Eesti-USA noorhäkkeri tabamine paljastas Windowsi nuhkimise

4 kuud tagasi - 11.07.2026 Autor: AM

19-aastase Eesti-USA topeltkodanikust küberkriminaali tabamine tõmbas eesriide Microsofti varjatud jälgimissüsteemilt. Just Windowsi telemeetria omadusega õnnestus kasutajat jälitada ja lõpuks aidata Soomes koos asitõenditega kinni võtta.

Helsingi lennujaamas aprillis Jaapani lennule suundumisel tabatud Peter Stokes polnud lihtsalt tavaline teismeline. USA justiitsministeeriumi ja FBI andmetel on tegemist kardetud küberkriminaalse sündikaadi Scattered Spider (tuntud ka kui Octo Tempest, UNC3944 ja Oktapus) liikmega. Rühmituse kombitsad on ulatunud sadadesse suurfirmadesse ning välja pressinud üle 100 miljoni dollari lunaraha.

Noormees on Eestis pikalt pangandus- ja *fintech*-sektoris (Estonian Air, Swedbank, Hansapank, TransferWise, Luminor) töötanud Wade Stokesi poeg.

Kuidas häkkida inimesi, mitte masinaid?

Kõige tõsisem süüdistus Stokesi vastu pärineb 2025. aasta maikuust, mil rühmitus võttis sihikule USA luksusjuveelide müüja. Kuidas nad sisse said? Nad ei kasutanud keerulisi koodijuppe ega murdnud toore jõuga läbi tulemüüride.

Selle asemel kasutasid nad sotsiaalset inseneeriat. Häkkerid ei püüa "ust" maha lõhkuda, vaid nad "helistavad" uksekella, kannavad virtuaalset postiljoni vormi ja paluvad sul endal uks avada.

Ründajad helistasid juveelifirma IT-toele Google Voice'i kaudu, esinedes firma enda töötajatena, ja veensid tugikeskust nende paroole lähtestama. Nii pääseti ligi kolmele kontole (millest kahel olid administraatori õigused), varastati kriitilisi andmeid ja nõuti 8 miljonit dollarit krüptovaluutas.

Kuigi ettevõte suutis oma süsteemid taastada ega maksnud lunaraha, läks see tööseisakute tõttu firmale maksma kaks miljonit dollarit.

GDID: digitaalne tätoveering, mida ei saa maha pesta

Kuidas aga jõudsid uurijad osava küberkurjategijani, kes varjas end virtuaalsete maskide taga? Siin astus mängu Microsoft. Uurijad järgisid "digitaalset puru", mille ründajad maha jätsid, ning avastasid, et Stokes kasutas Windowsi operatsioonisüsteemi. Microsoft ulatas FBI-le abikäe, pakkudes neile GDID (*Global Device Identifier*) andmeid, kirjutab Tom's Hardware.

Mis on GDID? Kujuta seda ette kui auto kerenumbrit, mis on keevitatud otse mootoriploki külge, aga selle vahega, et see number saadab pidevalt tootjale aruandeid selle kohta, kus sa sõidad ja millist muusikat raadiost kuulad. GDID on iga Windowsi installatsiooniga seotud unikaalne identifikaator, mis jälgib seadmespetsiifilist telemeetriat. Just seetõttu võib näiteks arvuti emaplaadi vahetamine tühistada sinu Windowsi litsentsi.

Uurimismaterjalidest selgub ehmatav tõsiasi: Microsoftil oli Stokesi kohta valmis sisuliselt täielik toimik juba enne, kui prokuratuur jõudis oma süüdistuse kokku panna. Tehnoloogiahiid edastas FBI-le ajatemplitega varustatud logid Stokesi veebitegevuse, videomängude ajaloo, IP-aadresside, kasutatud tööriistade (sealhulgas Ngroki) ja Azure'i staatuse kohta. Vaja oli vaid punktid omavahel ühendada.

Muidugi aitas tabamisele kaasa ka see, et teele asudes oli noormehel kaasas kaks kõvaketast täis inkrimineerivaid tõendeid ning tema isik oli uurijatele teada juba 2024. aastast, kuid toona AÜE ja Eesti vahet liikunud alaealist sai vaid distantsilt jälgida.

Kas turvalisus kaalub üles privaatsuse kao?

Kogu see saaga on pannud tehnoloogiakogukonna kihama. Tuntud tehnoloogiaportaal *Tom's Hardware* võtab tekkinud privaatsusmure kokku:

> "*Muidugi tõstatab see küsimusi, kui üksikasjalik ja potentsiaalselt sissetungiv võib Microsofti telemeetria olla. Sel juhul kasutati seda väidetava häkkeri vahistamiseks, kuid mis saab siis, kui kellelgi teisel, kellelgi pahatahtlikul, õnnestuks sellele andmehulgale ligi pääseda?*"

Tehnoloogiateadlikud tarbijad on Windowsi liigse telemeetria üle kurtnud juba pikka aega. Kogu nn *debloating* kultuur (süsteemi puhastamine ebavajalikust tausta-tarkvarast) on selle pretsedendi otsene kõrvalsaadus, kuid GDID on süsteemi sisse ehitatud nii sügavale, et seda ei saa lihtsalt ühe nupuvajutusega eemaldada ega keelata.

Stokes ootab nüüd Chicagos vahi all kohtuprotsessi, seistes silmitsi süüdistustega vandenõus, küberinfiltratsioonis ja pettuses. Tema juhtum on aga meile kõigile meeldetuletuseks.

GDID (Global Device Identifier)	
Põhifunktsioon:	Seadmepõhine telemeetria ja riistvara identifitseerimine
Integreeritud OS-i:	Windows 10, Windows 11
Kogutavate andmete tüüp:	IP-aadressid, veebitegevus, logid, rakenduste kasutus, riistvara ID
Eemaldatavus kasutaja poolt:	Ei ole eemaldatav ega lihtsalt keelatav
Andmete jagamine:	Microsofti siseselt, seaduse alusel ja nõudel ka õiguskaitseorganitele (nt FBI)

- Uudised

- Tarkvara
- Turvalisus

Pilt

