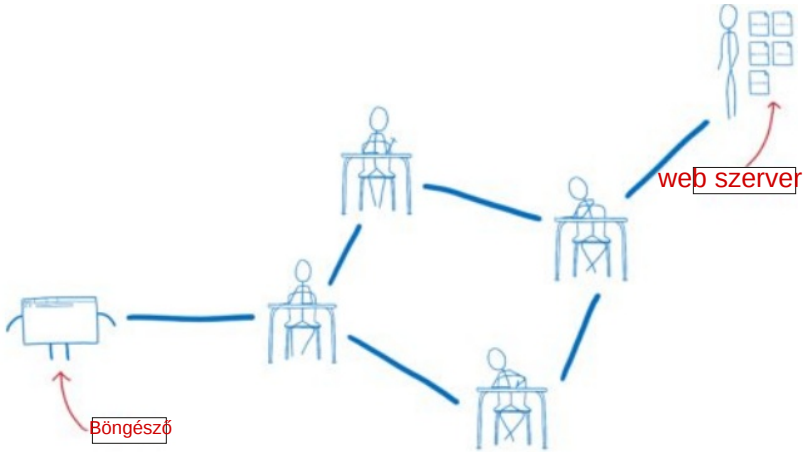
Cartoon Intro To DNS Over HTTPS - összefoglaló

PCLinuxOS Magazine – 2019. december

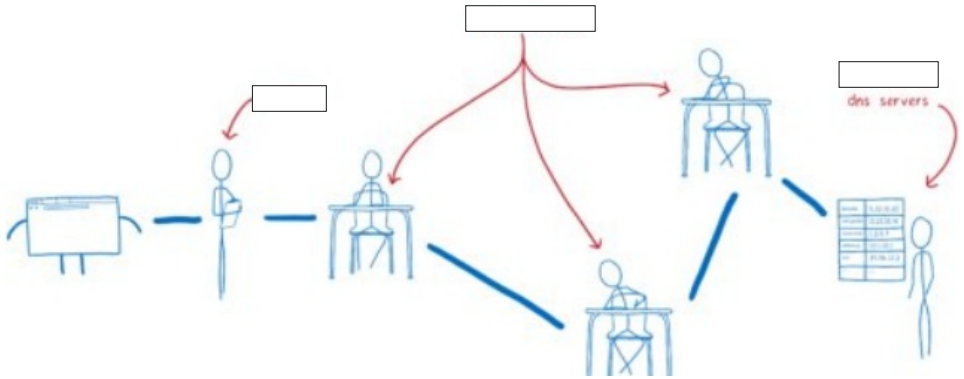
A cikk valójában Lin Clark Mozilla Hacks oldalán 2018 augusztusában megjelent írásának újranyomtatása.

A Mozilla a felhasználók adatainak védelme érdekében két új eljárást vezetett be, aminek a tesztelését várja a felhasználóktól.

Az új eszközök célja a DNS és a HTTP rendszer hiányosságainak kiküszöbölése, megakadályozandó egyrészt a **nyomkövetést (tracking)** és a **https-kérés eltérítését (spoofing)**. A problémát az okozza, hogy a két végpont nem közvetlenül, hanem szerverelken keresztül kommunikál:

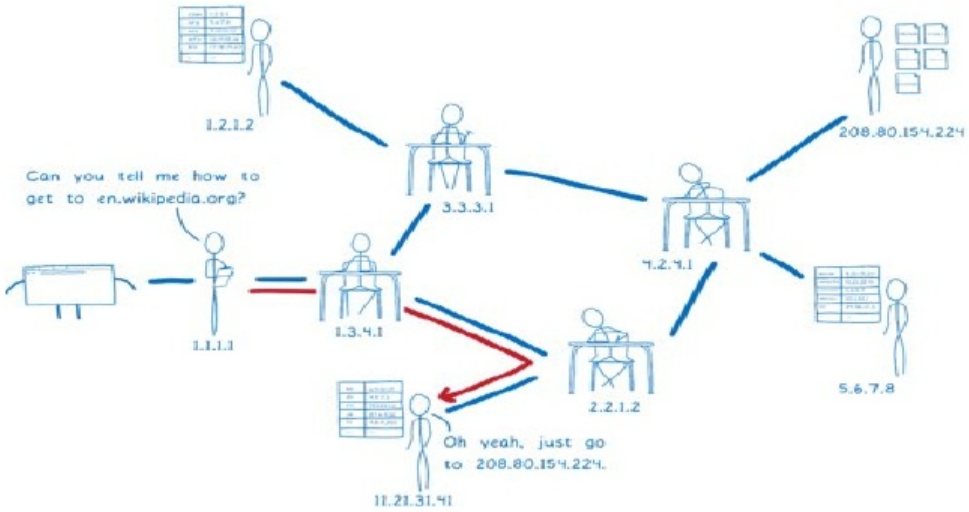


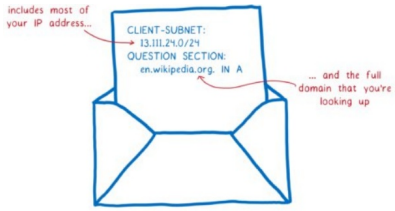
Lehetséges veszélyforrások:



A bevezetett eszközök a **TRR** (Trusted Recursive Solver) és a **DoH** (DNS over HTTPS). Ebből a TRR – biztonságos (DNS) rekurzív feloldó – célja kizárni az olyan szervereket, amik egyrészt követhetik a DNS-kéréseinket, másrészt meghamisíthatják, eltéríthetik azt. A DoH (DNS a HTTPS fölött) célja megakadályozni a forgalom figyelését, lehallgatását. Mindkettő célja, hogy a felhasználó lehető legtöbb adatának elrejtésével, nehezítse az anonimitása feltörését.

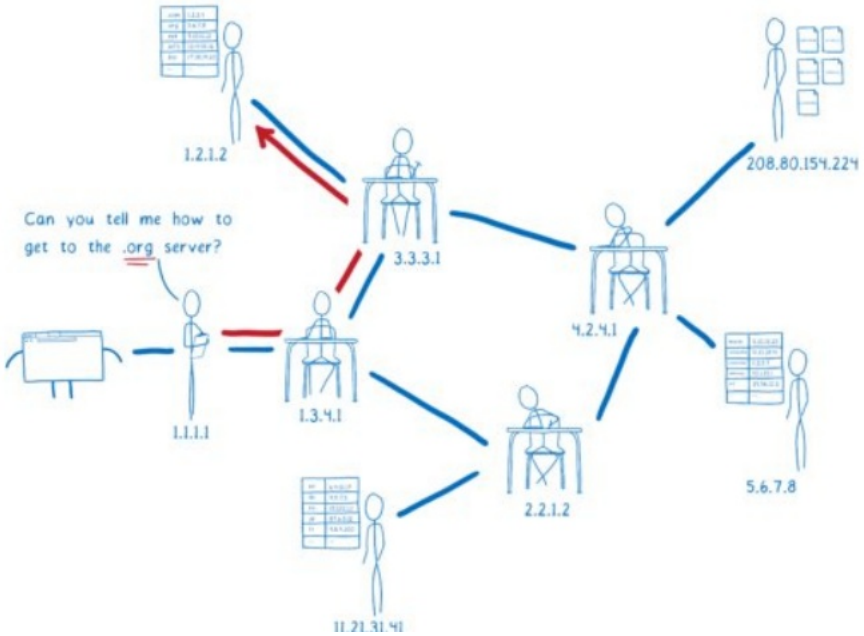
A **TRR** a felhasználói kérések feloldására a **Cloudfire** szervereit használja, amely cég a beazonosításra alkalmas kereséseket 24 óra leteltével automatikusan törli és soha nem ad át ilyen adatokat harmadik félnek. A választás azért esett a Cloudfire-re, mert elkötelezett a személyes adatok védelme mellett és szorosan együttműködött a Firefox-csapattal a DoH kidolgozásában is.





A közbeiktatott szerverekkel történő lehallgatás és hamisítást a HTTPS már jelentősen megnehezítette, mivel a forgalom titkosítva megy át azokon. Mindazonáltal, a DNS-kérés csomagok rejtjelezés nélkül mennek, ami elméletileg tartalmazza a küldő DNS-ének első

24 bitjét. Ez felhasználható a földrajzi hely közelítő megállapítására. A Cloudfire a felhasználói adatok helyett, egy hozzá közeli saját IP-címet ad meg.



Mi az amit a két új eszköz nem old meg?

A név feloldása után az IP címre küldeni kell egy indító kérést, ami nincs titkosítva és a szolgáltatód, illetve a kérést továbbító routerek látják az adatokat. Innentől kezdve minden titkosítottan megy. A jó oldala a dolognak, hogy ettől kezdve az adott szerverhez kapcsolódó valamennyi oldallal a forgalmazás titkosított.

Tehát az internetszolgáltatód és a közbenső szerverek már nem látják az adott szerverrel folytatott kommunikáció tartalmát.

A CDN (Content Delivery Network) rendszer kiterjedésével egyre több adat marad rejtve az illetéktelen figyelő szemek elől. A CDN – tartalom továbbító hálózat – az, amikor földrajzilag elkülönített szerverekhez kapcsolódnak a különféle független oldalak. Ezekhez kapcsolódhatsz, egyszerre többhöz is.

A fejlesztők kérik, hogy minél többen telepítsék az eszközöket és tesztelési célból osszák meg velük a tapasztalatokat.