Mechanizmus DDR v praxi

implementácia a fungovanie v sieti ISP

Blažej Krajňák | Levonet, s.r.o.
CSNOG 17.5.2023

Discovery of Designated Resolvers (DDR)

- RFC draft (draft-ietf-add-ddr-10)
- mechanizmus na objavenie šifrujúceho DNS servera
alebo objavenie alternatívnych šifrovaných protokolov
- stačí poznať IP adresu DNS servera
- podporu deklaruje Microsoft Windows 11, Apple iOS 16 a MacOS Ventura

Objavenie servera

- klientske zariadenie získa IP adresu DNS servera pomocou DHCP

109.236.119.2 / 109.236.120.2

2a02:6ca3:0:1::2 / 2a02:6ca3:0:2::2

Objavenie servera

- zariadenie sa opýta servera na **SVCB** záznam pre **_dns.resolver.arpa**

```
kdig -t svcb _dns.resolver.arpa @109.236.119.2
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 32382
;; Flags: qr aa rd ra; QUERY: 1; ANSWER: 2; AUTHORITY: 0; ADDITIONAL: 4

;; QUESTION SECTION:
;; _dns.resolver.arpa. IN SVCB

;; ANSWER SECTION:
_dns.resolver.arpa. 900 IN SVCB 1 dns.levonet.sk. alpn=dot port=853 \
    ipv4hint=109.236.119.2,109.236.120.2 ipv6hint=2a02:6ca3:0:1::2,2a02:6ca3:0:2::2
_dns.resolver.arpa. 900 IN SVCB 2 dns.levonet.sk. alpn=h2 port=443 \
    ipv4hint=109.236.119.2,109.236.120.2 ipv6hint=2a02:6ca3:0:1::2,2a02:6ca3:0:2::2 \
    key7="/dns-query{?dns}"

;; ADDITIONAL SECTION:
dns.levonet.sk.     900 IN A 109.236.119.2
dns.levonet.sk.     900 IN A 109.236.120.2
dns.levonet.sk.     900 IN AAAA 2a02:6ca3:0:1::2
dns.levonet.sk.     900 IN AAAA 2a02:6ca3:0:2::2
```

Objavenie servera

- nadviaže sa šifrované spojenie (DoH, DoT, DoQ) a overí sa validita certifikátu (musí obsahovať dopytovanú IP adresu ako subjectAltName)

= mechanizmus funguje iba ak koncové zariadenie dostane verejnú IP adresu DNS servera

Implementácia

Implementácia DDR - certifikát

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:8d:bf:03:e0:5d:28:43:a9:66:50:46:59:1b:ad:a6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
        Validity
            Not Before: Feb 21 00:00:00 2023 GMT
            Not After : Feb 21 23:59:59 2024 GMT
        Subject: C=SK, L=Levoča, O=LEVONET, s.r.o., CN=dns.levonet.sk
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:30:8d:ba:7f:bf:6c:04:3c:b2:93:5d:c5:22:51:
                    c2:a8:8a:c4:d3:9d:e7:30:96:f7:fe:be:72:21:51:
                    98:29:e6:a6:44:a5:d1:65:c4:07:2f:13:84:57:a5:
                    b6:03:77:6f:97:fb:74:a0:4f:d8:d9:2e:88:d8:50:
                    55:74:fc:f0:98
                ASN1 OID: prime256v1
                NIST CURVE: P-256
```

Implementácia DDR - certifikát

```
X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:90:58:FF:B0:9C:75:A8:51:54:77:B1:ED:F2:A3:43:16:38:9E:6C:C5

            X509v3 Subject Key Identifier:
                E7:A8:7E:8A:78:70:50:C0:51:F1:4F:3E:68:E6:90:A1:8E:FD:B8:87
            X509v3 Subject Alternative Name:
                DNS:dns.levonet.sk, IP Address:2A02:6CA3:0:2:0:0:0:2,
                IP Address:2A02:6CA3:0:1:0:0:0:2, IP Address:109.236.119.2,
                IP Address:109.236.120.2, DNS:ns1.levonet.sk, DNS:ns2.levonet.sk
 X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
```

Implementácia DDR – konfigurácia Knot Resolvera

```
local ffi = require('ffi')
local function DDR_SVCB(state, req)
    local answer = req:ensure_answer()
    if answer == nil then return nil end
    local qry = req:current()
    if qry.stype ~= kres.type.SVCB then
        return state
    end

    ffi.C.kr_pkt_make_auth_header(answer)
    answer:rcode(kres.rcode.NOERROR)
    answer:begin(kres.section.ANSWER)

    local records = kres.parse_rdata({
        'SVCB 1 dns.levonet.sk. alpn=dot port=853 ipv4hint=109.236.119.2,109.236.120.2 \
          ipv6hint=2a02:6ca3:0:1::2,2a02:6ca3:0:2::2',
        'SVCB 2 dns.levonet.sk. alpn=h2 port=443 ipv4hint=109.236.119.2,109.236.120.2 \
          ipv6hint=2a02:6ca3:0:1::2,2a02:6ca3:0:2::2 key7=/dns-query{?dns}',
    })


    for _, entry in ipairs(records) do
       answer:put(qry.sname, 900, answer:qclass(), kres.type.SVCB, entry)
    end
```

Implementácia DDR – konfigurácia Knot Resolvera

```
    answer:begin(kres.section.ADDITIONAL)
    answer:put(todname('dns.levonet.sk'), 900, answer:qclass(), kres.type.A, kres.str2ip('109.236.119.2'))
    answer:put(todname('dns.levonet.sk'), 900, answer:qclass(), kres.type.A, kres.str2ip('109.236.120.2'))
    answer:put(todname('dns.levonet.sk'), 900, answer:qclass(), kres.type.AAAA, \
      kres.str2ip('2a02:6ca3:0:1::2'))
    answer:put(todname('dns.levonet.sk'), 900, answer:qclass(), kres.type.AAAA, \
      kres.str2ip('2a02:6ca3:0:2::2'))
    return kres.DONE
end

policy.add(
    policy.domains(DDR_SVCB,
                   policy.todnames({'_dns.resolver.arpa‘})
    )
)
```

Implementácia DDR – tuning Knot Resolvera

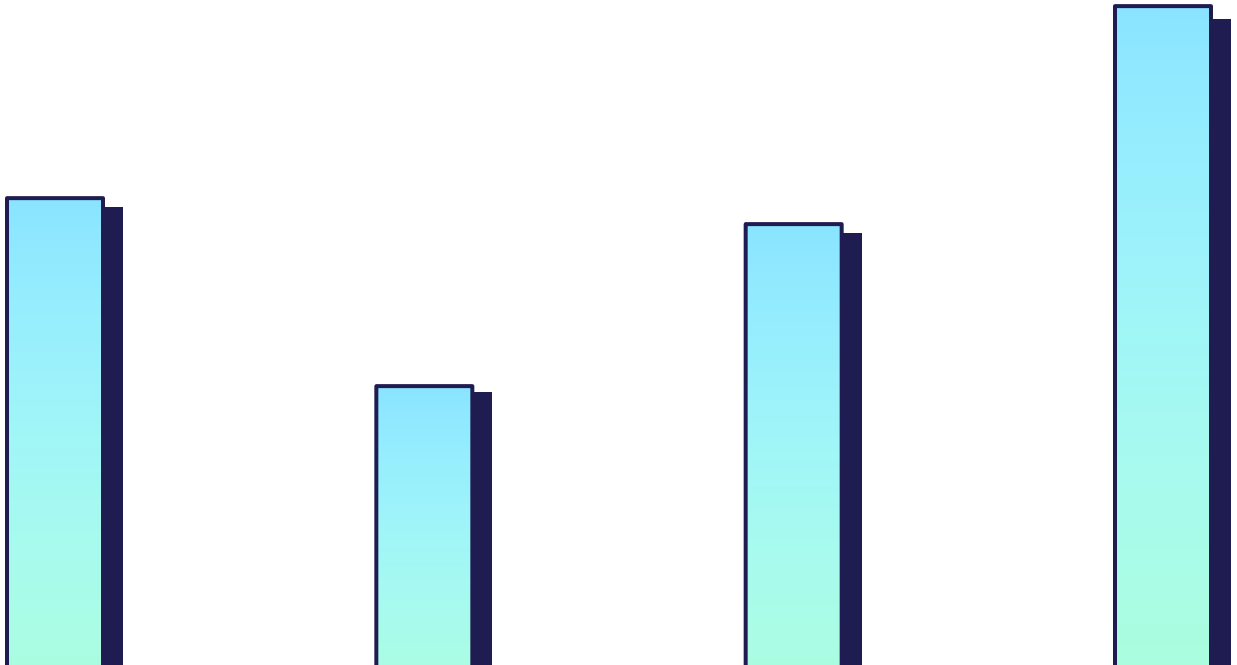
- Po akej dobe sa uzavrie DoH TCP spojenie?

time (echo -ne "GET /dns-query?dns=q80BAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB HTTP/1.1\r\nHost: cloudflare-dns.com\r\nAccept: application/dns-message\r\n\r\n") | openssl s_client -connect 1.1.1.1:443 –quiet

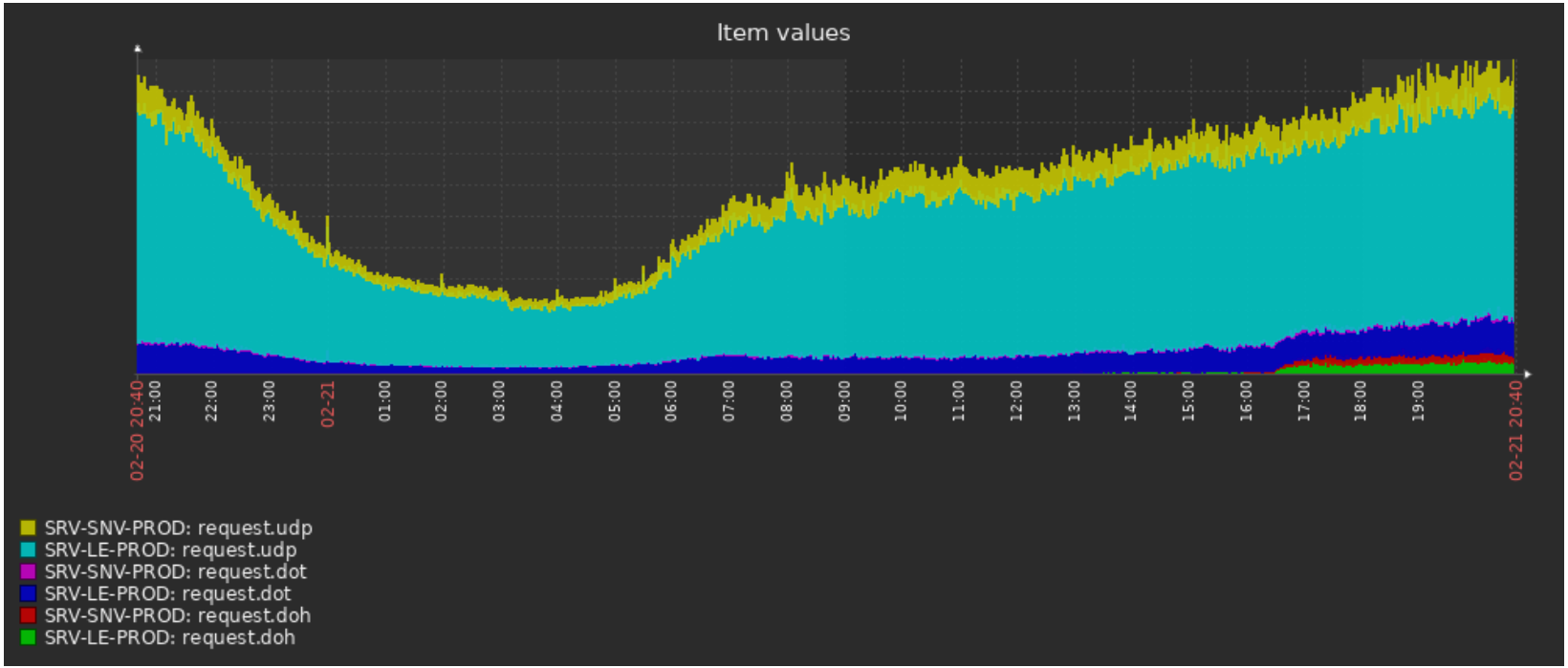
- Cloudflare DNS: 400s (15s pri prázdnom spojení)
- Google DNS: 240s
- Quad9 DNS: 10s
- AdGuard DNS: 120s
- **Knot Resolver: 10s**

tuning: net.tcp_in_idle(120000)

Štatistiky



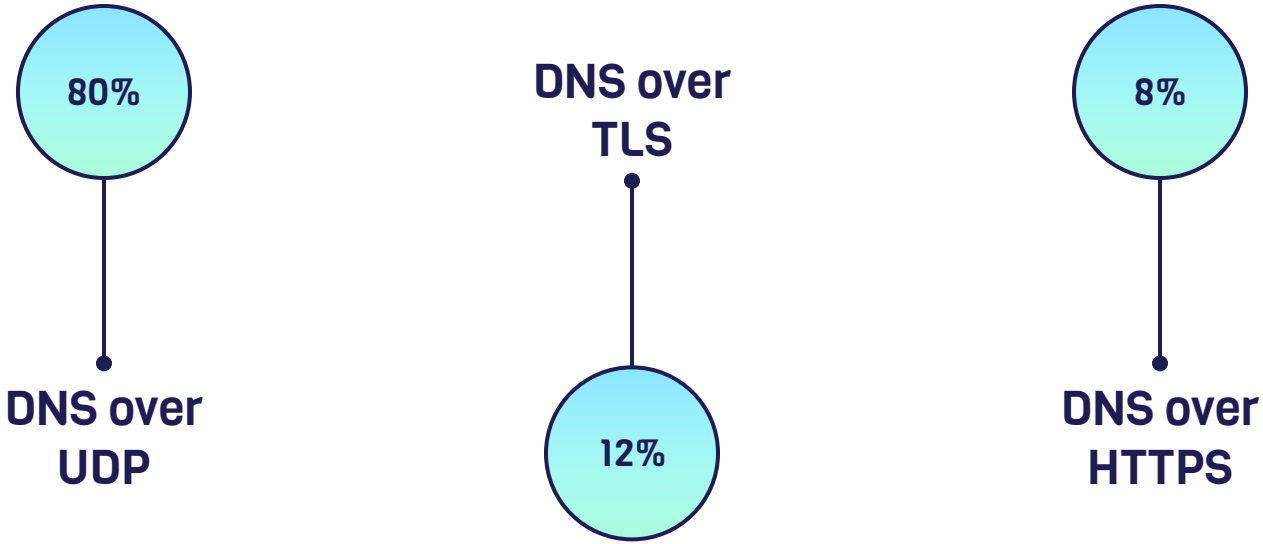
Štatistiky


Item values
02-20 20:40
21:00
22:00
23:00
02-21
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
02-21 20:40
SRV-SNV-PROD: request.udp
SRV-LE-PROD: request.udp
SRV-SNV-PROD: request.dot
SRV-LE-PROD: request.dot
SRV-SNV-PROD: request.doh
SRV-LE-PROD: request.doh

Štatistiky


Item values
05-16 01:50
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
05-17
01:00
05-17 01:50
SRV-SNV-PROD: request.udp
SRV-LE-PROD: request.udp
SRV-SNV-PROD: request.dot
SRV-LE-PROD: request.dot
SRV-SNV-PROD: request.doh
SRV-LE-PROD: request.doh

Štatistiky



20%

šifrovaných DNS požiadaviek

20%

šifrovaných DNS požiadaviek

*môže byť o 13% viac

60%

109.236.119.2

109.236.120.2

40%

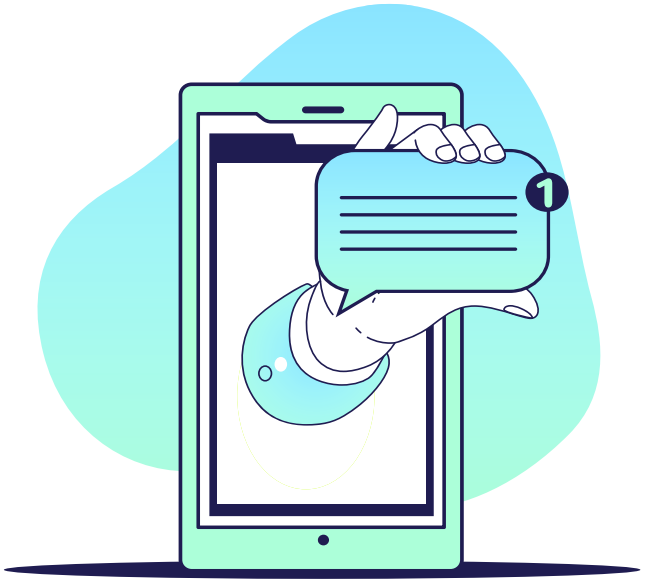
10.202.254.1

8.8.8.8

Otázky?

Email: blazej@ekrajnak.com

Twitter: @BlazejKrajnak



Blažej Krajňák | Levonet, s.r.o.
CSNOG 17.5.2023