Haittaohjelmien top 10: kiristysohjelma Mailto yhä suomalaisten suurin riesa, listanousijana Apachen uusi haavoittuvuus

Check Point Research kertoo, että Suomen yleisin haittaohjelma on edelleen kiristysohjelma Mailto. Maailmanlaajuisesti kärkisijaa pitää jo viidennen kerran Trickbot. Uusi Apachen haavoittuvuus on noussut nopeasti eniten hyödynnettyjen haavoittuvuuksien top10:een. Hakkereiden suosikkikohteita ovat maailmalla koulutus ja tutkimus, Suomessa teollisuus.

ESPOO – 11. marraskuuta 2021 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research (CPR) on julkaissut lokakuun haittaohjelmakatsauksensa. Tutkijat kertovat, että modulaarinen bottiverkko ja pankkitroijalainen Trickbot on maailman yleisin haittaohjelma. Sitä esiintyy neljässä prosentissa maailman yritysverkoista.

Trickbot kykenee varastamaan taloudellisia tietoja, tunnuksia ja muita henkilötietoja sekä levittämään verkossa kiristysohjelmia. Trickbot on ollut yleisimpien haittaohjelmien listalla jo viisi kertaa tammikuisen Emotetin alasajon jälkeen. Sitä päivitetään jatkuvasti uusilla ominaisuuksilla ja jakelutavoilla, minkä ansiosta se on joustava ja monikäyttöinen haittaohjelma.

Yleisimmin hyödynnettyjen haavoittuvuuksien joukkoon ylsi lokakuussa uusi haavoittuvuus nimeltään ”Apache HTTP Server Directory Traversal”. Apache julkaisi paikkauksen ohjelmistoonsa, mutta se todettiin riittämättömäksi. Apache HTTP Server -palvelinohjelmistossa on yhä haavoittuvuus, jonka onnistunut hyödyntäminen voi antaa hyökkääjälle pääsyn järjestelmän tiedostoihin.

”Apache-haavoittuvuus havaittiin vasta lokakuun alussa, ja se on jo maailman kymmenenneksi hyödynnetyin, mikä osoittaa, kuinka nopeita hyökkääjät ovat liikkeissään. Apache-käyttäjillä olisi ehdottomasti oltava käytössään riittävät turvatoimet”, sanoo Check Point Softwaren tietoturvatutkijoiden ryhmää johtava **Maya Horowitz**.

Toimialoista hakkerit hyökkäsivät maailmanlaajuisesti useimmin koulutus- ja tutkimusaloille. Suomessa hakkereiden suosikkiala oli teollisuus ja Pohjoismaissa valtionhallinto/puolustusvoimat.

”Maailmanlaajuisesti yksi 61:sta organisaatiosta kärsii kiristysohjelmista joka viikko. Se on järkyttävä luku ja yritysten on tehtävä enemmän. Monet hyökkäykset alkavat yksinkertaisella sähköpostilla, joten käyttäjien koulutus tunnistamaan nämä uhat on yksi organisaatioiden tärkeimmistä torjuntakeinoista”, toteaa Check Pointin Suomen ja Baltian maajohtaja **Sampo Vehkaoja**.

Suomen yleisin haitake lokakuussa oli edelleen kiristysohjelma Mailto. Sitä esiintyi noin seitsemässä prosentissa maan yritysverkoista.

Suomen yleisimmät haittaohjelmat lokakuussa 2021:

1. **Mailto** (tunnetaan myös nimellä NetWalker) – Päivitetty versio Kokoklock-kiristyshaittaohjelmasta, joka leviää enimmäkseen roskapostien kautta. Esiintyvyys 7,39 %.
2. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 3,5 %.
3. **Lokibot** – Tietorosvo, joka tunnistettiin ensimmäisen kerran vuonna 2016. Sillä on versiot sekä Windows- että Android-käyttöjärjestelmille. Haittaohjelma kerää tunnistetietoja

esimerkiksi sovelluksista, selaimista, sähköpostiohjelmista sekä IT-hallintatyökaluista, kuten PuTTY-ohjelmistosta. LokiBotia myydään hakkerointifoorumeilla, ja sen lähdekoodin uskotaan vuotaneen, mikä mahdollistaa lukuiset muunnelmat. Jotkin LokiBotin Android-versiot sisältävät myös kiristysominaisuuden. Esiintyvyys 3,11 %.

4. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 3,11 %.
5. **AgentTesla** – Edistyksellinen etäkäyttötroijalainen, joka pystyy esimerkiksi uhrinsa näppäinten painalluksia seuraamalla ja kuvakaappauksia ottamalla pääsemään käsiksi kohdelaitteen ohjelmistoihin (esimerkiksi Outlook-sähköposti, Google Chrome ja Mozilla Firefox) syötettyihin kirjautumistietoihin. Esiintyvyys 1,95 %.
6. **Taurus** – C/C++ -kielinen tietoja varastava, huhtikuusta 2020 alkaen palveluna myyty haittaohjelma (malware-as-a-service). Taitavasti piiloutuva Taurus leviää yleensä haitallisia liitetiedostoja sisältävien roskapostikampanjoiden välityksellä. Esiintyvyys 1,56 %.
7. **TrickBot** – Windows-alustaan kohdistettu, pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, jota levitetään lähinnä roskapostikampanjoiden tai muiden haittaohjelmaperheiden kautta. Esiintyvyys 1,56 %.
8. **Osiris**, **Rjump**, **Remcos**, **Genome**, **Vidar**, **Qbot** – Kaikkien haittaohjelmien esiintyvyys 1,17 %.

Maailman yleisimmät haittaohjelmat ja haavoittuvuudet lokakuussa 2021:

1. **Trickbot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, joka saa jatkuvasti uusia päivityksiä. Esiintyvyys 4 %.
2. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 3 %.
3. **Remcos** – Jakaa haittaohjelmia roskaposteihin liitettyjen Microsoft Office -asiakirjojen kautta. Esiintyvyys 2 %.

Mobiilihaittaohjelmien globaalilla listalla ensimmäisenä oli **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta sekä asentamaan itsensä uudelleen, jos käyttäjä poistaa sen. Toisella sijalla oli **AlienBot**, joka on palveluna myytävä Android-haittaohjelma (malware-as-a-service). Se sallii hyökkääjän ujuttaa pankkisovelluksiin haitallista koodia, jolloin hyökkääjä saa pääsyn uhrien tileille ja lopulta koko laitteen hallinnan. Kolmannella sijalla oli kiinalaisen hakkeriryhmän kehittämä haittaohjelma **XLoader**, joka levittää tartunnan saaneita Android-sovelluksia keräten niiden avulla pankki- ja henkilötietoja.

Check Pointin tutkijat listasivat myös lokakuun käytetyimmät **haavoittuvuudet**. Yleisintä haavoittuvuutta nimeltään ”**Web Servers Malicious URL Directory Traversal** (CVE-2010-4598, CVE-2011-2474, CVE-2014-0130, CVE-2014-0780, CVE-2015-0666, CVE-2015-4068, CVE-2015-7254, CVE-2016-4523, CVE-2016-8530, CVE-2017-11512, CVE-2018-3948, CVE-2018-3949, CVE-2019-18952, CVE-2020-5410, CVE-2020-8260)” on yritetty hyödyntää 60 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli nimeltään ”**Web Server Exposed Git Repository Information Disclosure**”, ja sen esiintyvyys oli 55 %. Kolmannella sijalla oli ”**HTTP Headers Remote Code Execution (**CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-13756)”, jonka esiintyvyys oli 54 %.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin™ tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä Check Pointin tietoturvalaitteilta

kautta maailman ja näyttää ne reaaliaikaisesti kartalla. ThreatCloud-tietokanta tarkastaa yli 3 miljardia verkkosivustoa ja 600 miljoonaa tiedostoa sekä tunnistaa yli 250 miljoonaa haittaohjelmatoimintaa päivittäin.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista.
Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa www.checkpoint.com.

Lisätiedot:
Sampo Vehkaoja, Country Manager, Finland and Baltics, Check Point Software Technologies, sampov@checkpoint.com, p. 050 555 5500
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

Seuraa Check Point Researchia:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_
Podcast: https://research.checkpoint.com/category/cpradio/
Facebook: https://www.facebook.com/checkpointresearch

Check Point Research
Check Point Research (research.checkpoint.com) huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvayhteisöllä on käytettävissään paras mahdollinen tieto kyberturvallisuuden riskeistä. Tutkijaryhmä kerää ja analysoi ThreatCloud-verkkopalvelun tallentamat maailmanlaajuiset kyberhyökkäystiedot, jotta hakkerit pysyvät kurissa ja kaikki Check Pointin tuotteet pystytään päivittämään uusimmilla suojauksilla. Tutkijaryhmä koostuu yli 100 analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvayhtiöiden ja viranomaisten kanssa.

Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Siihen sisältyvät Check Point Harmony etäkäyttäjille, Check Point CloudGuard pilven automaattiseen suojaukseen ja Check Point Quantum datakeskusten suojaukseen. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.