Venemaalt pärit ruuter saatis tuhandeid SMSe, tagajärjeks tuhandeeurone telefoniarve

1 aasta tagasi - 03.04.2025 Autor: AM

Läinud aasta lõpus pöördus Elisa poole klient, kelle teadmata oli tema telefoninumbriga saadetud üle 10 000 SMS-i välisriikidesse, mille tulemusel jõudis temani ligi 1000-eurone arve. Kahtlasi toiminguid teinud seadme ajalugu uurides selgus, et see on Venemaal toodetud internetiruuter.

Juhtum leidis aset möödunud aasta lõpus, kui klient paigaldas oma SIM-kaardi Venemaal toodetud internetiruuterisse. Kuigi internetiruuter võib esmapilgul tunduda seade, millel justkui SMS saatmise võimekus puudub, võib pahavaraga nakatumisel sõnumite saatmine olla siiski rakendatav. Kõigest loetud päevadega oligi tõenäoliselt pahavaraga nakatunud seade saatnud 10 000 sõnumit välisriiki, mis tõi endaga kaasa suure arve.

Nakatunud ruuter

Elisa digiturvalisuse teenustejuht Ivar Tennokese sõnul on pahavaraga nakatunud seadmed kasvav probleem.

"Klient ise ei olnud sellises mahus teenuseid kasutanud ega teadnud toimuvast enne, kui arve saabus," selgitas Tennokese. "Kahjuks on pahavaraga nakatunud seadmed kasvav probleem. Kui selline seade on ostetud välismaalt või tundmatu edasimüüja juurest, on hiljem väga raske selgeks teha, kas seade on olnud näiteks juba enne soetamist pahavaraga nakatunud või on see toimunud kasutamise vältel."

Lisaks rõhutas Tennokese, et paljud ei tea seda aga ka ruuterite puhul on SMS-sõnumite saatmine võimalik ning pahavara võib seda funktsiooni kuritarvitada: "Ruuteri seadete alt on võimalik SMS-ide saatmise funktsioon eraldi välja lülitada, mistõttu soovitame seda alati kontrollida."

Kuidas selliseid juhtumeid vältida?

Elisa soovitab klientidel seadmeid osta vaid volitatud edasimüüjatelt ning vältida tundmatu päritoluga ruutereid ja teisi internetiseadmeid, mille konfiguratsioon võib olla ebaturvaline või mis võivad sisaldada pahavara. Lisaks tuleb oma

seadmete operatsioonisüsteeme hoida ajakohasena ja ise rakenduste alla laadimisel on väga oluline teha seda usaldusväärsest keskkonnast ja kontrollida, mis õigused rakendusele antakse.

"Tagantjärgi on keeruline kontrollida, kas kahtlane äpp oli juba varem seadmesse paigaldatud, oli seadmel mõni turvanõrkus, mida võrku ühendamise järgselt hakati ära kasutama või sai kliendi enda poolt mõni viirust sisaldav rakendus alla laetud. Seetõttu ongi oluline rakenduste allalaadimisel kontrollida, nende päritolu ja seda, milliseid õiguseid neile antakse. Samuti võib pahavaraga nakatunud rakendus olla seadmesse eelinstalleeritud juba enne selle kliendini jõudmist, kui see ostetakse kasutatult või ebausaldusväärse edasimüüja juurest," lisas ta.

Samuti tasub jälgida oma mobiilsete andmeside ja SMS-teenuste kasutust ka kuu vältel, et märgata võimalikke kahtlasi tegevusi varakult. Lisaks pakuvad mobiilioperaatorid tänapäeval ka laia valikut erinevaid teenuseid, mis aitavad ennast erinevate küberohtude eest paremini kaitsta.

"Soovitamegi alati võtta ühendust meie klienditoega ja seda võimalikult kiiresti peale pahavara või küberrünnaku avastamist, et saaksime teenuse kasutamise peatada. Kui tegemist on välismaa numbritega seotud intsidentidega (kõned või sõnumid), siis kaasnevad Elisale sellega kulud, mis kuuluvad arvel kajastamisele ja mida kahjuks tagasi pöörata ei saa, sest meie peame teistele operaatoritele selle eest omalt poolt tasuma. Just seetõttu on oluline kiiresti reageerida," lisas ta.

- Uudised
- Turvalisus

Pilt


RESET
WiFi