**Yleisimmät haittaohjelmat: Trickbot pysyttelee kärjessä**

*Tietoturvayhtiö Check Pointin tutkijat kertovat, että kiristyshyökkäyksissä valmistelevana vaiheena usein käytetty Trickbot on pysytellyt maailman yleisimpien haittaohjelmien listakärjessä nyt kahden kuukauden ajan.*

**ESPOO – 13. heinäkuuta 2021 –** Maailman johtavan tietoturvayhtiön [Check Point Software Technologiesin](https://www.checkpoint.com/) tutkimustoiminnasta vastaava Check Point Research (CPR) on julkaissut uusimman haittaohjelmakatsauksensa. Tutkijat kertovat, että toukokuussa yleisimpien haittaohjelmien listakärkeen noussut Trickbot piti asemansa myös kesäkuussa.

Trickbot on troijalainen ja bottiverkko, joka kykenee nappaamaan henkilötietoja sekä pankki- ja muiden tilien käytössä tarvittavia tunnuksia. Se pystyy myös etenemään tietoverkossa ja salakuljettamaan sinne kiristyshaittaohjelmia. CPR kertoi jo viime kuussa, että yritysverkkoihin kohdistuva haittaohjelmahyökkäysten viikoittainen määrä oli lähes kaksinkertaistunut vuoden takaisesta. Samalla tietoturvatutkijat muistuttivat, ettei kiristykseen tähtäävä hyökkäys useinkaan ala kiristyshaittaohjelmalla. Esimerkiksi tyypillinen [Ryuk-kiristyshaittaohjelman hyökkäys](https://blog.checkpoint.com/2021/06/23/global-surge-in-ransomware-attacks-to-pay-or-not-to-pay-is-not-the-only-question/) eteni siten, että tietoverkkoon tunkeutui Emotet-haittaohjelma. Se valmisteli tietä Trickbotille, minkä jälkeen varsinainen kiristyshaittaohjelma salasi ja lukitsi datan.

[Emotet-bottiverkko hajotettiin](https://blog.checkpoint.com/2021/01/28/collaborative-global-effort-disrupts-emotet-worlds-most-dangerous-malware/) tammikuussa, minkä jälkeen Trickbot on kasvattanut mainetta ja kyberkonnien suosiota myös bottiverkkona. Se on [viime aikoina yhdistetty](https://thehackernews.com/2021/07/trickbot-botnet-found-deploying-new.html) myös uuteen kiristyshaittaohjelmaan nimeltä Diavol. Trickbotia päivitetään jatkuvasti uusilla ominaisuuksilla ja levitystavoilla, minkä ansiosta se on rikollisten kannalta joustava ja monikäyttöinen haittaohjelma.

”Tunnetut, Ryukin ja REvilin tyyppiset kiristyshaittaohjelmaryhmät antavat yleensä tartunnan alkuvaiheen jonkin muun haittaohjelman hoidettavaksi. Trickbot on tyypillinen tällainen apuohjelma. Organisaatioissa on hyvä ymmärtää akuutit tietoturvariskit ja huolehtia siitä, että riittävät suojaukset ovat paikoillaan ja toiminnassa. Trickbotin ohella tämän kuukauden Top 10 -lista sisältää joukon hyvin erityyppisiä haittaohjelmia: bottiverkkoja, takaovia, tietokaappareita, etäkäyttötroijalaisia (RAT) ja mobiilihaittaohjelmia. On tärkeää, että käytössä oleva tietoturvaratkaisu kattaa koko riskien kirjon. Lähes kaikilta hyökkäyksiltä on mahdollista suojautua niin, ettei normaali liiketoiminta häiriinny”, kommentoi **Maya Horowitz**, Check Pointin Director, Threat Intelligence & Research, Products.

Suomen yleisimpien haittaohjelmien listalla Trickbot oli kesäkuussa jaetulla ykkössijalla Arkei-troijalaisen kanssa. Trickbotin esiintyvyys ei meillä ollut aivan samaa luokkaa kuin kansainvälisesti.

**Suomen yleisimmät haittaohjelmat kesäkuussa 2021:**

1. **Arkei** – Troijalainen, joka anastaa luottamuksellisia tietoja, kuten salasanoja ja pankkitunnuksia. Esiintyvyys 1,65 %.
2. **TrickBot** – Bottiverkko ja pankkitroijalainen, jota levitetään lähinnä roskapostikampanjoiden tai muiden haittaohjelmaperheiden kautta. Trickbot lähettää eteenpäin tietoja tartunnan saaneesta tietoverkosta ja pystyy välittämään tietoverkkoon monenlaisia haittaohjelmapaketteja. Käytetään usein kiristyshyökkäysten valmisteluun. Esiintyvyys 1,65 %.
3. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 1,23 %.
4. **SpelevoEK** – Exploit Kit eli ohjelma, jota käytetään tunnistamaan tietoverkosta laitteet, joissa on haavoittuvuuksia. Esiintyvyys 0,82 %.
5. **Neshta** – Troijalainen, joka löydettiin vuonna 2010. Tekee tietokoneen rekistereihin ja hakukoneiden asetuksiin muutoksia, jotka mahdollistavat haitallisten lisäosien ja valikkojen lisäämisen. Esiintyvyys 0,82 %.
6. **Darkside** – RaaS eli palveluna ostettava kiristyshaittaohjelma tunnetaan hyökkäyksistään hieman harvinaisempiin kohteisiin, kuten öljy- ja kaasuyhtiöiden palvelimiin. Esiintyvyys 0,82 %.
7. **FluBot** – Esiintyvyys 0,82 %.
8. **NJRat** – Monipuoliset toiminnot omaava etäohjaustroijalainen, jonka uhreina on ollut valtiollisia toimijoita ja organisaatioita etenkin Lähi-Idässä. Esiintyvyys 0,82 %.
9. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 0,82 %.

Haittaohjelmat **MyDoom, Kryptik, Icedid, Formbook, Qbot, EtterSilent, Blakken, Auto CAD, GULoader, Pykspa, Remcos, RigEK, Scrinject, sLoad, Slugin, Tempedreve, Tepfer, Tofsee, Turla, Unruy ja Phorpiex.** jakoivat 10. sijan esiintyvyydellä 0,41 %.

**Maailman yleisimmät haittaohjelmat ja haavoittuvuudet kesäkuussa 2021:**

1. **Trickbot**– Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, joka saa jatkuvasti uusia päivityksiä. Esiintyvyys 7 %.
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 kesäkuussa Android-haittaohjelma **XHelper**, jota käytetään muiden haittaohjelmien lataamiseen ja mainosten näyttämiseen. Toiseksi yleisin oli **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa sekin levittää mainoksia. Kolmantena listalla oli kiinalaisen hakkeriryhmän kehittämä **XLoader,** joka levittää tartunnan saaneita sovelluksia keräten niiden avulla pankki- ja henkilötietoja.

Check Pointin tutkijat listasivat myös kesäkuun käytetyimmät haavoittuvuudet. Yleisintä haavoittuvuutta nimeltään **”HTTP Headers Remote Code Execution (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756)”** on yritetty hyödyntää 47 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli **“MVPower DVR Remote Code Execution”**, jonka esiintyvyys oli 45 %. Kolmannella sijalla oli **”Dasan GPON Router Authentication Bypass (CVE-2018-10561)”**, esiintyvyys 44 %.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudinTM 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.](https://blog.checkpoint.com/)

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa [www.checkpoint.com](http://www.checkpoint.com).

**Lisätiedot:**

Sampo Vehkaoja, Country Manager, Finland and Baltics, Check Point Software Technologies, sampov@checkpoint.com, p. 050 555 5500
Haastattelupyynnöt: Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065.

**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](https://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](http://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.