**Huhtikuun haittaohjelmakatsaus: Troijalaiset yleistyivät, Trickbot palasi listoille**

*Monitaitoinen Trickbot-pankkitroijalainen palasi huhtikuussa maailman yleisimpien haittaohjelmien Top 10 -listalle lähes kahden vuoden tauon jälkeen. Suomen listalla se oli kuudes ja kansainvälisellä listalla kahdeksas. Myös muut troijalaiset ovat yleistyneet.*

**ESPOO – 15. toukokuuta 2019 –** Tietoturvayhtiö Check Pointin ylläpitämälle maailman yleisimpien haittaohjelmien Top 10 -listalle nousi huhtikuussa seitsemän troijalaista, vaikka kolmen kärkeä pitivätkin edelleen hallussaan kryptolouhijat. Erityisen voimakkaasti kasvoi monitaitoisen Trickbot-pankkitroijalaisen esiintyvyys. Se kohosi takaisin listalle lähes kahden vuoden tauon jälkeen. Se oli kansainvälisellä listalla kahdeksantena ja Suomen listalla kuudentena.

Huhtikuun Trickbot-kampanja oli ajoitettu lähelle Yhdysvaltain veroilmoitusten jättöpäivää (Tax Day), joka oli 15. huhtikuuta. Kyberrikollisten roskapostikampanja levitti Excel-tiedostoa, joka latasi Trickbotin uhrin tietokoneelle. Troijalainen keräsi pankkiasiointiin liittyviä tietoja ja mahdollisesti nappasi verolomakkeita, jotka päätyivät täten asiattomiin käsiin.

Troijalaisten yleistyminen viittaa siihen, että useiden suosittujen kryptolouhintapalveluiden lopetettua toimintansa kyberrikolliset ovat vaihtamassa taktiikkaa ja etsimässä uusia ansaintamuotoja.

Check Pointin Threat Intelligence and Research Director **Maya Horowitz** kommentoi tilannetta sanoen, että sekä Trickbotin että Emotetin päätyminen kymmenen useimmin yritysverkoista tavatun haittaohjelman joukkoon on erityisen huolestuttavaa.

”Molempia käytetään nykyään henkilötietojen ja salasanojen urkkimisen ohella myös levittämään Ryuk-kiristyshaittaohjelmaa. Ryuk on tunnettu siitä, että se ottaa kohteikseen tietokantoja ja backup-palvelimia ja pyytää tietojen vapauttamisesta isoja, yli miljoonan dollarin lunnaita. Koska haittaohjelmat muuntuvat koko ajan, organisaatioiden on tärkeää suojata itsensä niiltä kehittyneen uhkientorjunnan avulla”, hän jatkoi.

**Suomen yleisimmät haittaohjelmat huhtikuussa 2019:**

1. Jsecoin– Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa. Esiintyvyys 10 % organisaatioista.
2. XMRig – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017. Esiintyvyys 8 % organisaatioista.
3. Cryptoloot – Kryptovaluutan louhija, joka louhii Moneroa. Esiintyvyys 8 %.
4. Nivdort – Troijalainen, joka kerää salasanoja ja tietoa käyttäjän asetuksista. Esiintyvyys 5 %.
5. Ramnit – Mato, joka leviää etenkin ulkoisten kovalevyjen ja julkisten FTP-palvelinten kautta. Esiintyvyys 4 %.
6. Trickbot, 7. Dorkbot, 8. Neshta, 9. Fireball, 10. Emotet

**Maailman yleisimmät haittaohjelmat huhtikuussa 2019 Top 3:**

1. Cryptoloot – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. XMRig – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan.
3. Jsecoin – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa.
4. Emotet, 5. Dorkbot, 6. Ramnit, 7. AgentTesla, 8. Trickbot, 9. Sality, 10. Lokibot

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli **Triada**, Android-laitteiden takaovi, jonka avulla hyökkääjä saa laitteen pääkäyttäjäoikeudet. **Lotoor**, joka on Android-laitteiden haavoittuvuuksia hyödyntävä hakkerityökalu, piti toisen sijansa. Listakolmoseksi putosi **Hiddad**, jonka tärkein toimintamuoto on mainosten levittäminen. Se pystyy kuitenkin myös nappaamaan käyttäjätietoja Android-puhelimelta ja välittämään ne eteenpäin vääriin käsiin.

Check Pointin tutkijat listasivat myös käytetyimmät haavoittuvuudet. Kärkeen nousi **OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)**, johon kohdistuvien hyökkäysten esiintyvyys yritysverkoissa oli 44 %. **Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow CVE-2017-7269** menetti paikkansa ensimmäisen kerran 12 kuukauteen. Hyökkäysten esiintyvyys oli 40 %. Kolmanneksi hyödynnetyin haavoittuvuus oli **Apache Struts2 Content-Type Remote Code Execution (CVE-2017-5638),** hyökkäysten esiintyvyys38 % organisaatioista.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista osoitteesta

<https://blog.checkpoint.com/2019/05/14/april-2019s-most-wanted-malware-cybercriminals-up-to-old-trickbots-crypto-cryptomining-security-ryuk/>

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa <http://www.checkpoint.com/threat-prevention-resources/index.html>

**Lisätiedot ja haastattelupyynnöt:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, [ramira@checkpoint.com](mailto:ramira@checkpoint.com)

Maija Rauha, viestintäkonsultti, OSG Viestintä, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065

**Seuraa Check Pointia:**

Twitter: <http://www.twitter.com/checkpointsw>

Facebook: <https://www.facebook.com/checkpointsoftware>

Blog: <http://blog.checkpoint.com>

YouTube: <http://www.youtube.com/user/CPGlobal>

LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

**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 kohdistettujen hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri käsittää uuden 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen kaikkia verkko-, pilvi- ja mobiilitoimintoja kaikilta tunnetuilta hyökkäyksiltä, ja sitä hallitaan alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän kautta. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.