Suomen ja maailman yleisimmät haittaohjelmat: Dridex katosi kartalta, kärkeen nousi Trickbot – ”Kyberhyökkäysten määrä kasvaa nyt valtavasti”

Tietoturvayhtiö Check Pointin tutkijat kertovat, että viime kuukausien yleisin, usein kiristyshyökkäysten alkuvaiheissa käytetty Dridex-troijalainen on pudonnut haittaohjelmien top 10 -listauksesta. Suomen ja koko maailman listakärjessä oli toukokuussa Trickbot.

ESPOO – 15. kesäkuuta 2021 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut toukokuun haittaohjelmakatsauksensa.

Tutkijat kertovat, että maailman ja Suomen yleisin haittaohjelma toukokuussa oli Trickbot, joka nousi kymmenen kärkeen ensimmäistä kertaa huhtikuussa 2019. Viime kuukausien maailmanlaajuisen ”kiristyshyökkäyspandemian” aikana kärkisijaa pitänyt Dridex-troijalainen on poistunut yleisimpien haittaohjelmien listauksesta kokonaan.

Vielä ei ole tiedossa, miksi Dridex on joukosta poissa. Viimeisimpien tietojen valossa syy saattaa kuitenkin olla siinä, että Dridexin jakelijana tunnettu Evil Corp -ryhmä on muuttanut toimintatapaansa pyrkiessään välttämään Yhdysvaltojen valtiovarainministeriön seuraamukset.

Ensimmäiselle sijalle nousi toukokuussa bottiverkko- ja pankkitroijalainen Trickbot, joka voi varastaa tilitunnuksia ja muita taloudellisia ja henkilökohtaisia tietoja sekä levittää kiristyshaittaohjelmia, erityisesti Ryukia. Sitä päivitetään jatkuvasti uusilla ominaisuuksilla, minkä ansiosta se on joustava ja monikäyttöinen haittaohjelma. Trickbot kasvatti suosiotaan Emotet-botnetin poistamisen jälkeen tammikuussa.

Check Point Research on havainnut merkittävän kasvun yrityksiin kohdistuvien kyberhyökkäysten määrässä vuoden 2021 alusta lähtien. Vuoden takaiseen, toukokuuhun 2020 verrattuna EMEA-alueella kasvua on tapahtunut 97 %, Suomessa jopa 146 %. Yhdysvalloissa kasvua on 70 % ja APAC-alueella huikeat 168 %.

"Viimeaikaisesta kiristyshyökkäysten määrän kasvusta puhutaan nyt paljon, mutta itse asiassa kyberhyökkäysten määrä kasvaa nyt valtavasti yleisestikin. Se on merkittävä ja huolestuttava trendi”, sanoo Check Pointin Threat Intelligence & Research -tuoteryhmän johtaja **Maya Horowitz**.

"Yritysten on oltava tietoisia riskeistä ja varmistettava, että niillä on käytettävissä asianmukaiset tietoturvaratkaisut. Hyökkäyksiä voidaan paitsi havaita, myös estää, mukaan lukien nollapäivän hyökkäykset ja tuntemattomat haittaohjelmat. Oikeiden tekniikoiden avulla suurin osa hyökkäyksistä, edistyneimmistäkin, voidaan estää ennen kuin ne pääsevät häiritsemään liiketoimintaa", toteaa Check Pointin Suomen ja Baltian maajohtaja **Sampo Vehkaoja**.

Suomenkin yleisin haittaohjelma toukokuussa oli Trickbot, jota esiintyi lähes kuudessa prosentissa maan yritysverkoista. Sitä seurasivat kryptovaluutan louhija XMRig ja kiristyshaitake REvil.

Suomen yleisimmät haittaohjelmat toukokuussa 2021:

1. **TrickBot** – Windows-alustaan kohdistettu, pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, jota levitetään lähinnä roskapostikampanjoiden tai muiden haittaohjelmaperheiden kautta. Esiintyvyys 5,69 %.

2. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 2,44 %.
3. **REvil** – Ensimmäistä kertaa vuonna 2019 havaittu, palveluna myyty kiristyshaittaohjelma (ransomware-as-a-service), joka salakirjoittaa uhrinsa tiedostot ja vaatii lunnaita niiden palauttamisesta. Esiintyvyys 1,63 %.
4. **Lokibot** – Android- ja Windows-laitteiden Infostealer-haitake, joka voi myös muuntua kiristysohjelmaksi. Esiintyvyys 1,63 %.
5. **Arkei** – Troijalainen, joka varastaa luottamuksellisia tietoja, kuten kirjautumistunnuksia. Esiintyvyys 1,22 %.
6. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 1,22 %.
7. **BLINDINGCAN** – Uusi etäkäyttötroijalainen (RAT). Esiintyvyys 0,41 %.
8. Lisäksi esiintyvyydeltään 0,41 % olivat haittaohjelmat **Bonzo**, **Darkcomet**, **Fareit**, **Neshta**, **Ramnit**, **ACLabuse**, **Slub**, **AutoRun**, **Swrort**, **Taurus**, **Underminer EK**, **Vidar**, **Zloader** ja **Shiz**.

Maailman yleisimmät haittaohjelmat ja haavoittuvuudet toukokuussa 2021:

1. **Trickbot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, joka saa jatkuvasti uusia päivityksiä. Esiintyvyys 8 %.
2. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 3 %.
3. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 3 %.

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 Android-laitteiden takaovi **Triada**, joka myöntää superkäyttäjäoikeudet ladattuihin haittaohjelmiin. Kolmannella sijalla oli Android-haittaohjelma **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia.

Check Pointin tutkijat listasivat myös toukokuun käytetyimmät **haavoittuvuudet**. Yleisintä haavoittuvuutta nimeltään **“Web Server Exposed Git Repository Information Disclosure”** on yritetty hyödyntää 48 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli nimeltään **”HTTP Headers Remote Code Execution (CVE-2020-13756)”**, jonka esiintyvyys oli 47,5 %. Kolmannella sijalla oli **“MVPower DVR Remote Code Execution”**, jonka esiintyvyys oli 46 %.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin™ tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä 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. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.