Ohtlik WiFi hotellides: DNS-mürgitamisega näpatakse sisselogimise andmeid

1 tund tagasi - 25.07.2026 Autor: AM

Hotelli saabudes teed sa tavaliselt seda, mida kõik külastajad: logid end sisse avalikku WiFi-võrku, et kiirelt e-kirjadele pilk peale visata või pilveteenusesse siseneda. See pealtnäha kahjutu liigutus võib osutuda veaks.

ReliaQuesti värske ohuraporti kohaselt on küberkurjategijad võtnud sihikule just hotellide, konverentsikeskuste ja muude jagatud ruumide WiFi-väravad. Kui ründaja on saanud kontrolli kohaliku ruuteri üle, suunab ta sinu seadme salamisi kurjategijate serveritesse ja varastab su Microsoft 365 kontode andmed – ja seda kõike ilma, et peaksid avama ainsatki õngitsuskirja või laadima alla mõne kahtlase faili.

Kuidas rünnak toimub?

DNS-süsteem (*Domain Name System*) on kui interneti telefoniraamat. Kui tahad helistadakuhugi, otsid sa nime ja leiad numbri. Kui sa trükid brauserisse veebiaadressi, küsib sinu arvuti kohalikult ruuterilt, milline on selle veebilehe numbriline IP-aadress või kust tabelist seda leida.

DNS-mürgitamine (*DNS Poisoning*) on aga olukord, kus küberkurjategija on salaja sisse murdnud ja asendanud hotelli interneti "telefoniraamatus" õiged numbrid enda omadega. Kui su arvuti küsib teed Microsofti sisselogimislehele, suunab mürgitatud andmebaas sind hoopis kurjategijate loodud, identsena näivale koopia-lehele. Sa sisestad pahaaimamatult oma parooli ning kurjamid saavad selle endale.

Peidetud lisaoht: WPAD ja *proxy*

Raport toob välja veel ühe kavala nipi, mida ründajad mõnel juhul kasutavad – WPAD (*Web Proxy Auto-Discovery*) kuritarvitamise. Kujuta seda ette olukorrana, kus hotelli WiFi mitte ainult ei anna sulle valet telefoniraamatut, vaid surub sulle peale ka isikliku "tõlgi", kes on tegelikult vaenlase spioon.

Kuna Windows kontrollib võrku ühendudes tihti automaatselt vahendaja ehk *proxy* seadeid, pakub ründaja kontrollitud WiFi välja oma seadistuse. Kui see

kavalus õnnestub, suunatakse väga suur osa sinu arvuti rakenduste liiklusest (sealhulgas Chrome'i brauseri päringud ja autentimised) otse läbi ründaja serveri. Seda on seadme kasutajal äärmiselt raske märgata, sest liiklus tundub väliselt tavalise ja krüpteerituna.

Kes on rünnaku taga?

ReliaQuesti eksperdid hindavad, et see tegevusmuster sarnaneb kurikuulsa rühmituse käekirjaga, keda tuntakse nimede all APT28, Fancy Bear või Forest Blizzard. Tegemist on Venemaa sõjaväeluurega seostatud rühmitusega, mis on varemgi sarnaseid ruuteritele suunatud laiaulatuslikke andmevarguse kampaaniaid läbi viinud.

Seekordne operatsioon paistab silma oma geograafilise ulatuse poolest. Kompromiteeritud WiFi-väravaid on tuvastatud nii USA-s, Indias kui ka Saudi Araabias alates 2026. aasta juunist. Ohvriteks on langenud finants-, õigus-, tervishoiu-, energia- ja jaemüügisektorite töötajad.

Kurjategijaid ei huvita otseselt tööandja tegevusala – nad sihivad professionaale ja rändavaid töötajaid, diginomaade, kes kipuvad end avalikesse võrkudesse ühendama.

> „Seadmed, millel on kõvakodeeritud lahendajad, nagu 8.8.8.8, ei ole oma olemuselt kaitstud: päring lahkub seadmest endiselt krüpteerimata liikluse kujul, mida pahatahtlik värav saab lugeda, võltsida ja ümber suunata.“
>
> (Tsitaat ReliaQuesti raportist)

Kuidas end ja oma ettevõtet kaitsta?

Õnneks on olemas mõned tehnoloogilised nipid selle nähtamatu ohu peatamiseks:

- **Alati sisselülitatud VPN** (täistunneliga ehk *full-tunnel*): see on reisil olles kõige olulisem kaitsekilp. Kui VPN on sisse lülitatud, ehitab see sinu seadme ja ettevõtte võrgu vahele turvalise suletud kanali. Kogu seadme liiklus, sealhulgas DNS-päringud, liiguvad kõigepealt läbi selle "toru" otse ettevõtte serverisse, jättes hotelli mürgitatud ruuteri pika ninaga.
- **Keela WPAD**: kui organisatsioon ei vaja automaatset *proxy*-seadistust, on tungivalt soovitatav see Windowsi seadmetes *Group Policy* kaudu täielikult välja lülitada, et likvideerida veel üks ründevektor.

- **Krüpteeritud DNS-i rangem režiim** (*Strict Mode*): tavaline veebibrauserites kasutatav krüpteeritud DNS (nagu DoH või DoT) kipub ühendusprobleemi korral sageli tagasi lülituma tavalisele, krüpteerimata lahendusele. See *fallback* teebki ründe võimalikuks. Kindlaim lahendus on *strict mode*, mis ei luba DNS-päringuid turvamata kujul teele saata.

Kuidas DNS Strict Mode sisse lülitada?

Google Chrome brauseris	• Ava brauseri seaded (kolm täppi paremal üleval -> **Seaded** või *Settings*). • Vali vasakpoolsest menüüst **Privaatsus ja turvalisus** (*Privacy and security*). • Klõpsa valikul **Turvalisus** (*Security*). • Keri alla jaotiseni **"Turvalise DNS-i kasutamine"** (*Use secure DNS*). • Veendu, et lüliti on aktiivne, ning vali automaatse sätte ("Praeguse teenusepakkuja") asemel teine valik ehk **"Vali teenusepakkujaga"** (*With*). Vali rippmenüüst tuntud turvaline pakkuja, näiteks **Cloudflare (1.1.1.1)** või **Google (Public DNS)**. See sunnib brauserit kasutama alati krüpteeritud kanalit.
Mozilla Firefoxis	• Ava seaded (kolm kriipsu paremal üleval -> **Sätted** või *Settings*). • Vali vasakult **Privaatsus ja turvalisus** (*Privacy & Security*). • Keri lehe täiesti alla jaotiseni **"DNS üle HTTPS-i"** (*DNS over HTTPS*). • Vali seal **"Maksimaalne kaitse"** (*Max Protection*). See on Firefoxi vaste rangele režiimile, mis blokeerib ühenduse või hoiatab sind, kui turvalist DNS-i ei suudeta luua, välistades täielikult ohtliku tagasilangemise.

- Uudised

- Turvalisus
- Võrguseadmed

Pilt


HOTEL