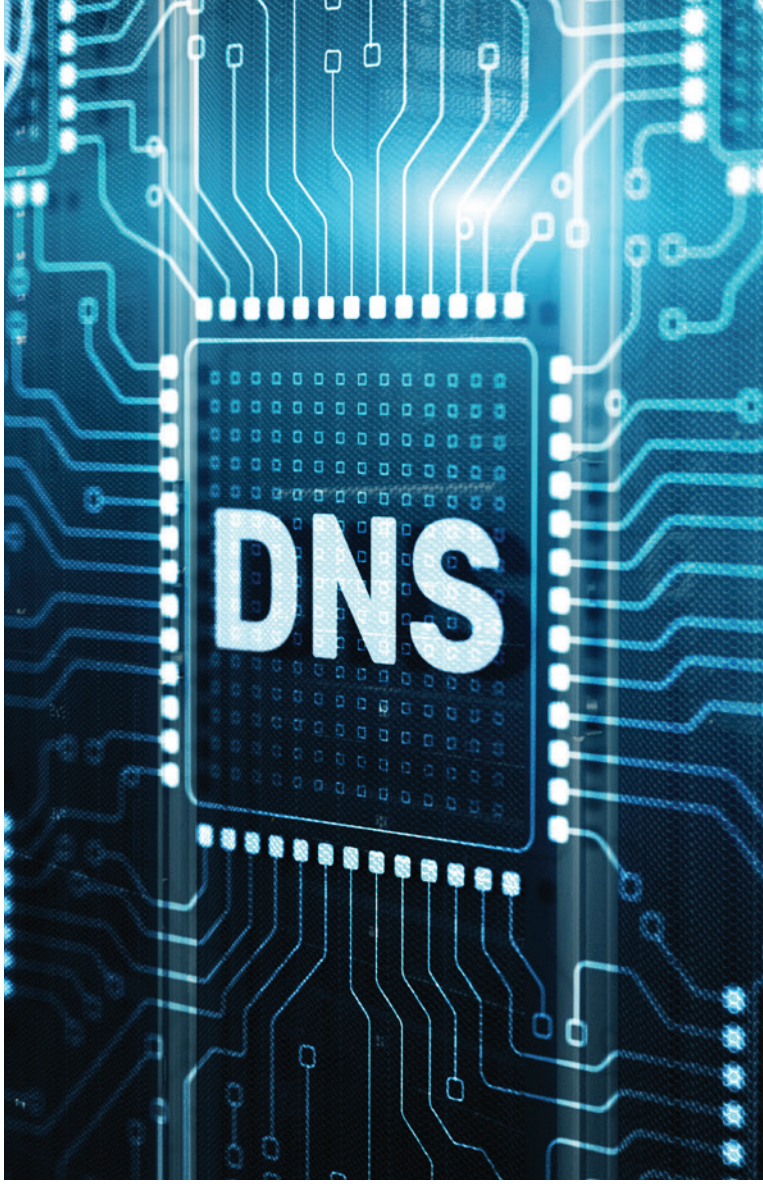
SMART COM

Bela knjiga

# Kako zagotavljamo VARNOST DNS protokola?

# Kazalo vsebine

# UVOD




Storitev DNS je za poslovanje podjetij in organizacij vitalnega pomena, česar se zavedajo tudi kibernetski napadalci.

Varovanje DNS storitev zahteva celovitejši pristop, saj je potrebno nameniti pozornost vsaj dvema pogledoma - varovanju samih DNS storitev na eni strani ter varovanju ostalih virov v IT sistemu preko DNS zaščite.

Katere grožnje pretijo DNS storitvam, kako zastaviti koncept varovanja in kakšne so rešitve, bo podrobneje predstavljeno v naslednjih poglavjih.

# 1. Kaj je DNS in kako deluje?

Ves promet, ki potuje po internetu, uporablja DNS protokol, ki zagotavlja dostavo elektronske pošte, spletni promet in zlonamerni promet. DNS prevaja imena domen v IP naslove, ki jih računalniki uporabljajo za medsebojno prepoznavanje in komunikacijo v internetu.

Vpis imena domene v spletni brskalnik ali pošiljanje e-pošte sproži zahtevo DNS strežniku, ki nato poišče ustrezen IP naslov za to ime domene. DNS je **ključna sestavina internetne infrastrukture**, ki omogoča nemoteno delovanje različnih spletnih storitev. Uporabnikom pomaga pri dostopu do spletnih mest in drugih virov, saj prikazuje imena domen, ki jih je lahko razumeti in si jih zapomniti, kar poenostavi postopek spletne navigacije.

Vse aplikacije uporabljajo domenska imena. Elektronska pošta potrebuje domenska imena za delovanje. Delilniki prometa in omrežja za dostavo vsebin (CDN) ter odkrivanje storitev (AD in VoIP) so odvisni od DNS. Https protokol in certifikati prav tako ne morejo brez domenskih imen.

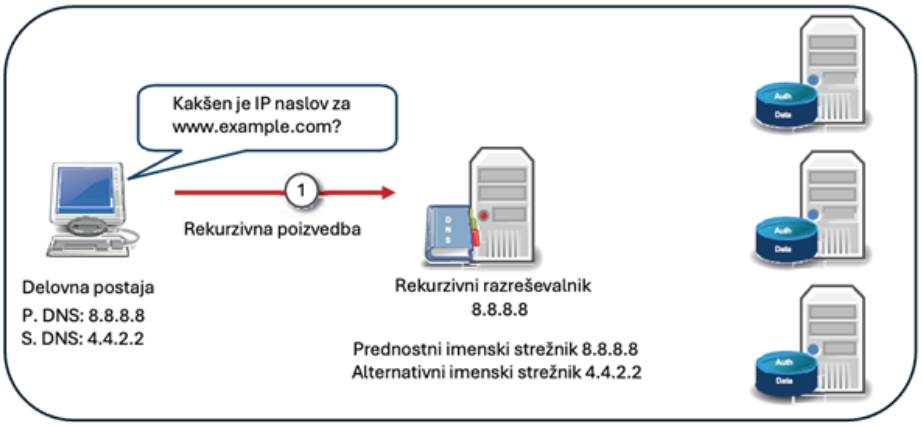
Postopku, pri katerem se človeku prijazno domensko ime (npr. www.example.com) pretvori v številčni IP naslov, ki ga računalniki uporabljajo za komunikacijo na internetu, pravimo postopek razreševanja domenskega imena (Domain Name System Resolution). Z razumevanjem tega procesa lahko bolje razumemo, kako internet deluje in kako smo zaščiteni pred različnimi kibernetskimi grožnjami.

Poglejmo postopek razreševanja domenskega imena s pomočjo spodnjih **osmih korakov**.

## 1 Rekurzivna poizvedba

Delovna postaja ima vpisan primarni in sekundarni DNS strežnik. Delovna postaja, z vpisom url naslova v brskalnik, sproži rekurzivno poizvedbo (Recursive Query) na primarni DNS strežnik z IP naslovom 8.8.8.8.

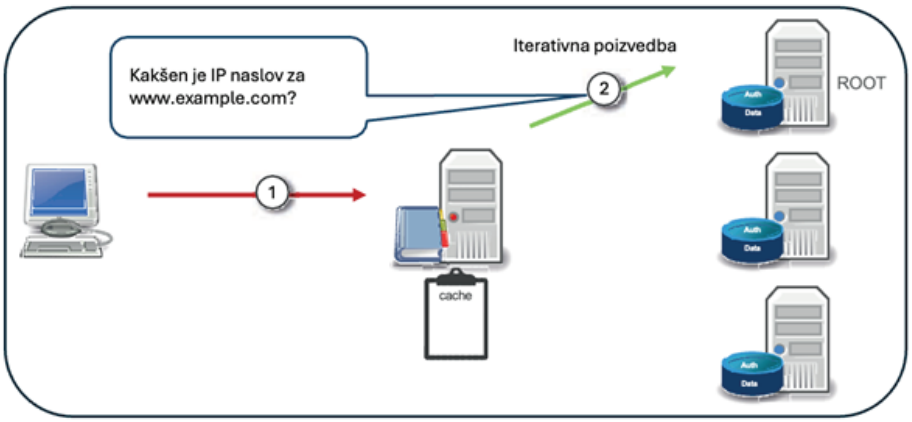
Le-ta predstavlja rekurzivni razreševalnik *(Recursive resolver)*.




## 2 Iterativna poizvedba

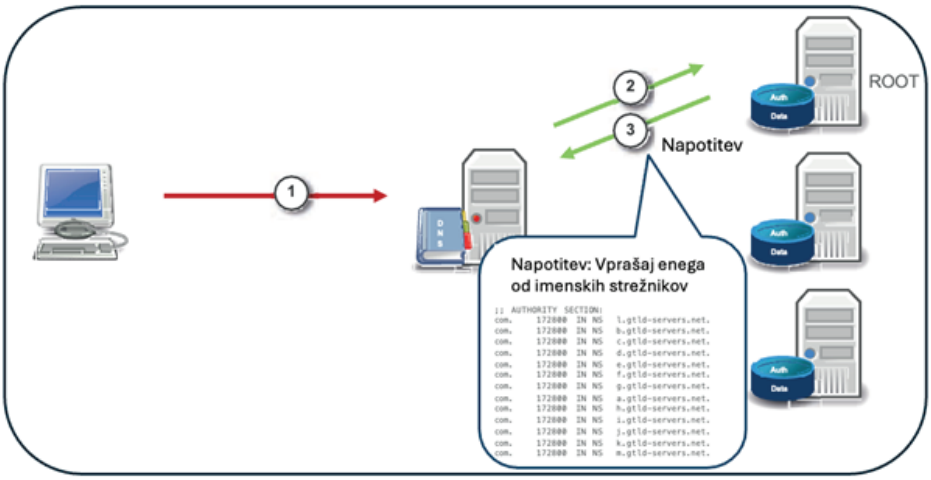
Ker rekurzivni razreševalnik nima zahtevanega imena shranjenega v predpomnilniku *(cache)*, izvede iterativno poizvedbo *(Iterative Query)* pri korenskem strežniku *(root)*.

Rekurzivni razreševalnik poišče IP naslov korenskega strežnika v datoteki z root strežniki. Samostojno se odloči za enega izmed njih.



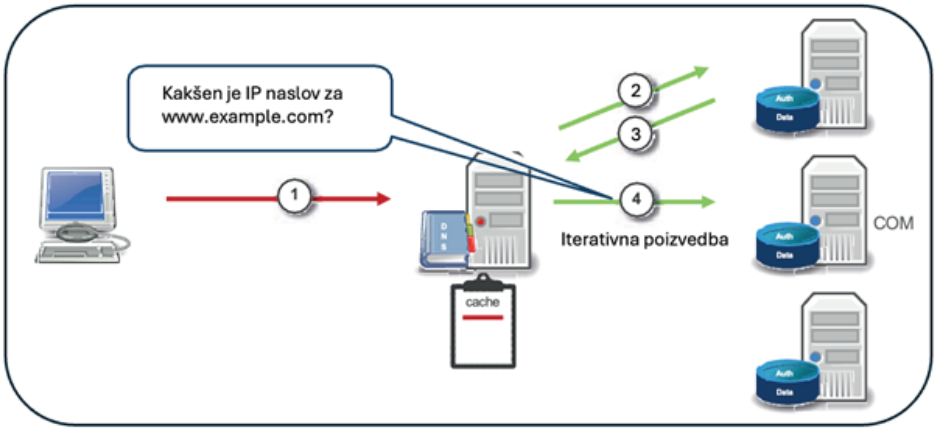
## 3 Napotitev

Glede na tip poizvedbe, ki se konča s .com, korenski strežnik posreduje rekurzivnemu razreševalniku napotke *(Referral)*, kako priti do .com. Pošlje mu name server records *(NS records)*, ki vsebuje zapis za vse .com strežnike. Rekurzivni razreševalnik se sam odloči, katerega bo izbral.



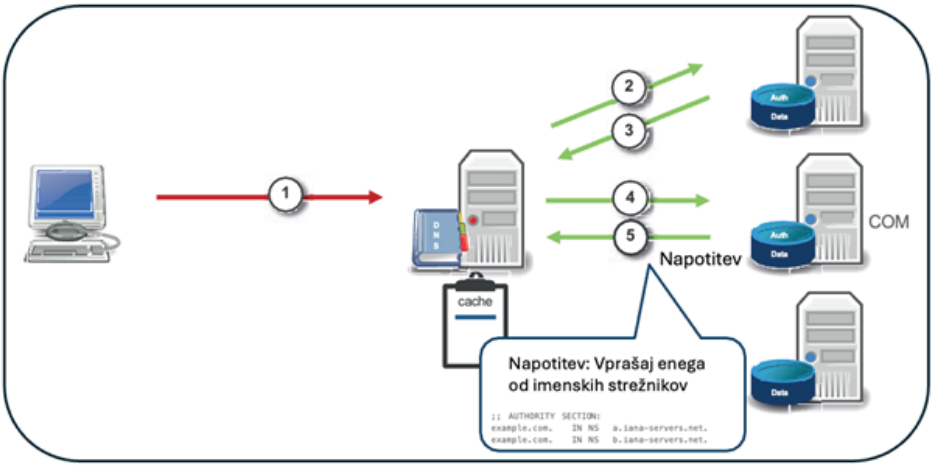

## 4 Iterativna poizvedba

Rekurzivni razreševalnik shrani v predpomnilnik odgovor (NS zapis za .com) iz korenskega strežnika. Izbere enega od com imenskih strežnikov in izvede iterativno pozivedbo.



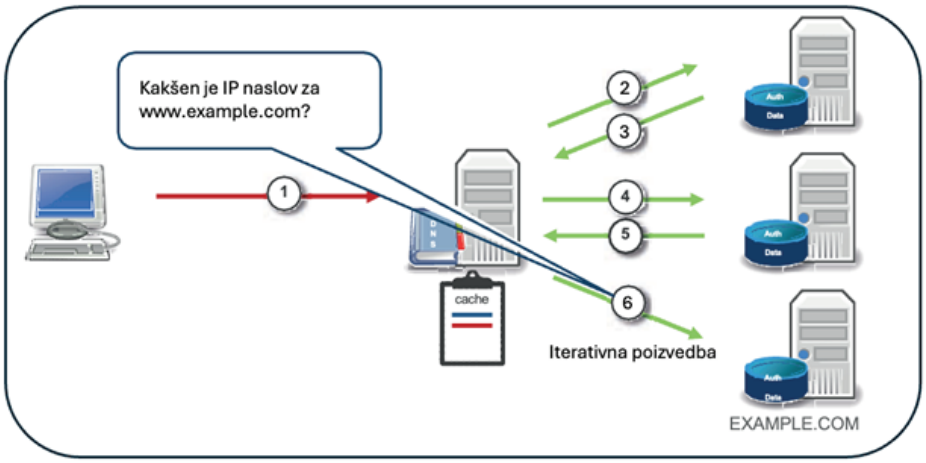

## 5 Napotitev

Imenski strežnik com posreduje rekurzivnemu razreševalniku napotke (Referral), kako priti do example.com strežnika. Pošlje mu name server records (NS records), ki vsebuje zapis za vse example.com strežnike. Rekurzivni razreševalnik se sam odloči, katerega bo izbral.



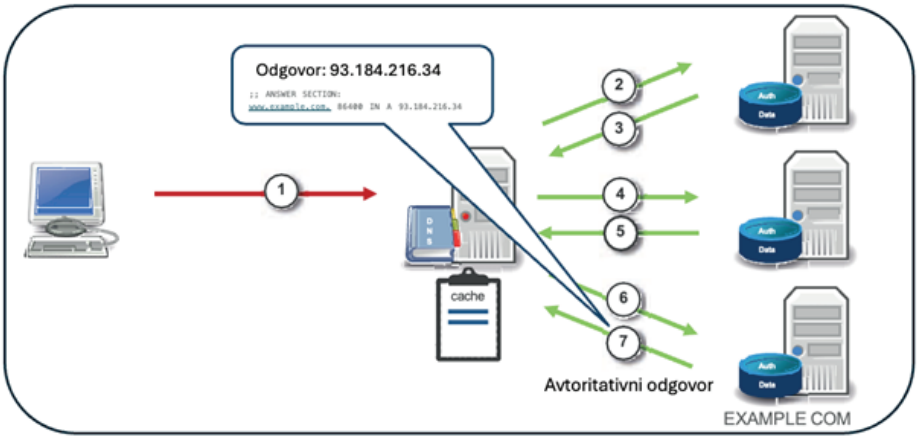
## 6 Iterativna poizvedba

Rekurzivni razreševalnik shrani v predpomnilnik odgovor (NS zapis za *example.com*) iz com strežnika. Rekurzivni razreševalnik se sam odloči, kateri *example.com* strežnik bo izbral in mu pošlje poizvedbo.



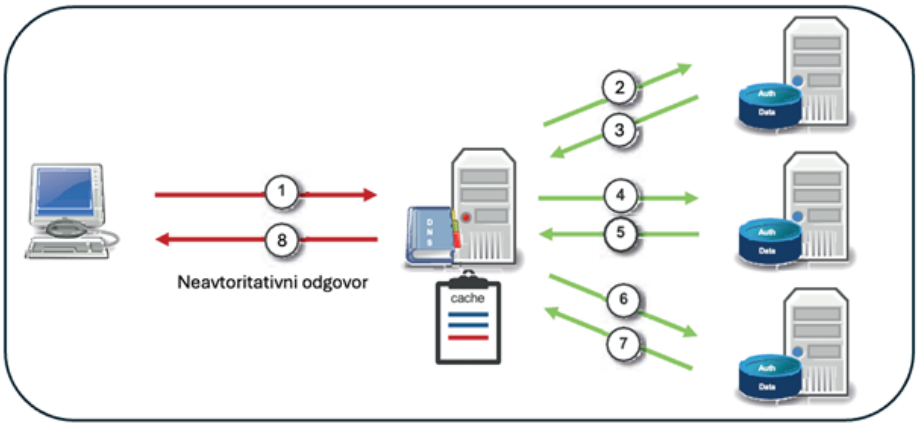

## 7 Avtoritativni odgovor

Avtoritativni *(Authoritative)* imenski strežnik za example.com odgovori z avtoritativnim odgovorom, ki vsebuje TTL *(Time to live)*. Če domena ne bi obstajala, bi odgovoril z NXDOMAIN *(non-existent domain)*.




## 8 Neavtoritativni odgovor

Rekurzivni razreševalnik shrani v predpomnilnik odgovor avtoritativnega imenskega strežnika za *example.com*. Rekurzivni razreševalnik posreduje neavtoritativni odgovor delovni postaji. Delovna postaja shrani v predpomnilnik odgovor rekurzivnega razreševalnika za *example.com*.

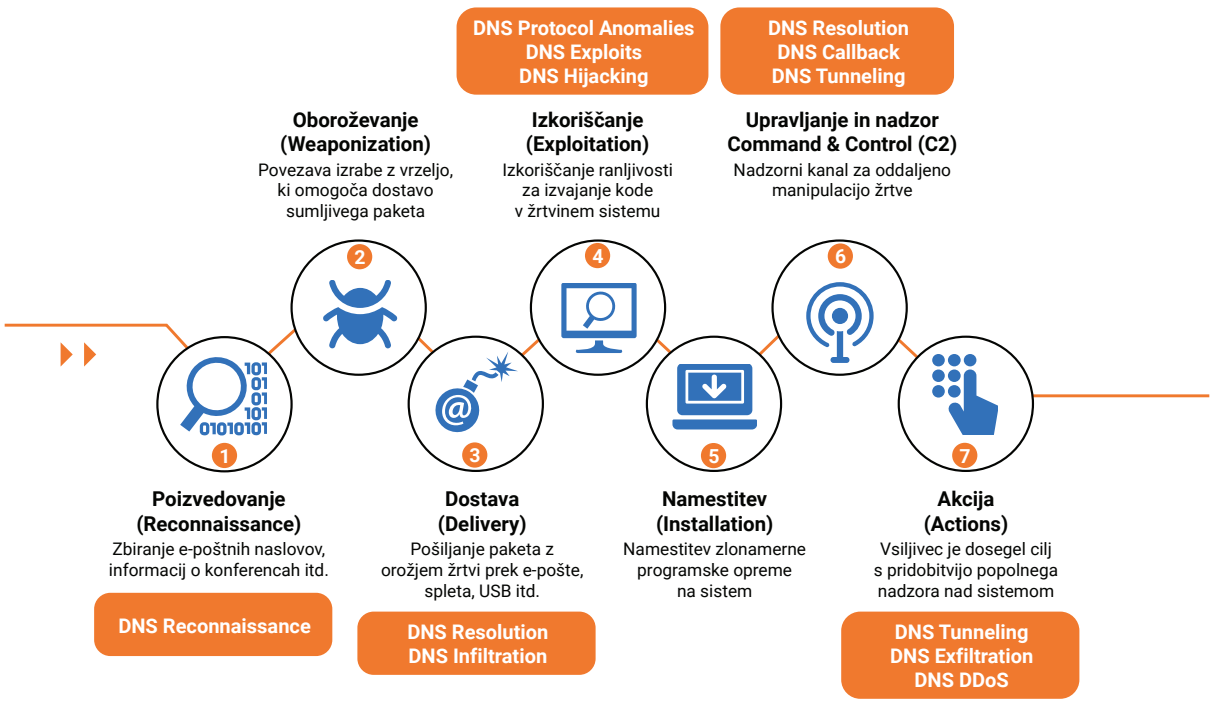


DNS je pogosta tarča kibernetskih napadov. Zato je pomembno, da je DNS sistem varen in zanesljiv. Varnost DNS sistema je ključna za varnost celotnega interneta. Z razumevanjem, kako deluje DNS in kakšne so najpogostejše grožnje, lahko organizacije sprejmejo ustrezne ukrepe za zaščito svojih sistemov in podatkov.

# 2. Kibernetska ubijalska veriga in DNS napadi

Model kibernetske ubijalske verige so zasnovali v podjetju Lockheed Martin in predstavlja zaporedje sedmih korakov, ki nam pomagajo razumeti, kako poteka kibernetski napad od začetka do konca. Gre torej za najpogosteje uporabljen konceptualni okvir, ki skuša razložiti metodologijo in motivacijo kibernetskih kriminalcev v celotnem časovnem obdobju napada. **Organizacijam pa pomaga razumeti grožnje in se ustrezno spopasti z njimi.**

Na spodnji sliki je predstavljenih vseh sedem korakov, ki so v nadaljevanju tudi podrobno opisani. Slika obenem prikazuje tudi pregled DNS napadov, ki se pojavljajo v posamezni fazi kibernetske ubijalske verige. Njim se bomo še podrobneje posvetili v naslednjem poglavju.




**S pomočjo modela lažje razumemo, kako napadalci izkoriščajo DNS, kakšne so različne faze napada, kje so šibke točke ter nenazadnje, kako se zaščititi.**

## 1 **Poizvedovanje** (Reconnaissance)

V prvi fazi gre za poizvedovanje. Napadalec skuša preveriti tarčo napada in o njej zbrati čim več informacij, ki mu pomagajo odkriti morebitne ranljivosti in potencialne vstopne točke. Gre lahko za preprosto zbiranje javnih e-poštnih naslovov ali pa za uporabo naprednih vohunskih orodij in avtomatiziranih skenerjev, ki odkrivajo tipe uporabljenih varnostnih sistemov ali aplikacij tretjih oseb.

Govorimo o **ključnem koraku** vsakega zahtevnega kibernetskega napada. Več podatkov kot napadalci pridobijo na tej stopnji, bolj uspešen bo napad.

## 2 **Oboroževanje** (Weaponization)

Na podlagi zbranih podatkov o žrtvi, predvsem njenih slabostih, pripravi napadalec strategijo napada. Ustvari zlonamerno programsko opremo in zlonamerne pakete, pri čemer izvede prilagoditev, ki bo ustrezala odkritim ranljivostim.

## 3 **Dostava** (Delivery)

V fazi dostave napadalec poskuša vdreti v ciljno omrežje. S pomočjo phishing elektronske pošte ali preko orodij za socialni inženiring skuša v omrežje prenesti zlonamerno programsko opremo. Druga možnost je vdor v omrežje in izraba ranljivosti v strojni ali programski opremi.

## 4 **Izkoriščanje** (Exploitation)

Po uspešni dostavi zlonamerne programske opreme ali drugih oblik vdora pridemo do faze izkoriščanja slabosti, ki so bile odkrite. Poleg tega lahko sedaj napadalec vdre še globje v omrežje in odkrije dodatne ranljivosti. V tej fazi se začne tudi **bočno premikanje po omrežju** iz enega na drug sistem. Na tej poti napadalec odkrije še dodatne potencialne vstopne točke.

## 5 **Namestitev** (Installation)

Napadalec poizkuša namestiti zlonamerno programsko opremo in z njeno pomočjo pridobiti dodaten nadzor nad več sistemi, uporabniškimi računi in podatki. Napadi se tako stopnjujejo, saj napadalec s silo prodira v ciljno omrežje ter išče nezaščitene varnostne poverilnice in spreminja nivo pravic kompromitiranih uporabniških računov.

## 6 Upravljanje in nadzor (Command and Control)

Eden od **ključnih korakov kibernetske ubijalske verige** je vzpostavitev kanala za upravljanje in nadzor, ki ga imenujemo C2. Ko napadalec pridobi nadzor nad delom ciljnega sistema ali uporabniškega računa, lahko na daljavo spremlja, nadzoruje in vodi svojo nameščeno kibernetsko orožje in zbirko orodij. To fazo lahko razdelimo na dve metodi:

- **Obfuskacija** je postopek, s katerim napadalec ustvari videz, kot da ni prisotna nobena grožnja in tako v bistvu zakrije svoje sledi. To vključuje metode, kot so brisanje datotek, binarno oblazinjenje in podpisovanje kode.

- **Zavračanje storitev** (DoS) je metoda, ko napadalec povzroča težave v drugih sistemih/področjih, da odvrne pozornost varnostnih ekip od odkrivanja glavnih ciljev napada. To pogosto vključuje zavrnitev storitve v omrežju ali zavrnitev storitve na končni točki, pa tudi tehnike kot so ugrabitev virov in zaustavitev sistema.

## 7 Akcija (Action)

V zadnji fazi napada napadalec želi doseči temeljni cilj napada. Proces lahko traja več tednov ali mesecev, odvisno od uspešnosti, dosežene v prejšnjih korakih. **Najpogostejši končni cilji kibernetskega napada so:**

- napad na dobavno verigo,
- odtekanje podatkov,
- šifriranje podatkov,
- stiskanje podatkov.

# 3. Opis DNS napadov

## 1 DNS reconnaissance

Za DNS poizvedovanje (reconnaissance) pogosto uporabljamo tudi izraz DNS enumeration. Gre za proces odkrivanja vseh DNS zapisov, povezanih z domeno. Poleg DNS strežnikov se odkrijejo poddomene, IP naslovi in ostale z DNS povezane informacije tarče.

| Record Type | Name | Description |
|---|---|---|
| **A** | Address (IPv4) | Maps a domain name to an IPv4 address |
| **AAAA** | Address (IPv6) | Maps a domain name to an IPv6 address |
| **CNAME** | Canonical Name | Maps an alias or subdomain to the canonical domain name. It is used to associate multiple domain names with a single IP address or hostname. |
| **NS** | Name Server | Specifies the authoritative name servers for a domain. It identifies the DNS servers responsible for a spacific domain. |
| **SOA** | Start Of Authority | Provides information about the authoritative name server for a domain. It includes details such as the primary name server for the domain, the email address of the responsible person, and various timers. |
| **MX** | Mail Exchange | Specifies the mail server respondible for handlong email messages for a domain. It identifies the hostname of the mail server that should receive email messages for a specific domain. |
| **SRV** | Service | Specifies the location of the services in a domain. It is used to define the location of the servers for a specific protocols, such as SIP (VoIP) |
| **TXT** | Text | Contains arbitrary text information. It is often used for verification purposes, such as domain ownership verifivation or email authentication. |

Primer uporabe "dig orodja" je prikazan na spodnji sliki.

```
term% dig www.example.com

; <<>> DiG 9.10.6 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8133
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 3364 IN A 93.184.215.14

;; Query time: 128 msec
;; SERVER: 77.111.1.1#53(77.111.1.1)
;; WHEN: Sat Jul 20 18:22:23 CEST 2024
;; MSG SIZE  rcvd: 60
```

Zanimajo nas podatki za strežnik *www.example.com*. Rezultat poizvedbe je prikazan na sliki levo. V **questions section** se prikaže tip poizvedbe. Privzeta nastavitev je poizvedba za A *record* zapis. V **answer section** se nahaja odgovor, ki nam pove, v kateri IP naslov se preslika ime strežnika. V zadnjem delu izpisa "dig" ukaza se nahajajo statistični podatki o tem, kateri imenski strežnik je posredoval odgovor in v kakšnem času.

# 2 DNS resolution

DNS preslika človeško berljiva domenska imena v strojno berljive IP naslove. Proces translacije imenujemo DNS resolution (o čemer smo podrobneje pisali v 1. poglavju). Uporabnikom omogoča dostop do spletnih strani in online storitev z uporabo enostavno zapomnljivih domenskih imen. Proces vključuje zaporedje rekurzivnih in ponavljajočih poizvedb, ki jih izvajamo v distribuirani in hierarhični infrastrukturi DNS strežnikov, razreševalnikov in predpomnilniških mehanizmov.

Primer verifikacije DNS preslikave z uporabo orodja "nslookup" je prikazan na spodnji sliki.

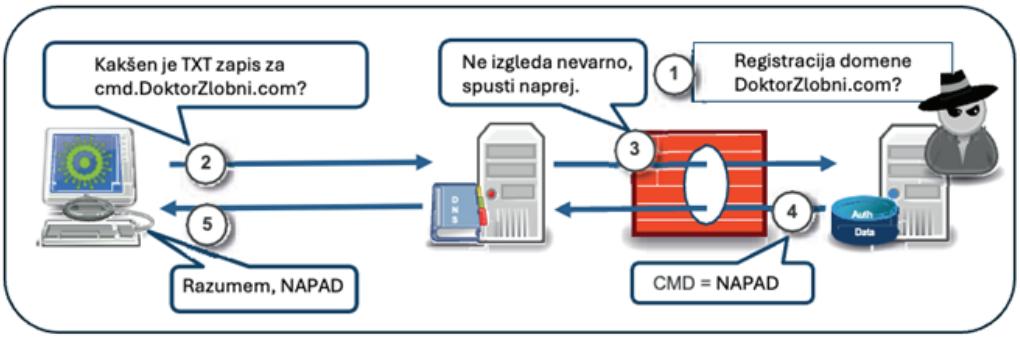
```
term% nslookup www.example.com
Server: 77.111.1.1
Address: 77.111.1.1#53

Non-authoritative answer:
Name: www.example.com
Address: 93.184.215.14
```

# 3 DNS tunneling

DNS tuneliranje je metoda kibernetskega napada, pri kateri se podatki aplikacije ali protokola kodirajo v DNS zahtevkih in odgovorih. V podatkovnem delu tuneliranih paketov, ki se naložijo na napadeni DNS strežnik, se lahko nahajajo podatki, ki se uporabijo za upravljanje oddaljenega strežnika in aplikacij.

Ta tip napada omogoča napadalcem, da ohranjajo vzpostavljeno povezavo za eksfiltracijo ukradenih podatkov. DNS uporabi za prikrito komuniciranje in gre tako neopazno skozi požarno pregrado. Napadalec v njem tunelira SSH ali HTTP protokol. Na spodnji sliki je prikazan postopek tuneliranja. To omogoča prenos datotek ven iz lokalnega omrežja in namestitev nove zlonamerne kode. S pomočjo DNS tunela je možno zaobiti vhodni *(captive)* portal in se s tem izogniti temu, da moramo zaprositi za uporabniško ime in geslo.




# 4 DNS infiltration

DNS infiltracija pomeni prenos podatkov iz Interneta v lokalno omrežje. Temelji na DNS tuneliranju. Podatke v omrežje je možno poslati znotraj različnih DNS zapisov:

- A zapis dovoli uporabo 4 bajtov,
- AAAA zapis dovoli uporabo 16 bajtov,
- MX zapis dovoli uporabo 2 bajtov + domensko ime (255 bajtov),
- CNAME zapis dovoli uporabo do 110 bajtov,
- TXT zapis dovoli uporabo do N x 220 bajtov,
- NULL zapis dovoli uporabo do 256 bajtov.

# 5 DNS protocol anomalies

O DNS protokolnih anomalijah govorimo, ko gre za neveljaven DNS promet in DNS podatke, ki niso v skladu s standardi. Zlonamerni programi ustvarjajo DNS pakete, ki kršijo obliko veljavne glave DNS. To je mogoče odkriti na ravni omrežja in s pomočjo skripte, ki je sposobna analizirati pakete in dekodirati DNS promet ter preverjati veljavnost. DNS nepravilnosti se lahko odkriva v realnem času ob samem prihodu paketov. Druga metoda izvaja statistično analizo velikega nabora podatkov. S tem lahko odkrivamo nepravilnosti v količini poizvedb ali v odzivih na poizvedbe v določenem časovnem obdobju.

### Indikatorji DNS anomalij so:

- povečanje števila DNS paketov,
- zmanjšanje deleža zadetkov v predpomnilniku,
- povečanje povprečnega števila DNS poizvedb posameznih izvornih IP naslovov,
- povečanje števila rekurzivnih poizvedb,
- povečanje števila izvornih IP naslovov v omejenem časovnem intervalu,
- zmanjšanje razmerja rešenih poizvedb.

# 6 DNS exploits

DNS exploit pomeni, da napadalec izrabi ranljivost v DNS protokola, preko katere vdre v omrežje.

### Med najbolj pogoste izrabe spadajo:

- anomalija protokola,
- DNS tuneliranje,
- botneti,
- ojačitev in preusmeritev DNS prometa,
- zavrnitev storitve pri porazdeljenem prometu (DDoS),
- izsiljevalska programska oprema.

# 7 DNS hijacking oz. redirection

DNS ugrabitev opisuje napad, pri katerem napadalec zavede klienta, da komunicira z legitimnim domenskim imenom, pa čeprav v resnici komunicira z domenskim imenom oziroma IP naslovom, ki ga nadzoruje napadalec. Drugo ime za tak tip napada je DNS preusmeritev *(DNS redirection)*.

Najbolj običajna metoda napada je, da napadalec spremeni DNS nastavitve uporabnika na način, da začne uporabljati DNS strežnik pod napadalčevim upravljanjem. Drugi način je pridobitev nepooblaščenega dostopa do avtoritativnih DNS podatkov, s pomočjo kraje gesel ali izkoriščanja DNS ranljivosti.

Obstajajo tudi *homograph* napadi, pri katerih se uporablja podobne *(lookalike)* domene. Primer je napad s pomočjo paypai.com domene. Znani so tudi napadi, ki s pomočjo java skripte skrijejo ali pa celo zamenjajo oziroma prikazujejo napačno URL vrstico.

# 8 DNS callback

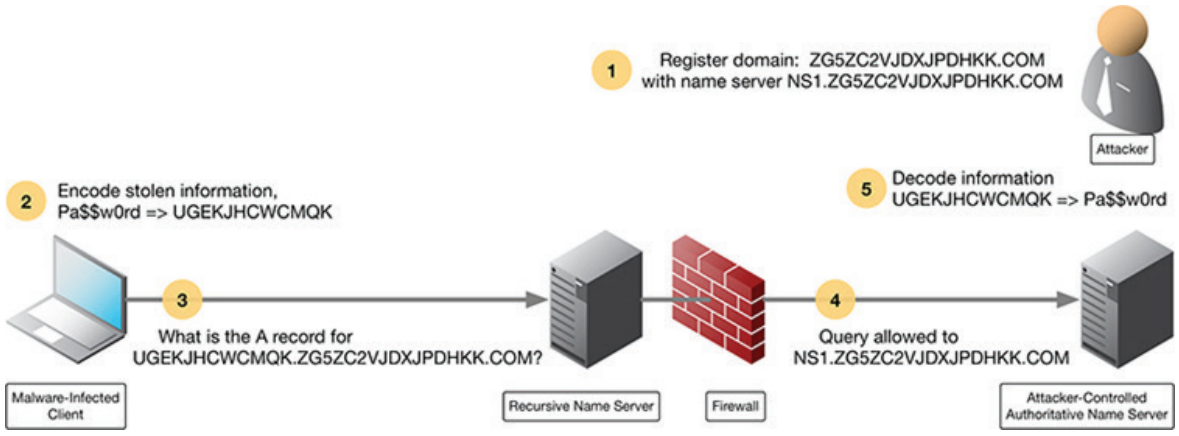
DNS callback aktivnost se pojavlja pri Fast Flux napadih. Gre za posebno tehniko napadov, pri kateri napadalec poveže veliko število IP naslovov z eno domeno. IP naslovi se menjajo zelo hitro s pomočjo DNS zapisov. Fast flux omrežje je sestavljeno iz velikega števila kompromitiranih delovnih postaj, ki so flux agenti. Dejanski C2 strežnik se skriva za temi IP naslovi in ga je težko odkriti. S pomočjo spremljanja DNS odgovorov, ki so v bistvu povratni klici, skušamo poiskati DNS promet, povezan s sumljivo domeno.

# 9 DNS exfiltration

DNS eksfiltracija uporablja DNS tuneliranje. V tem primeru mora biti klient sposoben izvajati DNS poizvedbe. V primeru odtujitve podatkov se klienti izognejo odkrivanju tako, da podatke razčlenijo na koščke v velikosti poizvedb, saj tako izgledajo kot DNS poizvedbe in jih pošljejo zlonamernim DNS strežnikom na oddaljeni lokaciji. Tam se poizvedbe razpakirajo in rekonstruirajo v odtujene podatke.

**Primer DNS eksfiltracije je prikazan na spodnji sliki:**

1. Napadalec registrira domeno ZG5ZC2VJDXJPDHKK.COM in postavi imenski strežnik NS1.ZG5ZC2VJDXJPDHKK.COM
2. Na okuženem klientu se ukradena vsebina (zapis “Pa$$w0rd”) kodira v “UGEKJHCWCMQK”
3. Klient naredi DNS poizvedbo za domeno s kodirano besedo, ki predstavlja poddomeno: UGEKJHCWCMQK.ZG5ZC2VJDXJPDHKK.COM.
4. Rekurzivni imenski strežnik poišče avtoritativni imenski strežnik NS1.ZG5ZC2VJDXJPDHKK.COM in mu pošlje poizvedbo.
5. Napadalec prepozna poddomeno, kot kodirano besedilo in ga dekodira v “Pa$$w0rd”.




V tem primeru ni potrebno, da dobi klient odgovor, saj je bil cilj odtujitev podatkov. Lahko pa bi v proces brez težav vključili pošiljanje zlonamerne vsebine klientu.

# 10 DNS DDoS

Obstaja več vrst napadov zavrnitve storitve pri porazdeljenem prometu (DDoS-Distributed Denial of Service). Glavni namen teh napadov je preobremenitev DNS strežnikov z namenom onemogočiti delovanje DNS storitev. Ko podjetje ne more objaviti naslovov za svoje spletne in poštne strežnike, se poslovanje ustavi.

Poznamo dve glavni metodi DDoS napadov in kombiniran napad.

### a) DDoS napad z ojačitvijo (Amplified Attack)

Napadalec uporabi tehniko, pri kateri lahko majhna poizvedba sproži ogromen odziv. Na primer poizvedba za TXT zapis ali prenos cone, pri čemer ni poskrbljeno, da se prenos cone izvaja samo do lastnih zaupanja vrednih virov.

S poplavljanjem strežnika z majhnimi zahtevki, ki zahtevajo obsežne odgovore, lahko relativno šibek računalnik obremeni DNS strežnik. Primer je prikazan na spodnji sliki.

DNS strežnik je tako zaposlen z odgovarjanjem na lažne zahtevke, da nima časa odgovarjati na legitimne. Sam DNS strežnik postane ojačevalnik, saj lahko poizvedba velika 44 bajtov sproži odgovor dolg 4077 bajtov (približno 93-kratna ojačitev). Računalnik z 1 Mb/s povezavo lahko tako prepriča DNS strežnik, da zgenerira 93 Mb/s prometa. 11 računalnikov pa že 1Gb prometa, ki predstavlja napad.

### b) DDoS napad z odbojem (Reflection Attack)

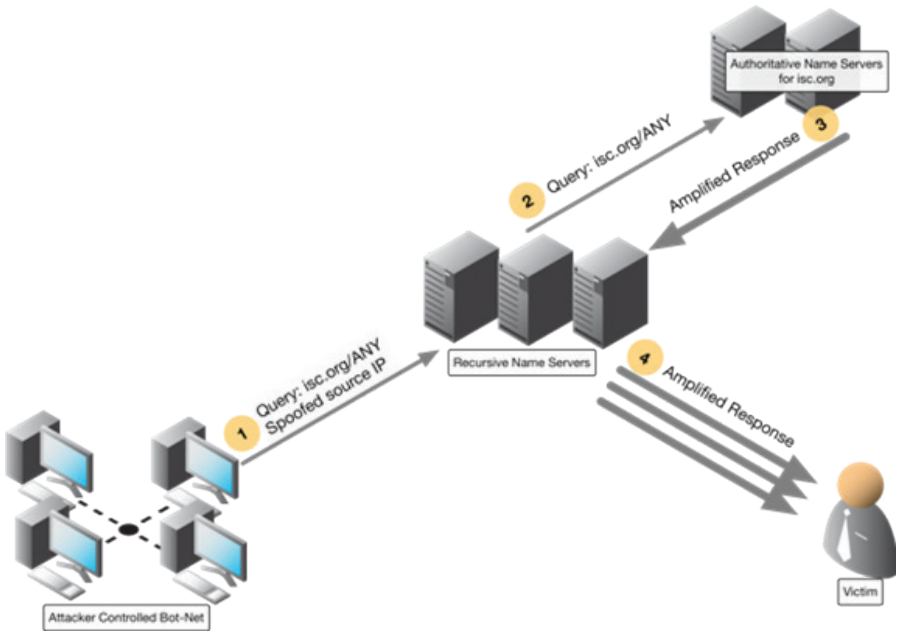
Napad z odbojem pošilja poizvedbe, ki izgledajo tako, kot da bi prišle s strani žrtve napada. Odgovor (običajno obsežen in ojačan) je poslan žrtvi, ki nikoli ni naredila poizvedbe. Velikost odgovora je tako velika, da lahko poplavi omrežje žrtve.

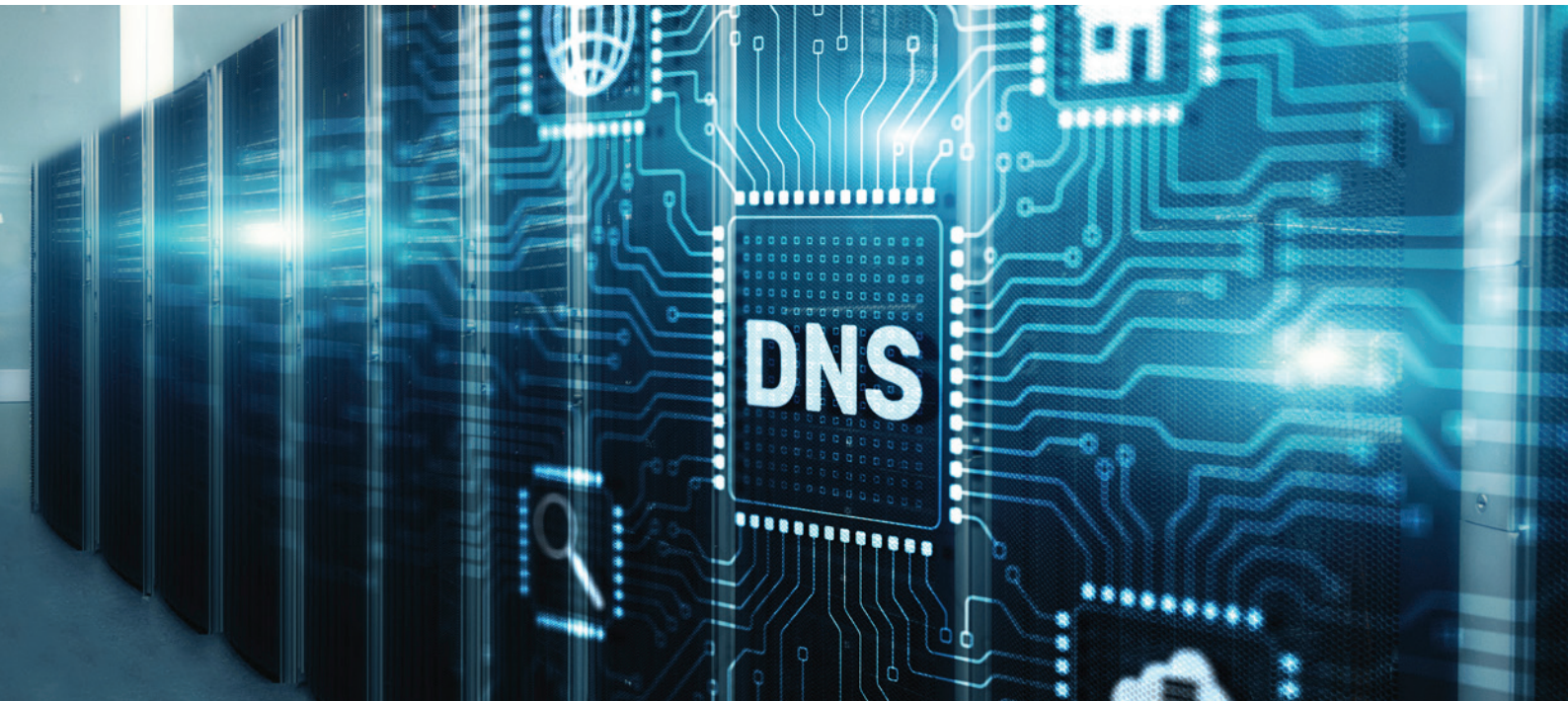
Spodnja slika prikazuje napad z odbojem, pri katerem napadalec pošlje poizvedbo rekurzivnemu imenskemu strežniku z izmišljenim (spoofed) izvornim IP naslovom.

Napadalec kot izvorni naslov namesto svojega dejanskega IP naslova uporabi IP naslov žrtve. Rekurzivni imenski strežnik opravi svoje običajno delo, tako da pridobi odgovor na poizvedbo s strani avtoritativnega imenskega strežnika in ga pošlje nič hudega sluteči žrtvi.

### c) Kombinirani DDoS napadi

Napadalci uporabljajo kombinacijo obeh tehnik IP naslov (spoofed) žrtve in pošiljanje natančno pripravljenih poizvedb, ki se odražajo v velikih paketih. Spodnja slika prikazuje, kako v prvi fazi avtoritativni strežnik izvede ojačitev, medtem ko v drugi fazi rekurzivni strežnik izvede odboj. Tak način omogoča napadalcu istočasno izvedbo napada na dve žrtvi. Obstaja možnost, da žrtev napada z ojačitvijo misli, da je bila napadena s strani druge žrtve, kar povzroči še večjo zmešnjavo.



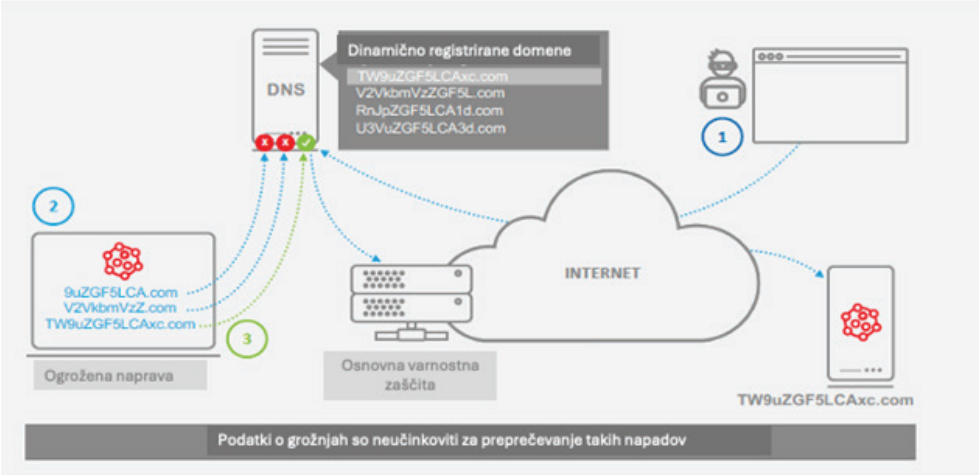



# 4. Kaj je DGA (Domain Name Algorithms)

Napadalci iščejo vedno nove načine, kako se izogniti zaščiti podjetij in ukrasti dragocene podatke in jih spremeniti v zaslužek. Bolj kot je njihov pristop dinamičen, bolj uspešni so pri izogibanju varnostnim kontrolam, ki uporabljajo statične metode, kot so črne liste, ki se ne posodabljajo pogosto.

Ena od naprednih tehnik, ki jo napadalci uporabljajo, se imenuje DGA *(Domain Generation Algorithm)* oziroma **algoritem za generiranje dinamičnih domen**. DGA je programska koda za generiranje domen, ki jih klienti, sodelujoči pri napadu z zlonamerno kodo, uporabljajo v fazi povezovanja s strežniki za upravljanje in nadzor *(Command and Control)*. V trenutku, ko varnostni sistem odkrije in blokira eno izmed dinamično generiranih domen, zlonamerni klient in C2 strežnik preklopita na naslednjo na seznamu in se tako izogneta blokadi. Postopek je prikazan na spodnji sliki:

1. Napadalec uporabi algoritem za kreiranje dinamičnih domen.
2. Zlonamerna koda uporabi isti algoritem za iskanje strežnikov za upravljanje in nadzor *(Command and Control)*.
3. Veljavna in dosegljiva domena omogoča povezavo z zlonamernim strežnikom, kjer se nahaja zlonamerna koda.




### DGA domene imajo naslednje karakteristike:

- Imajo dolga, nesmiselna imena s končnico .com, saj je tako manj možnosti, da bi se prekrivale z obstoječimi, registriranimi domenami.
- Običajno so kodirane ali kriptirane z istimi kriptografskimi algoritmi, ki jih uporabljata zlonamerni klient in C2 strežnik in jih je tako težko dekodirati ali dekriptirati.
- Na tisoče DGA domen se generira v enem dnevu, vendar jih je samo nekaj aktivnih ali razrešljivih ter hkrati znanih zlonamernim klientom in C2 strežnikom.
- Tudi ko so aktivne, imajo kratko življenjsko dobo (običajno samo nekaj dni) in jih je prav zaradi tega težko uvrstiti na črno listo.

Zaradi dinamičnega spreminjanja jih je težko odkriti in blokirati s pomočjo črnih list, ki vsebujejo domenska imena. Večina algoritmov uporablja različne pristope za naključno razvrščanje črk v delu domenskega imena, pred delom .com. Ker se te domene nenehno spreminjajo glede na statično in dinamično osnovo, jih je zelo težko odkriti.

Tehnika DGA je postala popularna v času Confiker črva leta 2008, ko se je generiralo 250 domen na dan. Pri novejši verziji Conficker (.C) se generira 50.000 domen na dan, čemur je še težje slediti.

Potrebno je opozoriti, da se lahko menjajo tudi IP naslovi, v katere se preslikajo DGA domene in se tako skušajo izogniti požarnim pregradam, ki uporabljajo črne liste z IP naslovi. V tem primeru se izvajajo *Fast Flux* napadi. Gre za posebno tehniko napadov, pri kateri napadalec poveže veliko število IP naslovov z eno domeno. IP naslovi se menjajo zelo hitro s pomočjo DNS zapisov. *Fast Flux* omrežje je sestavljeno iz velikega števila kompromitiranih hostov, ki so flux agenti. Dejanski C2 strežnik se skriva za temi IP naslovi in ga je težko odkriti. Poleg tega se je potrebno zavedati, da C2 omrežja ne gostijo zlonamerne vsebine, ampak so zadolžena samo za preusmeritev na dejanske strežnike z zlonamerno vsebino.

# 5. Response policy zone (RPZ)

S pomočjo *Response policy zones* (RPZs) lahko nadziramo, kakšne poizvedbe lahko in kakšne se ne sme izvajati proti rekurzivnemu razreševalniku.

Na podlagi ugleda strežnikov in storitev, po katerih klienti poizvedujejo, je možno določiti ukrepe, ki jih je potrebno sprejeti, ko rekurzivni razreševalnik prejme poizvedbo za določeno domeno ali opazi informacijo v DNS odzivu, ki nakazuje, da gre za zlonamerni strežnik.

Glavna ideja delovanja RPZ je v tem, da se nastavi politike, ki določajo, kako se obravnava določene poizvedbe (ali odgovore) in se izbere, katera akcija bo izbrana. Primeri možnih akcij vključujejo preusmeritev zahteve klienta na notranje varnostne strani in hranjenje politik v posebnih avtoritativnih conah v lastnih DNS strežnikih. Podprt je tudi prenos RPZ con iz enega na drug DNS strežnik.

RPZ podatke je možno dobiti pri ponudniku informacij o grožnjah, lahko pa jih ustvarimo tudi sami. Lastne oziroma lokalne RPZ, ki vsebujejo bele in črne liste, prevladajo nad zunanjimi.

Priprava RPZ temelji na konceptu ugleda, ki opisuje zgodovino ponujanja zlonamerne vsebine določene cone. Različne storitve ugleda, ki jih imenujemo tudi *Threat Intelligence*, sledijo in analizirajo ponudnike zlonamernih vsebin. *Threat Intelligence* skuša loviti napadalce, predvideva njihovo naslednjo potezo in ugotavlja algoritme, ki ji uporabljajo za generiranje novih slabih domen. Ti podatki so na voljo vsem v obliki RPZ, ki jih uporabimo v politikah za zaščito DNS con.

### Kako deluje DNS RPZ zaščita?


1. Okužena naprava se je povezala v lokalno omrežje. Zlonamerna okužba se razširi na ostale naprave.
2. Zlonamerna okužba naredi DNS poizvedbo, da bi našla C2 strežnik. Funkcionalnost DNS požarne pregrade preverja DNS odgovore in izvaja s strani administratorja nastavljene akcije (prepreči komunikacijo do zlonamernih strani ali preusmeri promet do interne strani za ozaveščanje uporabnikov).
3. V SIEM ali v obliki poročila pošlje spisek RPZ zadetkov vključno z izvedeno akcijo.
4. Posodobitve se dogajajo občasno oziroma ob nevarnih grožnjah.
5. *Threat intelligence*, ki ga uporablja DNS, prihaja iz različnih virov.

RPZ je orodje, ki nam omogoča, da imamo večji nadzor nad tem, kaj lahko naši uporabniki počnejo na internetu.

# 6. Kako odkrijemo DNS eksfiltracijo

Ker napadalec obvladuje oba konca komunikacije, si lahko sam izbere tip kodiranja, ki ga bo uporabil. Tip kodiranja se lahko časovno spreminja, da se izogne detekciji. Vzorec, ki je uporabljen danes, je lahko jutri drugačen. Ena od možnosti za preprečevanje enostavnih DNS eksfiltracij je blokada zlonamernih domen s pomočjo tehnologije *Response policy zones* (RPZs), opisane v prejšnjem poglavju.

Ker se napadalci zavedajo, da obstajajo RPZ, registrirajo več domen, ki jih rotirajo in se tako izognejo detekciji. Tako blokada ene sumljive domene (ZG5ZC2VJDXJPDHKK.COM iz primera v tretjem poglavju) ne bo učinkovito blokirala napada. Tak način je pogosto v uporabi, saj napadalci uporabljajo Domain Generation Algorithm (DGA) (opisan v četrtem poglavju), ki avtomatično generira naključna

domenska imena in jih registrira več sto ali tisoč hkrati. Take poizvedbe je zelo težko spoznati.
Za odkrivanje DNS podatkovne eksfiltracije je potreben kompleksen proces leksikalne analize, ki je zahteven zaradi velikega števila in pogostega pojavljanja DNS poizvedb. Pri tem pomaga vrhunska računalniška moč in strojno učenje, ki odkriva DNS podatkovno eksfiltracijo hitreje in z večjo natančnostjo.

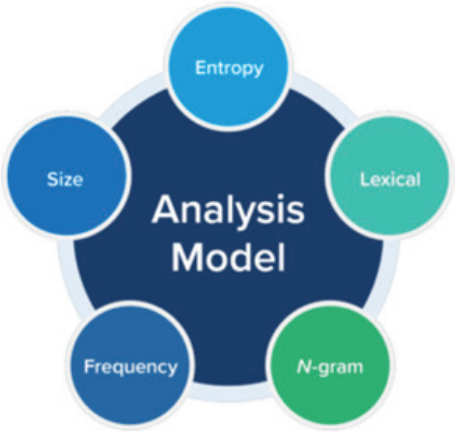
**Obstajata dve glavni metodi odkrivanja DGA napadov:**

- **Metoda povratnega inženiringa:** V primeru, da obstaja dostop do izvorne kode zlonamerne programske opreme (in morda strežnikov) lahko izračunamo naslednji seznam DGA domen. Druga možnost je, da se na podlagi zaporedja že opaženih DGA domen ugane ali oceni algoritem. Ta metoda ima kar nekaj pomanjkljivosti.

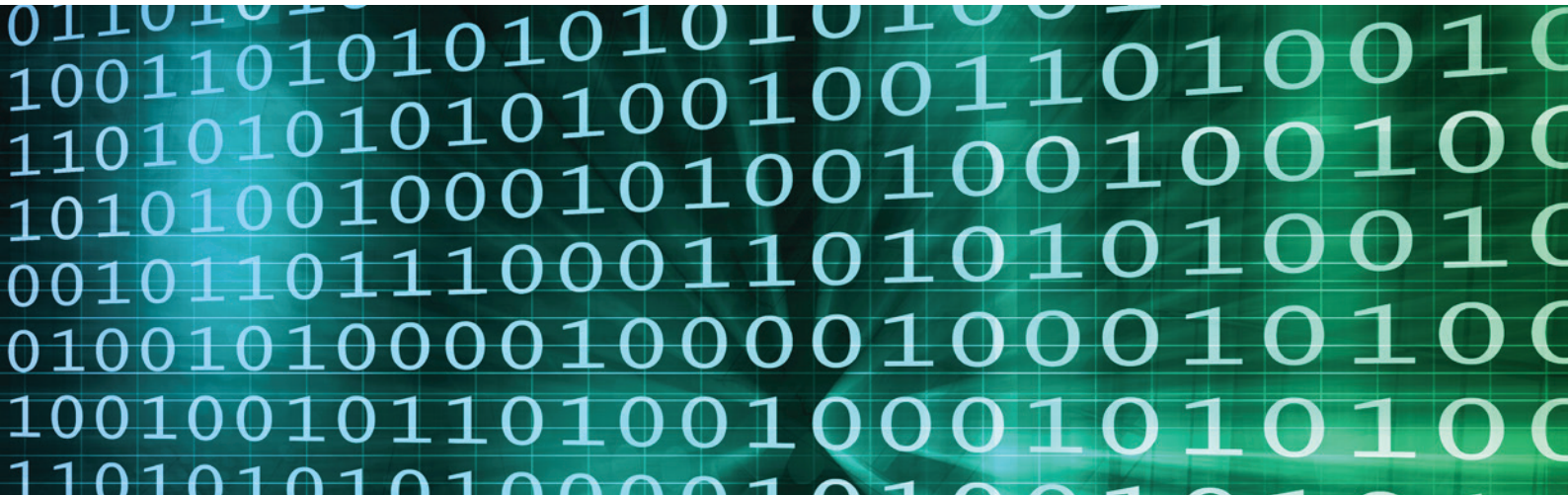
- **Metoda strojnega učenja:** Je bolj zanesljiva in robustna. Na podlagi obstoječega vzorca domenskih imen, ki jih generira DGA, lahko zgradimo podatkovne modele in predvidimo neznane DGA, ki bodo uporabljene.

Statistični modeli, ki jih uporablja strojno učenje, so ustrezen način odkrivanja DGA domenskih imen. Na spodnji sliki so predstavljeni dejavniki, ki jih je potrebno upoštevati:

- **Entropija (Entropy):** Koliko naključnosti je v imenu domene?
- **Leksikalno (Lexical):** Ali se zdi, da je kodirano ali šifrirano?
- **N-gram:** Ali ime domene vsebuje besede v jeziku?
- **Pogostost (Frequency):** Kako pogosto se pojavlja domensko ime? Ali je poslanih preveč zahtevkov za isto domeno?
- **Velikost (Size):** Ali je ime domene nenavadno dolgo?




Vsaki od zgoraj omenjenih statističnih karakteristik se dodelijo točke. Posamezne točke prispevajo k konsolidirani oceni. Ko le-ta preseže prag, lahko varnostni analitik določi, če je domena uporabljena s strani zlonamerne programske opreme ustvarjena z DGA.



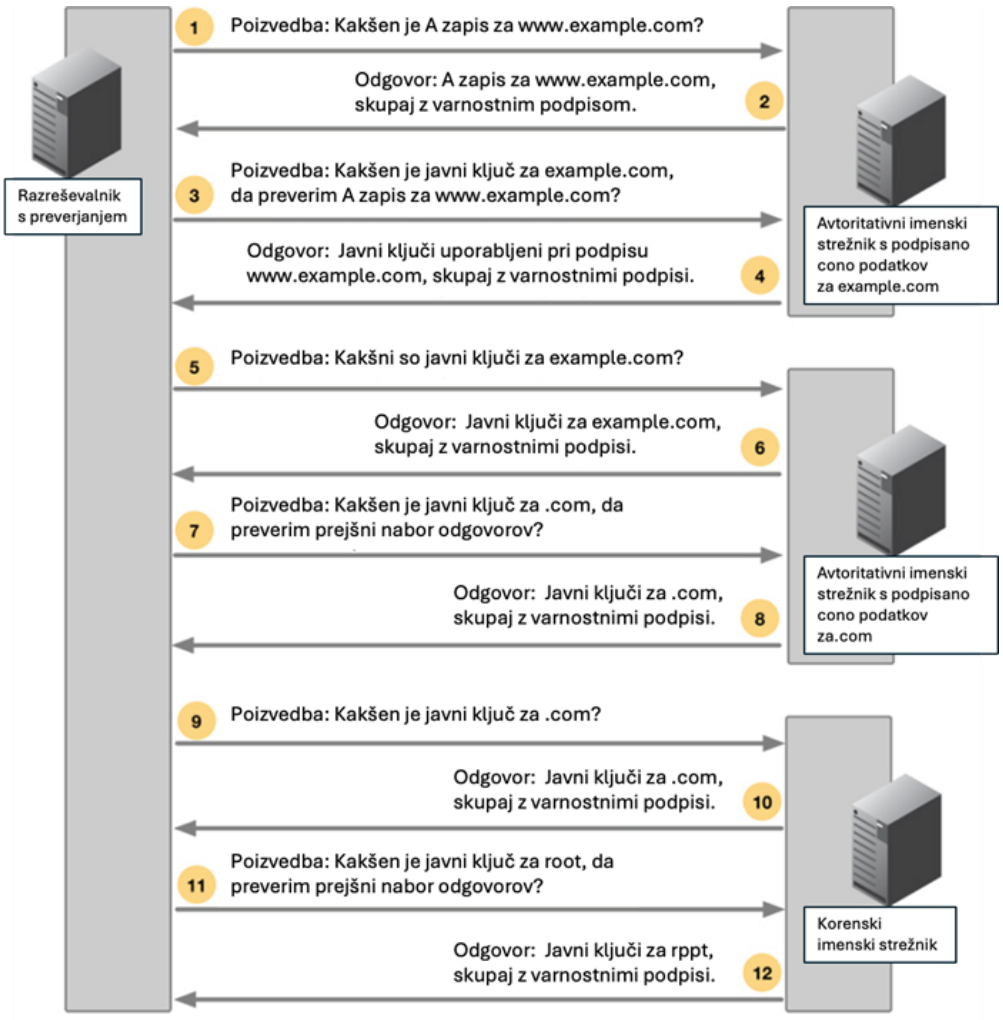
# 7. DNSSEC

*DNS Security Extensions* (DNSSEC) želi odpraviti pomanjkljivosti pri zagotavljanju varnosti DNS prometa. DNSSEC omogoča potrditveni odgovor s pomočjo uporabe javne kriprografije (PKI). PKI uporablja par ključev, od katerih je en javni drug pa privatni. To omogoča DNS strežniku, da preveri, da je odgovor na poizvedbo prišel od pošiljatelja, za katerega se predstavlja (to z drugimi besedami pomeni, da odgovor ni prišle iz podtaknjenega naslova) in da vsebina sporočila ni bila spremenjena med samim prenosom. Ključi za podpisovanje con kriptirajo podatke, ki se lahko preberejo samo z drugim ključem. Ta proces zagotavlja avtentikacijo in integriteto sporočila.

DNSSEC je povratno kompatibilen, kar pomeni, da ga lahko vzpostavimo vzporedno s tradicionalnim DNS-om. V primeru, da domena še ne podpira DNSSEC, se DNSSEC imenski strežnik obnaša kot običajni DNS.

DNSSEC ne kriptira prometa, saj se par javno/privatnega ključa uporablja samo za avtentikacijo. Tako je še vedno možno branje DNS sporočil, ni pa možno njihovo spreminjanje ali podtikanje. DNSSEC zahteva implementacijo na rekurzivnem in avtoritativnem imenskem strežniku. Rekurzivni imenski strežnik sprašuje za dodatne varnostne informacije in izvaja validacijske postopke, medtem ko avtoritativni imenski strežnik podpisuje zapise in odgovore samih virov.

Na spodnji sliki je prikazan poenostavljen postopek delovanja rekurzivnega imenskega strežnika, ki ga v tem primeru imenujemo razreševalnik s preverjanjem.



Razreševalnik s preverjanjem na vsakem koraku preverja dodatne varnostne informacije. Preverjanje se vrši do vrhnje domene in se konča, ko poda odgovor korenski imenski strežnik. Javni ključ korenskega imenskega strežnika je edini ključ, ki mu razreševalnik s preverjanjem zaupa.

*DNS spoofing* (DNS s podtaknjenim naslovom) je poznan tudi kot t. i. *cache poisoning*. Gre za tip napada, pri katerem se podtakne pokvarjene podatke v predpomnilnik DNS razreševalnika, kar povzroči, da le-ta posreduje napačne podatke. Pogosto se uporablja v kombiniranih napadih in ga je zelo težko odkriti. Ustrezna uporaba DNSSEC to prepreči. DNSSEC okrepi tudi druge varnostne zaščite. Veliko organizacij objavlja anti-spam informacijo kot so SPF *(Sender Policy Framework)* ali DKIM *(DomainKeys Identified Mail)*, ki temeljita na DNS.

Vedno več izdajateljev certifikatov *certificates authorities* (CA) zahteva uporabo *Certificate Authority Authorization* (CAA) zapisa pri izdaji novih SSL/TLS certifikatov, kot drugi dejavnik avtentikacije.

Uporaba DNSSEC omogoča podjetjem, da bolje zaščitijo svoje spletne storitve.

# 8. DNS Client Security

V prejšnjem poglavju smo govorili o DNSSEC, ki zagotavlja varnost med DNS strežniki, ne pa tudi med lokalnim DNS strežnikom in klientom. To zagotovimo z *DNS Client Security*, ki jo je možno izvajati na dva načina:

- DNS over TLS *(Transport Layer Security)* ali “DoT”
- DNS over HTTPS ali “DoH”

Obe funkcionalnosti zagotavljata zasebnost uporabnika, vendar po drugi strani uporabnikom omogočata, da se izognejo uveljavljeni DNS zaščiti podjetja. Tako so lahko izpostavljeni podatkovni eksfiltraciji in širjenju zlonamerne programske opreme.

## 1 DNS over TLS (Transport Layer Security) ali “DoT”

DoT uporablja TCP vrata 853 za varno DNS komunikacijo, ki temelji na TLS. DoT DNS klient poskuša naprej komunicirati z DNS strežnikom, ki podpira DOT na vratih 853 in vzpostavi TLS izmenjavo. DoT klient dobi strežniški certifikat in preveri njegovo veljavnost. Nato generira simetrični enkripcijski ključ, ki se uporabi za enkripcijo podatkov. DoT uporablja isto tehnologijo kot se uporablja za spletne strežniške certifikate. Razlikuje se samo v uporabi drugih TCP vrat.

**DoT podpira dva načina:**

- *strict* način: DOT klient ima spisek zaupanja vrednih certifikatov DoT strežnika in komunicira s samo zaupanja vrednimi DoT strežniki.
- oportunistični način: DoT klient poskuša komunicirati z vsemi DNS strežniki preko vrat TCP 853. V primeru, ko ne uspe vzpostaviti varnega komunikacijskega kanala, se vrne nazaj na vrata 53, kjer se vzpostavi običajna nezaščitena DNS komunikacija.

V primeru uporabe DoT gre samo za enkripcijo podatkov, ne pa za preverjanje avtentikacije in integritete, ki jo zagotavlja DNSSEC. DoT se lahko uporabi tudi za varno komunikacijo med strežniki, hkrati z DNSSEC. DOT je zaradi uporabe TCP bolj potraten in izpostavljen TCP napadom.

## 2 DNS over HTTPS ali “DoH”

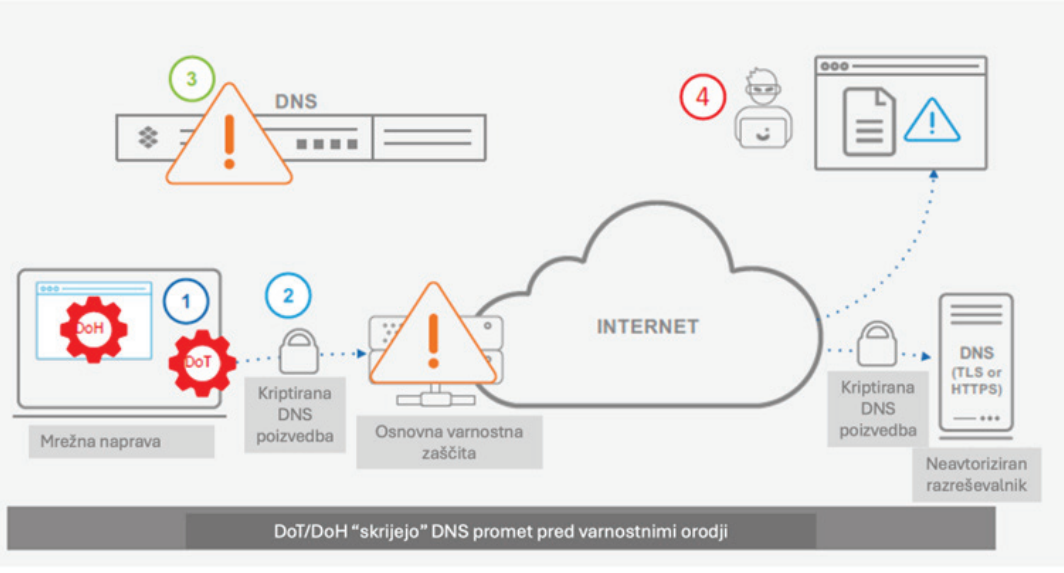
DoH klient komunicira z DNS strežnikom TCP vrat 443. DoH klient dobi strežniški certifikat, ga preveri in generira simetrični enkripcijski ključ, ki se uporabi za enkripcijo podatkov. DoH se obnaša podobno kot spletni strežnik, le da zakodira DNS podatke znotraj HTTPS seje v obliki GET in POST sporočil.

DoH ščiti komunikacijo med klientom in strežnikom, ni pa sposoben nuditi zaščite za komunikacijo med dvema strežnikoma. Prav tako ne zagotavlja preverjanja avtentikacije in integritete.

Zasebnost uporabnikov je lahko po eni strani dobra stvar, vendar pa lahko po drugi strani povzroči še večjo izpostavljenost, ko govorimo o zaščiti uporabnikov v podjetjih.

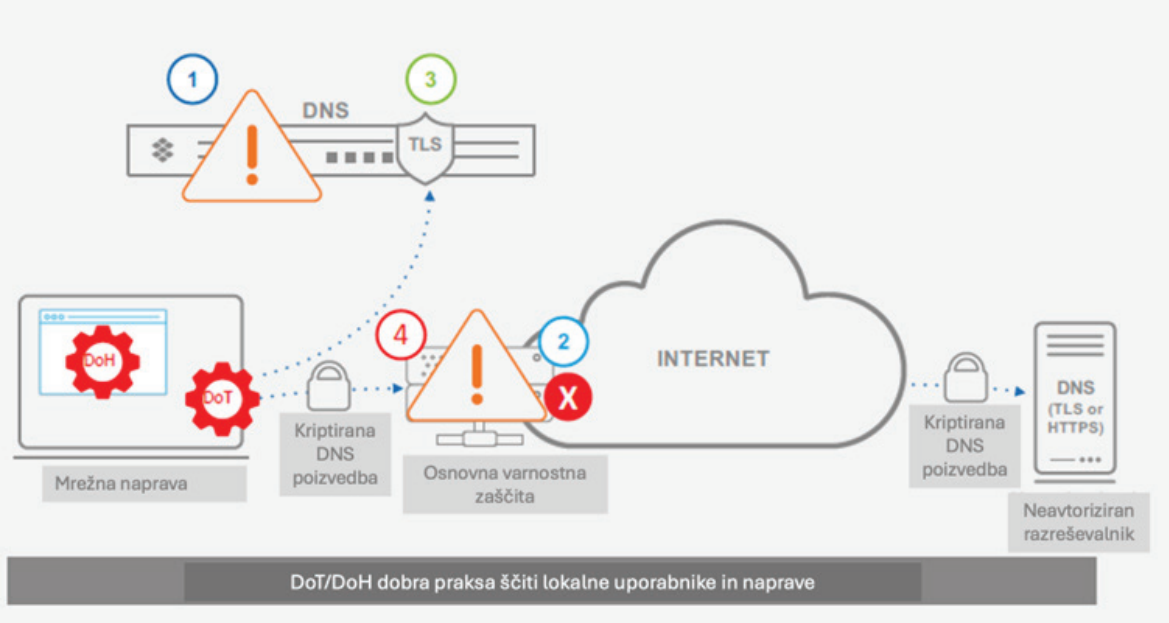
**Na spodnji sliki je predstavljen izziv, ki smo mu priča v primeru uporabe DoT/DoH.**

1. Naprava, ki uporabi TLS ali spletni brskalnik z uporabo HTTPS ima nastavljen neavtoriziran DNS razreševalnik.
2. Zaradi uporabe DoT/DoH se kriptirane DNS poizvedbe pošljejo na zunanji razreševalnik.
3. Interni DNS razreševalnik smo zaobšli zaradi uporabe DoT/DoH in tako ni bil sposoben izvajati pregledovanja DNS prometa.
4. Napadalec lahko izrabi DoT za svoje zle namene.



**DoT/DoH dobra praksa sledi naslednjim korakom, ki so predstavljeni na spodnji sliki.**

1. Izogibanje internemu DNS strežniku ni dobra ideja.
2. Potrebno je preprečiti dostop do neavtoriziranih DNS strežnikov.
3. Uporabiti je potrebno interni DNS strežnik, ki podpira DoT, da se ohrani nadzor in varnost.
4. Blokada DoH z uporabo Threat Intel list neavtoriziranih razreševalnikov.




# DNS varnost - vaša prva obrambna linija v kibernetskem prostoru

Kibernetski napadalci vedno iščejo nove načine za izkoriščanje ranljivosti. Brez ustrezne zaščite so vaši podatki in storitve izpostavljeni nevarnostim, ki vodijo do finančne škode in izgube zaupanja strank.

DNS zaščita ne pomeni le preprečevanja napadov, ampak tudi zagotavljanje neprekinjenega delovanja vaših spletnih storitev.

**Smart Com strokovnjaki vam bodo pomagali do celovite rešitve za zaščito vaše omrežne infrastrukture. Zgradimo neprebojni obrambni sistem skupaj!**

www.smart-com.si 01 561 16 06 info@smart-com.si

SMART COM

Smart Com več kot 34 let deluje na področju IKT in je eden izmed vodilnih sistemskih integratorjev v Jugovzhodni Evropi. Naši strokovnjaki so specialisti na področju kibernetske varnosti v industriji, procesnih okoljih in okoljih kritične infrastrukture (ICS/OT/IoT), varnih in naprednih informacijsko-komunikacijsih sistemov in podatkovnih centrov. Vzpostavljamo dolgoročna poslovna partnerstva, ki temeljijo na medsebojnem zaupanju, strokovnosti in integriteti.

www.smart-com.si