**Korona-aiheiset roskapostit kylvävät WiFi-salasanoja vaanivaa haittaohjelmaa**

*Tietoturvayhtiö Check Pointin tutkijoiden mukaan Dridex-pankkitroijalainen oli huhtikuun yleisin kyberuhka maailmassa. Kolmanneksi kiri Agent Tesla -etäkäyttötroijalaisen uusi versio, joka pystyy muun muassa varastamaan WiFi-salasanoja.*

**ESPOO – 11. toukokuuta 2020 –** Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research kertoo haittaohjelmakatsauksessaan, että maailman yleisimpien haittaohjelmien listan kolmannelle sijalle on noussut Agent Tesla -etäkäyttötroijalaisen uusi versio. Haittaohjelmaa esiintyi huhtikuussa kolmessa prosentissa maailman yritysverkoista. Sitä on levitetty useissa koronavirusaiheisissa roskapostikampanjoissa.

Agent Teslaa on muokattu varastamaan kohdetietokoneilta WiFi-salasanoja muiden tietojen, kuten Outlook-sähköpostitietojen, lisäksi. Huhtikuussa haittaohjelmaa jaettiin liitetiedostona useissa koronavirusaiheisissa roskapostikampanjoissa, jotka houkuttelivat uhria lataamaan haitallisen tiedoston tarjoamalla mielenkiintoista tietoa pandemiasta. Esimerkiksi Maailman terveysjärjestö WHO:n nimissä lähetetyn viestin aiheena olivat koronavirusrokotteet (‘URGENT INFORMATION LETTER: FIRST HUMAN COVID-19 VACCINE TEST / RESULT UPDATE”). Tämä osoittaa, kuinka hakkerit hyödyntävät maailmanlaajuisia uutisia ja huolenaiheita hyökkäystensä onnistumiseksi.

Tunnettu pankkitroijalainen Dridex, joka oli maaliskuussa ensimmäistä kertaa kymmenen yleisimmän haittaohjelman listalla, oli huhtikuussa entistä vaikuttavampi. Se nousi listan kolmannelta sijalta ensimmäiseksi, esiintyen neljässä prosentissa organisaatioista maailmanlaajuisesti. Maaliskuun yleisin haittaohjelma XMRig putosi toiselle sijalle.

"Huhtikuussa havaitsemamme Agent Teslaa levittävät kampanjat osoittavat, kuinka ketteriä kyberrikolliset ovat uutisten hyödyntämisessä ja hyväuskoisten uhriensa huijaamisessa napsauttamaan haitallisia linkkejä", kertoo Check Pointin **Maya Horowitz**, Director, Threat Intelligence & Research, Products.

”Sekä Agent Tesla että Dridex ovat haittaohjelmien kolmen kärjessä, joten kyberrikolliset keskittyvät nyt käyttäjien henkilökohtaisten ja yritystietojen varastamiseen rahaa ansaitakseen. On välttämätöntä, että yritykset pitävät henkilökuntansa ajan tasalla uusimmista suojautumistekniikoista ja työkaluista, etenkin kun yhä useampi työskentelee nyt etänä."

Check Pointin tutkijat varoittavat myös, että ”MVPower DVR Remote Code Execution” oli yhä yleisin hyväksikäytetty haavoittuvuus. Sitä esiintyi 46 prosentissa yritysverkoista maailmanlaajuisesti. Tätä seurasi ”OpenSSL TLS DTLS Heartbeat Information Disclosure”, jonka esiintyvyys oli 41 prosenttia. Kolmannella sijalla oli “Command Injection over HTTP Payload”, esiintyvyydeltään 40 prosenttia.

Suomessa huhtikuun yleisin haittaohjelma oli modulaarinen Emotet-troijalainen, jota esiintyi 1,8 prosentissa maan yritysverkoista. Toisella sijalla oli Mirai, joka on tunnettu IoT (Internet of Things) -laitteiden tartuttamisesta ja massiivisista DDoS-hyökkäyksistä. Maan kolmanneksi yleisin haittaohjelma oli kryptovaluutan louhija XMRig.

**Suomen yleisimmät haittaohjelmat huhtikuussa 2020:**

1. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään nykyään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 1,87 %.
2. **Mirai** – Tunnettu haavoittuvien IoT (Internet of Things) -laitteiden tartuttamisesta ja massiivisista DDoS-hyökkäyksistä. Esiintyvyys 1,87 %.
3. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 1,87 %.
4. **Jsecoin** – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 1,40 %.
5. **Shiz** – Haittaohjelma, joka kätkeytyy Windows-ohjelmiin ja pyrkii varastamaan käyttäjän tietoja. Esiintyvyys 1,40 %.
6. **TrickBot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 1,40 %.
7. **Tofsee** – Windows-alustaan kohdistuva haittaohjelma yrittää ladata ja suorittaa muita haitallisia tiedostoja kohdejärjestelmissä. Esiintyvyys 1,40 %.
8. **RigEK** – Haittaohjelmien lataaja Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksissa. Esiintyvyys 0,93%.
9. **Ramnit** – Mato, joka leviää pääasiassa ulkoisten kovalevyjen ja avoimien FTP-palvelinten kautta. Mato luo itsestään kopion ja tartuttaa laitteen ulkoiset ja sisäiset muistit. Esiintyvyys 0,93%.
10. **Adposhel**. Esiintyvyys 0,93%.
11. **Adylkuzz**. Esiintyvyys 0,93%.
12. **Catch22**. Esiintyvyys 0,93%.
13. **Facexworm** – Haittaohjelma varastaa salasanoja ja kryptovaluuttaa ja levittää roskapostia Facebook-käyttäjille. Esiintyvyys 0,93%.
14. **Valerie**. Esiintyvyys 0,93%.

**Maailman yleisimmät haittaohjelmat ja haavoittuvuudet huhtikuussa 2020:**

1. **Dridex** – Windows-laitteiden pankkitroijalainen, joka ohjaa uhrin pankkitiedot hyökkääjän hallitsemaan palvelimeen. Dridex ottaa yhteyttä etäpalvelimeen, lähettää tietoja tartunnan saaneesta järjestelmästä ja voi myös ladata ja suorittaa lisämoduuleja kauko-ohjausta varten. Esiintyvyys 4 %.
2. **XMRig** – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan. Esiintyvyys 4 %.
3. **Agent Tesla** – Edistyksellinen etäkäyttötroijalainen, joka pystyy esimerkiksi uhrinsa näppäinten painalluksia seuraamalla ja kuvakaappauksia ottamalla pääsemään käsiksi WiFi-salasanoihin ja muihin kohdelaitteen (esimerkiksi Outlook-sähköposti, Google Chrome ja Mozilla Firefox) tietoihin. Esiintyvyys 3 %.

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli huhtikuussa **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta ja asentamaan itsensä uudelleen, jos käyttäjä poistaa sen. Toiseksi yleisin oli Android-laitteiden haavoittuvuuksia hyödyntävä hakkerityökalu **Lotoor**. Kolmannella sijalla oli Android-käyttäjiin kohdistuva mainosohjelma **AndroidBauts.**

Check Pointin tutkijat listasivat myös huhtikuun käytetyimmät **haavoittuvuudet**. Luettelon kärjessä oli **“MVPower DVR Remote Code Execution”**, jota yritettiin hyödyntää 46 prosentissa yritysverkoista maailmanlaajuisesti. Toiseksi yleisin oli **“OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)”**, esiintyvyys 41 prosenttia. Kolmannella sijalla oli **“Command Injection Over HTTP Payload”**, esiintyvyys 40prosenttia.

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 2,5 miljardia verkkosivustoa ja 500 miljoonaa tiedostoa sekä tunnistaa yli 250 miljoonaa haittaohjelmatoimintaa päivittäin.

Täydellinen Top 10 -haittaohjelmalista löytyy [Check Pointin blogista](https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/).

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

**Lisätiedot:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com.
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

**Seuraa Check Point Researchia:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**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.