Endgame´i arvutihiir sisaldas pahavara

1 aasta tagasi - 28.07.2025 Autor: AM

Ostad oma uuele võimsale mänguarvutile tippklassi mänguhiire, lootes selle abil domineerida virtuaalsetel lahinguväljadel, siis laadid aga alla ametlikult tootja veebilehelt alla seadistustarkvara, et kõik viimseni paika timmida ja just sel hetkel, otsekui trooja hobune poetab end masinasse salakaval pahavara. Taoline kurb reaalsus tabas hiljuti tuhandeid Endgame Geari mänguhiirte omanikke, kui nende ametlik tarkvara muutus kurjategijate peidupaigaks.

Kuidas kõik alguse sai?

Kõik toimus 26. juunist 9. juulini 2025, mis on valus näide niinimetatud tarneahela rünnakust, mis on viimasel ajal üha sagedamini sihiks võtnud ka mängutööstuse.

Kui pahavara levib tootja ametliku kanali kaudu, on seda uskumatult raske tuvastada. Nagu hoiatas üks Redditi kasutaja Admirable-Raccoon597 MouseReview kogukonnast, kes esimesena kahtlasest käitumisest teada andis: "See ei tulnud mingilt kahtlaselt saidilt ega kolmanda osapoole peegelportaalist. See tuli täiesti ametlikult tarnija lehelt."

Mis peitus Xred-i pahavara taga?

Kurjategijate relvaks oli Windowsi-põhine pahavara nimega Xred. See kogenud tagauks, mis on ringelnud netis juba alates 2019. aastast, on kui digitaalne vampiir, mis imeb arvutisüsteemist välja kõik eluliselt tähtsa. Xred kogub tundlikku süsteemiteavet – MAC-aadresse, kasutajanimesid, arvutinimesid – ja edastab selle kõik ründajatele pahavarasse sisse programmeeritud SMTP e-posti aadresside kaudu.

Eriti murettekitav on Xredi püsivusmehhanism. Kord süsteemi pugenud, loob see peidetud kausta $C:\ProgramData\Synaptics$ ning loob Windowsi registrisse vastava Run-võtme, et säilitada pidev kohalolek nakatunud süsteemides. Nagu osav näitleja, maskeerib see end seadusliku Synapticsi puuteplaadi draiveri tarkvarana, muutes tuvastamise veelgi keerulisemaks.

Lisaks baasandmete vargusele sisaldab Xred ka klahvilogimise funktsionaalsust, mis suudab klaviatuurikonksude abil hõivata pangaparoole ja muu tundliku

teavet.

See tähendab, et iga teie klahvivajutus – olgu see siis salasõna internetipangas või sõbra nimi sotsiaalmeedias – on kurjategijatele kui avatud raamat. Veelgi enam, Xred käitub kui uss, levides USB-mälupulkade kaudu, luues *autorun.inf* faile ja nakatades Exceli faile pahatahtlike VBA makrodega.

Endgame Gear'i vastus ja tulevik

Endgame Gear asendas nakatatud failid puhaste versioonidega 17. juulil, ilma et oleks avalikke hoiatusi väljastanud või rikkumist koheselt tunnistanud, kirjutab Cyber Security News. Alles hiljem ilmus ettevõttelt ametlik turvateade, mis kinnitas intsidenti.

Ettevõte rõhutas, et "ligipääs meie failiserveritele ei olnud ohustatud ning kliendiandmed ei olnud meie serverites kättesaadavad ega mõjutatud ühelgi ajahetkel".

Kuigi see on lohutav, et kliendiandmed otseselt ohustatud ei olnud, tekitab juhtum siiski ekspertide sõnul muret tarneahela turvalisuse pärast. Tootja on sellest ajast alates rakendanud mitmeid turvalisuse parandusi, sealhulgas täiendavaid pahavara skaneerimise protseduure, tugevdatud pahavaravastast kaitset majutavate serverite peal ja kavatseb lisada digitaalsed allkirjad kõikidele tarkvarafailidele.

See juhtum on meeldetuletus, et digitaalses maailmas ei saa kunagi olla liiga ettevaatlik. Isegi ametlikud allikad võivad peita ohte ja digitaalsed kurjategijad on vägagi loovad oma rünnakute meetodites.

Soovitused kasutajatele:

- **Kontrollige failide päritolu:** Enne tarkvara allalaadimist veenduge, et allikas on legitiimne. Kuigi antud juhul oli allikas ametlik, tasub alati kahelda.
- **Kasutage viirusetõrjet:** Veenduge, et teie süsteemis on aktiivne ja ajakohane viirusetõrjetarkvara. See aitab tuvastada ja eemaldada pahavara.
- **Olge tähelepanelik ebatavalise käitumise suhtes:** Kui teie arvuti käitub kummaliselt – aeglustub, kuvab veateateid või avab tundmatuid programme – uurige asja koheselt.
- **Varundage andmed:** Regulaarne andmete varundamine aitab leevendada kahjusid pahavara rünnaku korral.

Endgame Gear OP1w 4K V2: mis hiir see on?

Kuigi artiklis käsitleti peamiselt tarkvara turvaprobleeme, on oluline märkida ka Endgame Gear OP1w 4K V2 hiire tehnilisi omadusi ja jõudlust, mille konfiguratsioonitarkvara pahavaraga nakatati. See hiir, mis on müügil ka Eestis (hind ligikaudu 115 eurot), on mõeldud tõsisele mängurile, pakkudes tipptasemel tehnoloogiat ja kohandamisvõimalusi.

PLUSSID

- **Ülimalt madal latentsus:** hiir pakub 4000 Hz juhtmevaba sagedust, mis tagab erakordselt madala klõpsu- ja liikumisviivituse, andes mängijale olulise eelise. Keskmine klõpsu latentsus on alla 310 mikrosekundi.
- **Täpne andur:** Custom PixArt PAW3950 andur pakub kuni 30 000 CPI resolutsiooni, 750 IPS ja 50G kiirendust, tagades erakordse täpsuse.
- **Vahetatavad lülitid:** peamised nupulülitid on vahetatavad, võimaldades kasutajatel kohandada klõpsutunnetust vastavalt oma eelistustele.
- **Ergonoomiline disain:** uuendatud kuju on optimeeritud *claw grip* haarde jaoks, pakkudes mugavust ka pikkade mängusessioonide ajal.

MIINUSED

- **Tarkvara turvanõrkused:** nagu käesolev artikkel rõhutab, oli konfiguratsioonitarkvara haavatav pahavara suhtes, mis on tõsine murekoht.
- **Võimalik keerukus algajatele:** tänu laialdastele kohandamisvõimalustele ja kõrgetele tehnilistele näitajatele võib hiire seadistamine olla algajatele veidi keeruline.

- Uudised

- Arvutihiired
- Tarkvara
- Turvalisus

Pilt