# IPv6 Bingo

## „IPv6 je bezpečnější než IPv4“ a další časté mýty a omyly o IPv6

Radek Zajíc, radek@zajic.v.pytli.cz • KKDS 2023 Plzeň, 21. 9. 2023

# about::myself

Radek Zajíc





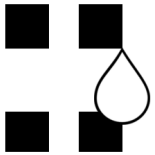
**Blog:** showmax.engineering
**Twitter:** @ShowmaxDevs

# IPv6 101 pro ISP

**IPv4 a IPv6 žijí vedle sebe**

**IPv4:**
32 bitů, 192.0.2.1, masky /0 až /32, typická koncová síť /24, NAT
**IPv6:**
128 bitů, 2001:db8:dead:ba00:20c:29ff:feb6:d023, masky /0 až /128, koncová síť /64
2001:db8:… – 32 bitů příděl od RIPE NCC (obvykle dnes /29, dříve /32 nebo /35)
…:dead:ba… – 24 bitů, které spravujete vy jako ISP (v případě přídělu /56 = 32+24)
…00:… – 8 bitů, které spravuje zákazníkův router (v případě přídělu /56)
…:79ae:7a48:143b:ce10 – 64 bitů, které si „vymyslelo“ zařízení u zákazníka doma

typický příděl pro domácnost /56, tj. 256 koncových sítí /64 (64 bitů pro zařízení v síti)
typický příděl pro firmu /48, tj. 65536 koncových sítí /64
žádný NAT = všechny adresy jsou globálně routovatelné
Prefix Delegation: mechanismus pro ISP, jak zákazníkovi přidělit blok adres a automaticky ho naroutovat

| | | | | |
|---|---|---|---|---|
| NAT444 nám stačí | Tohle zařízení IPv6 podporuje | Prostor IPv6 adres je tak velký, že nejde proskenovat | IPv6 nikdo nenasazuje | IPv6 je bezpečnostní riziko |
| Privacy Extensions: pořád se mi mění adresa | IPv4 je lepší, protože má NAT; NAT nás chrání | Díky IPv6 mě mohou weby/policie snáz sledovat | Koncoví uživatelé IPv6 neřeší | IPv6 prozrazuje mou MAC adresu, a to nechci |
| Tolik adres přece nepotřebujeme | Naši zákazníci IPv6 nechtějí |  | IPv6 je jen IPv4 s více adresami. 96 nových bitů – a víc nic | Nasazení IPv6 je příliš rizikové |
| IPv6 neprovozuji, proto mě nezajímá | Hackeři IPv6 neřeší, na IPv6 nikdo neútočí | IPv6 v produktech našich dodavatelů nefunguje dobře | DNS64 rozbije DNSSEC | IPv6 je díky vestavěnému zabezpečení bezpečnější než IPv4 |
| IPv6 nám rozbije GeoIP | IPv6 je rozbitý protokol a moc nefunguje | IPv6 je nedopečený protokol | Kvůli IPv6 musíme přepsat *všechny* naše aplikace | Nemáme laboratoř, kde IPv6 testovat |

# NAT444 nám stačí

I'm not a robot

reCAPTCHA
Privacy - Terms

**About this page**

Our systems have detected unusual traffic from you
network. This page checks to see if it's really you s
requests, and not a robot. Why did this happen?

IP address: 420.420.420.69
Time: 2022-07-05T95:97:36Z
URL: https://www.google.com/search?
q=...&aqs=chrome..69i57.6131j0j1&sourceid=chrome&ie=UTF-8


Daryll Swer: Shortcomings of CGNAT and Potential Workarounds

# IPv4 je lepší, protože má NAT; NAT nás chrání

NAT není firewall
NAT lze prorazit
Firewally existují v IPv4 i IPv6
Chcete-li se chránit, nakonfigurujte firewall pro oba protokoly
(a to i pokud IPv6 aktivně nepoužíváte)

Johannes Weber: Why NAT has nothing to do with Security!

# IPv6 neprovozuji, proto mě nezajímá

```
# ping6 ff02::1%eth1
(...)
64 bytes from fe80::9209:d0ff:fe0b:ad46%eth1: icmp_seq=1 ttl=64 time=0.387 ms
64 bytes from fe80::20c:29ff:feb6:d023%eth1: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from fe80::9ade:d0ff:fe02:284b%eth1: icmp_seq=1 ttl=64 time=0.427 ms
64 bytes from fe80::20c:29ff:feb0:4f2d%eth1: icmp_seq=1 ttl=64 time=0.439 ms
(...)

# nmap -6 fe80::20c:29ff:feb6:d023%eth1
Nmap scan report for fe80::20c:29ff:feb6:d023
Host is up (0.00097s latency).
Not shown: 985 closed tcp ports (reset)
PORT     STATE SERVICE
(...)
53/tcp   open  domain
(...)
111/tcp  open  rpcbind
(...)

# dig +short isp-konference.cz @fe80::20c:29ff:feb6:d023%eth1
77.93.223.89
```

Chris Grundemann: I'm Not Running IPv6 so I Don't Have to Worry

# IPv6 neprovozuji, proto mě nezajímá

Příklad ze života

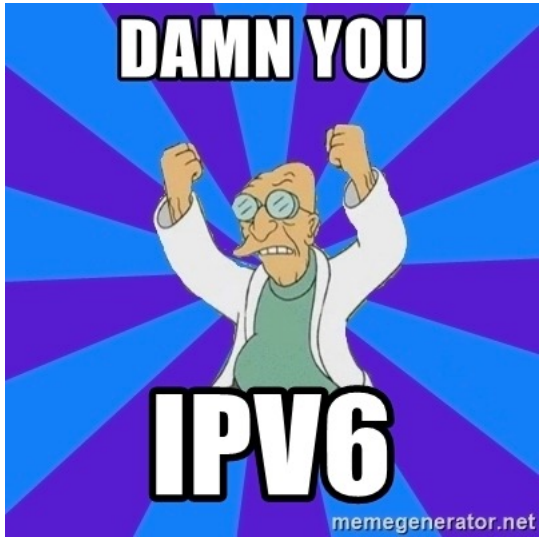
1. V síti nemáte IPv6 first hop security (RA Guard, DHCPv6 Guard/Snooping, …)
2. Připojí se uživatel, který má IPv6 konektivitu odjinud
3. Uživatel začne do vaší sítě vytrubovat „routuji IPv6!“
4. Routery vašich klientů mají IPv6 zapnuté a proto získají IPv6 adresy od uživatele s cizí konektivitou
5. V nejhorším případě uživatel s cizí konektivitou bude záškodník, který routerům vašich klientů přidělí i IPv6 prefixy pro LAN
6. Uživatelská zařízení v LAN IPv6 preferují a provoz po IPv6 poženou skrze router uživatele s cizí konektivitou
7. **$$$PROFIT?$$$**

# IPv6 je jen IPv4 s více adresami. 96 nových bitů – a víc nic

1. Nový formát adresy: hexadecimální zápis, nulové bloky lze vynechávat
2. Nové protokoly: ICMPv6 (RA/SLAAC), DHCPv6
3. Jiné konfigurace firewallu (kvůli ICMPv6, DHCPv6, atp.)
4. Nové vektory útoku: stržení provozu v sítích, které se nechrání
5. Nový způsob konfigurace domácích zařízení (Prefix Delegation, přiřazování bitů sítím v LAN)
6. Chybějící NAT
7. Vícero IPv6 adres na každém rozhraní (link-local, globální stabilní, globální dočasné, ULA, …)

# IPv6 je bezpečnostní riziko

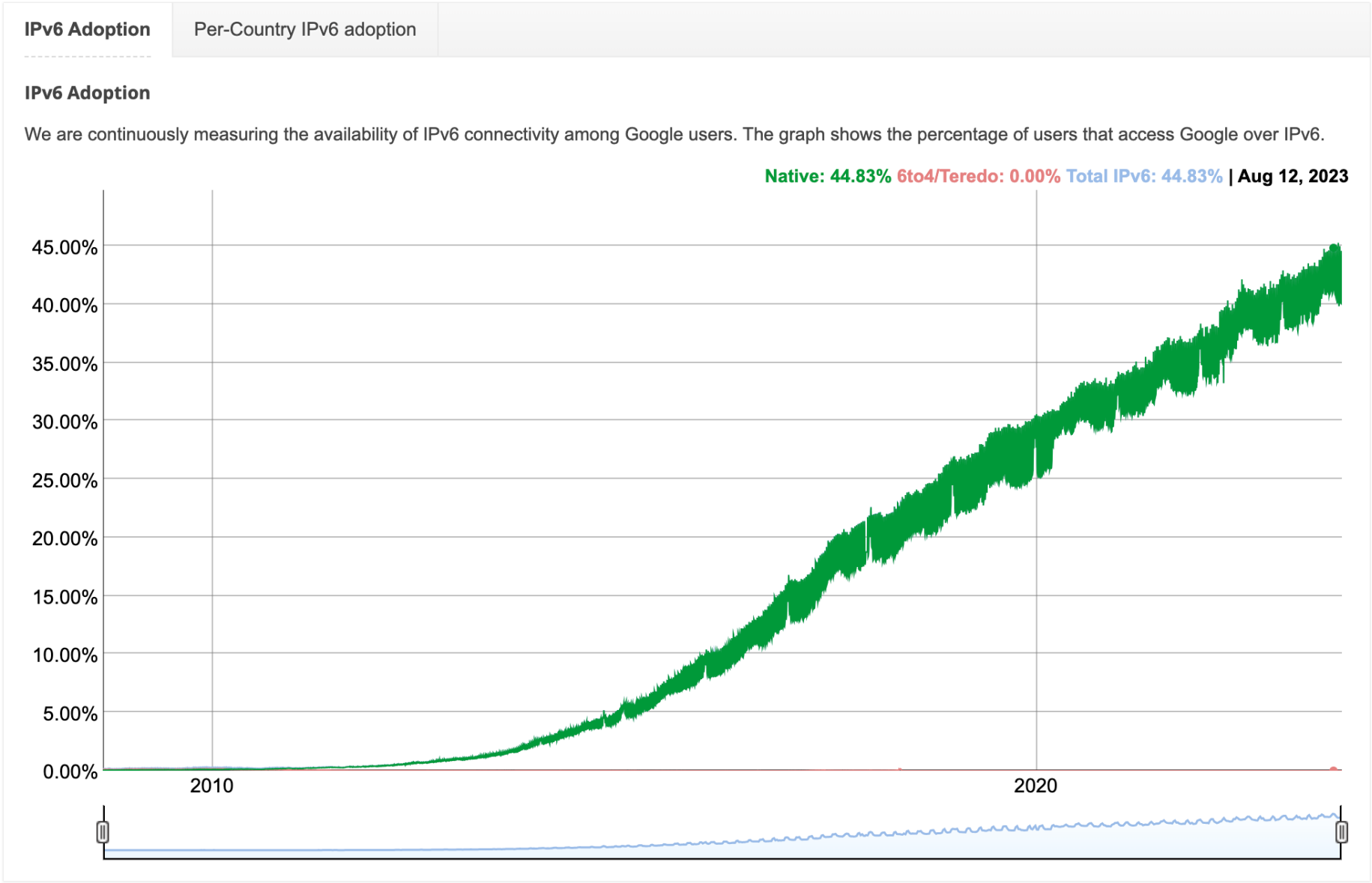
Pokud se IPv6 nebudete věnovat a necháte ve svých sítích otevřená dvířka, není bezpečnostním rizikem protokol, ale vy



# IPv6 je nedopečený protokol

IPv6 je internetový standard (RFC8200) od roku 2017

# IPv6 nikdo nenasazuje



# IPv6 je díky vestavěnému zabezpečení bezpečnější než IPv4

Jde o mýtus kvůli (původně) povinnému IPSec, který ale sám o sobě bezpečnost ničeho nezlepšuje.

Tolik adres přece nepotřebujeme

*$2^{128}$ je obrovské číslo, jenže…*

…29 bitů přiděluje regionální registrátor

…64 bitů používá autokonfigurace v lokálních sítích

…8, 12 nebo 16 bitů by měl mít možnost využít uživatel pro své domácí sítě

…pro ISP zbývá < 27 bitů, které snadno vyčerpá hierarchickým přidělováním síťových prefixů (pro obec, okres, kraj, …)

# IPv6 prozrazuje mou MAC adresu, a to nechci

**Globální adresy na moderních OS dávno neobsahují MAC adresu, 64 „host“ bitů se generuje náhodně**

2001:db8:dead:ba00:79ae:7a48:143b:ce10

(navíc jste stejně za stavovým firewallem, není-liž pravda?)

Link-local adresy mohou stále obsahovat MAC (např. na Linuxu)

# Privacy Extensions: pořád se mi mění adresa

**Díky RFC7217 mají zařízení stabilních 64 „host“ bitů uvnitř sítě (pro každou síť jde o jiných 64 bitů)**

**Díky RFC4941 mají zařízení i další adresy, dočasné, kterým se skutečně průběžně mění 64 „host“ bitů**

Pokud chcete např. otevřít firewall pro nějakou adresu, použijte „stabilní“ adresy

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 14:1d:da:cf:fc:3f
        inet6 fe80::18ae:4593:1fe0:183e/64 secured scopeid 0x6
        inet6 2001:db8:dead:beef:107c:45f4:e7a7:b32a/64 autoconf secured
        inet6 2001:db8:dead:beef:79ae:7a41:143b:ce10/64 autoconf temporary
```

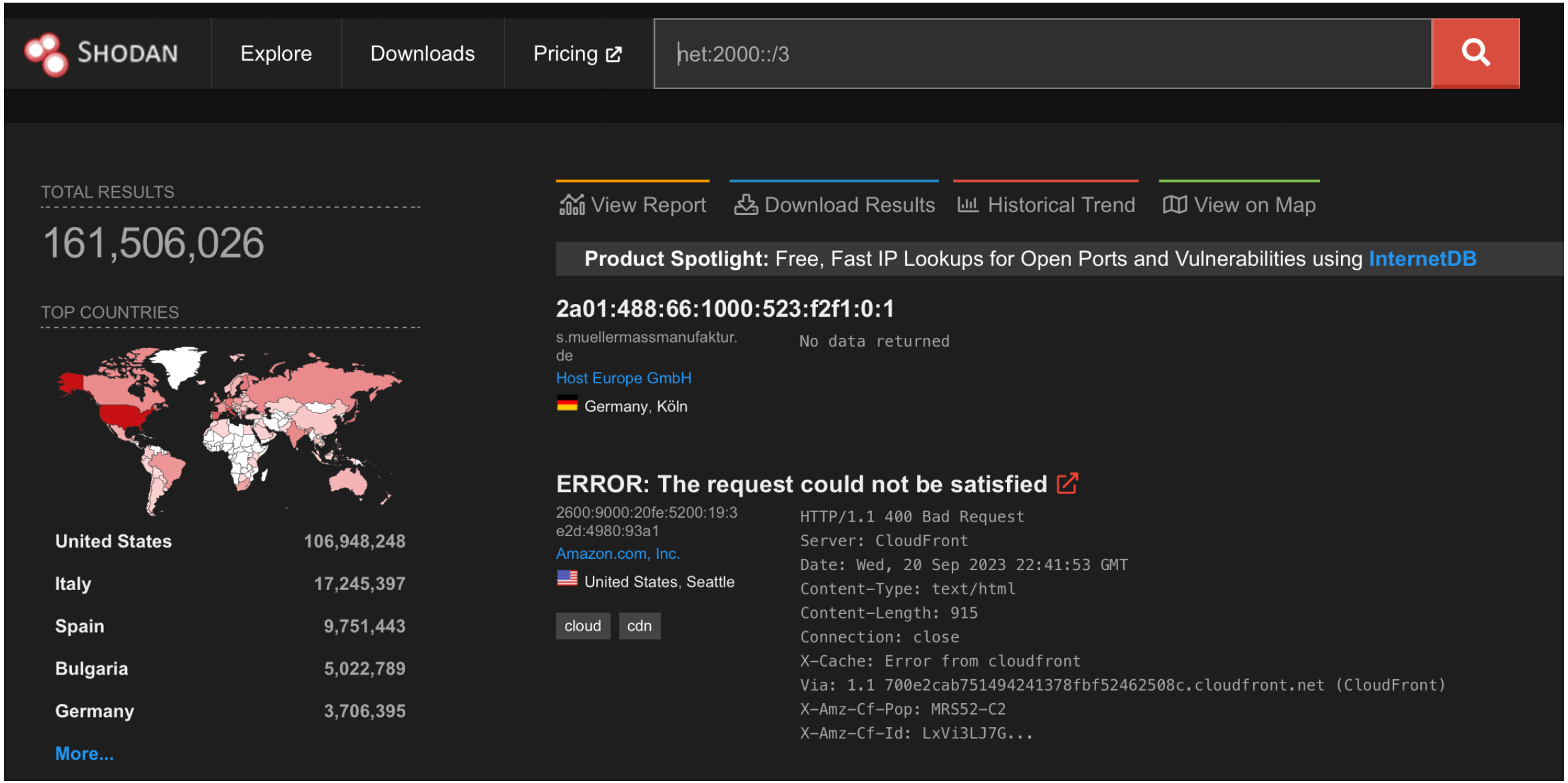
Díky IPv6 mě mohou weby/policie snáz sledovat

**Každý** v Internetu uvidí vaši globální IPv6 adresu…
2001:db8:dead:ba00:79ae:7a48:143b:ce10

…stejně jako **každý** v Internetu vidí vaši veřejnou IPv4 adresu!
192.0.198.146

Prvních 64 bitů identifikuje síť = analogie k IPv4 veřejné
Zbylých 64 bitů se dnes generuje náhodně

# Hackeři IPv6 neřeší, na IPv6 nikdo neútočí



# Prostor IPv6 adres je tak velký, že nejde proskenovat

- DNS AAAA záznamy
- Záznamy o vydaných certifikátech (Certificate transparency streams)
- IPv6 hitlist
- ping6 ff02::1%interface
- Enumerace (2001:db8::1, 2001:db8::2, …, 2001:db8::ffff, …)
- IPv6 traceroute (efektivní metoda pro detekci sítí využívajících prefix Delegation)
- …

- Hello IPv6 Scanning World!
- Using IPv6 with Linux? You've likely been visited by Shodan and other scanners
- New Ways of IPV6 Scanning
- IPv6 Scanning
- Akamai: Who's Scanning the IPv6 Space? And, Frankly, Why Do We Even Care?
- Scanning the IPv6 Internet: Towards a Comprehensive Hitlist

# IPv6 nám rozbije GeoIP

Všechny moderní GeoIP databáze IPv6 podporují a obsahují aktuální data (byť ne možná na úroveň města – ta je ale pochybná i u IPv4)

# „Koncoví uživatelé IPv6 neřeší“, „Naši zákazníci IPv6 nechtějí"

Koncoví uživatelé nechtějí ani IPv4. Chtějí „jen“ používat Internet – a pokud nemáte IPv6 (správně) nasazenou, zatímco konkurence ano, půjdou tam, kde jim bude fungovat vše. Včetně IPv6-only služeb.

# IPv6 je rozbitý protokol a moc nefunguje

To platilo zejména před rokem 2012, kdy se masivně používaly IPv6 tunely. Dnes s nativní IPv6 konektivitou už k rozbitosti dochází jen velmi výjimečně.

Platit to může i dnes, pokud máte špatnou implementaci IPv6 a konektivita/služba není funkční. Jde ale o problém správce, nikoli samotného protokolu. (Zdravíme státní správu.)

# Tohle zařízení IPv6 podporuje

Častý předpoklad každého, kdo s IPv6 začne pracovat. Platí ale známé pořekadlo: důvěřuj, ale prověřuj.

Existuje mnoho dodavatelů a produktů, které neumí IPv6 vůbec, neumí pracovat v sítích bez IPv4, nebo mají podporu IPv6 pouze částečnou nebo rozbitou.

# Kvůli IPv6 musíme přepsat *všechny* naše aplikace

Pokud používáte open-source, podpora už je často přítomná a na dobré úrovni. U komerčního softwaru záleží na kvalitě vývojového týmu – opět je potřeba důkladně prověřovat.

# IPv6 v produktech našich dodavatelů nefunguje dobře

Hlasujte peněženkou.

# Nemáme laboratoř, kde IPv6 testovat

Ať chceme nebo ne, svět se vydal cestou IPv6.

I na nepřítele je ale lepší se včas připravit.

Máte nejvyšší čas začít ji stavět!

# DNS64 rozbije DNSSEC

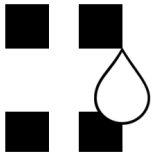
NAT64 a DNS64 jsou oblíbené mechanismy, jak ze sítí, ve kterých už je jen IPv6 (a žádná IPv4), zpřístupnit IPv4 internet.

DNS64 a DNSSEC je problém jen pro „validující stub resolvery“, tedy DNS servery kontaktující rekurzivní DNS servery vás (ISP). Takové se prakticky nevyskytují.

V laboratoři (už ji stavíte?) si například můžete bez problémů spustit rekurzivní DNS server Unbound s podporou DNSSEC i DNS64 zároveň.

# Je IPv6 (ne)bezpečnější než IPv4?

# Záleží na vás, ne na protokolu!

| | | | | |
|---|---|---|---|---|
| NAT4… …m stačí | Tohle … …ní IPv6 p… …ie | Prosto… …Pv6 …ures je tak vel… …e nejde p… …ken… …t | IPv… …ado ne… …e | IPv6 je … …pečnostní … |
| Privac… …nsions: pořád… …i mění …adres… | IPv4 je … …rotože má NA… …AT nás …hrán… | Díky IP… …nohou weby/… …e snáz …edova… | Koncov… …atelé IP… …ie… | IPv6 p… …uje mou MAC … …su, a to … …nech… |
| Tolik … …přece nep… …ieme | Naši za… …ci IPv6 n… …í |  | IPv… …ien I… …s více ad… …n. 96 nových … …a víc nic | Nasa… …IPv6 je p… …kové |
| IPv6 … …vozuji, proto… …zajímá | Hacke… …IPv… …ešeší, na I… …nikdo …eúto… | IPv6 … …ro… …ktech našich … …avatelů nef… …guje … …bře | DNSo… …bije D… …s | …v6 je … …ky ve… …ému …ení bez… …ečnější … …ž IPv4 |
| IPv6 … …rozbije … …P | IP… …e n… …ný proto… …a moc … …ung… …e | IPv6 je … …pečený n… …l | Kvůli … …6 n… …sme přepsa… …echny na… …apli… …e | Nema… …aboratoř, kde… …stovat |

# Q & A

# Díky

linkedin.com/in/radek-zajic/

@zajDee