**Kiristyshaittaohjelma leviää Excel-tiedostoissa  
– Vanha tuttu pankkitroijalainen on nyt vaarallisempi kuin koskaan**

*Tunnettu Dridex-pankkitroijalainen kylvää nyt kiristyshaittaohjelmia roskapostikampanjoiden liitetiedostojen avulla. Tietoturvayhtiö Check Pointin tutkijat kehottavat varsinkin etätyöntekijöitä tarkkaavaisuuteen.*

**ESPOO – 9. huhtikuuta 2020 –** Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research kertoo haittaohjelmakatsauksessaan, että tunnettu pankkitroijalainen Dridex on noussut ensimmäistä kertaa kymmenen yleisimmän haittaohjelman joukkoon. Vuonna 2011 ensimmäisen kerran havaittu Dridex oli maaliskuussa maailman kolmanneksi yleisin haittaohjelma. Sitä käytetään kohdennettujen kiristysohjelmien, kuten BitPaymerin ja DoppelPaymerin, lataamiseen.

Dridex on lähtenyt uuteen nousuun useiden roskapostikampanjoiden avulla. Sähköpostiviesteissä on mukana Excel-liitetiedosto, joka klikattaessa lataa Dridexin uhrin laitteelle. Windows-laitteille tähdätty Dridex pyrkii nappaamaan uhrin pankkitietoja ja muita henkilötietoja mahdollistaakseen rikolliset rahansiirrot. Haittaohjelmaa on järjestelmällisesti päivitetty ja kehitetty viimeisen vuosikymmenen aikana.

Ensimmäisellä sijalla yleisimpien haittaohjelmien listalla säilyi XMRig. Sitä esiintyy 5 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavina ovat Jsecoin ja Dridex, joita esiintyi 3–4 prosentissa organisaatioista.

”Dridex on nyt ensimmäistä kertaa käytetyimpien haittaohjelmien listalla, mikä osoittaa, kuinka nopeasti verkkorikolliset voivat vaihtaa menetelmiä. Tällainen kehittynyt haittaohjelma voi olla rikollisille erittäin tuottoisa. Sitä käytetään nyt myös kiristyshaittaohjelman lataajana, mikä tekee siitä aiempia versioita vaarallisemman. Kannattaa olla tarkkana liitetiedostojen suhteen, vaikka ne näyttäisivät tulevan luotettavasta lähteestä, etenkin etätyön lisäännyttyä viime viikkoina. Organisaatioiden tulee ohjeistaa työntekijänsä tunnistamaan haitalliset roskapostit ja ottaa käyttöön tietoturva, joka auttaa niitä suojaamaan tiiminsä ja verkkonsa tällaisilta uhilta, sanoo Check Pointin Threat Intelligence & Research -tuoteryhmän johtaja **Maya Horowitz**.

Suomessa maaliskuun yleisin haittaohjelma oli kryptovaluutan louhija XMRig, jota esiintyi noin kuudessa prosentissa maan yritysverkoista. Toisella sijalla oli RigEK, joka käyttää Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksia. Tartuntaketju alkaa uudelleenohjauksella aloitussivulle, joka sisältää haavoittuvat plug-init tarkistavan JavaScriptin. Dridex-pankkitroijalainen oli kolmanneksi yleisin haittaohjelma myös Suomessa.

**Suomen yleisimmät haittaohjelmat maaliskuussa 2020:**

1. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 6,05 %.
2. **RigEK** – Haittaohjelmien lataaja Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksissa. Esiintyvyys 5,58 %.
3. **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-ohjauksella. Esiintyvyys 4,65 %.
4. **TrickBot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 4,19 %.
5. **Tofsee** – Windows-alustaan kohdistuva haittaohjelma yrittää ladata ja suorittaa muita haitallisia tiedostoja kohdejärjestelmissä. Esiintyvyys 3,72 %.
6. **Loyeetro** – Tämä uhka yrittää varastaa arkaluontoisia ja luottamuksellisia tietoja. Esiintyvyys 2,79 %.
7. **Jsecoin** – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 1,86 %.
8. **Facexworm** – Haittaohjelma varastaa salasanoja ja kryptovaluuttaa ja levittää roskapostia Facebook-käyttäjille. Esiintyvyys 1,40 %.
9. **Valerie**. Esiintyvyys 1,40 %.
10. **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 1,40 %.
11. **NanoCore** – Etäkäyttöön tarkoitettu troijalainen, joka on suunnattu Windows-käyttöjärjestelmän käyttäjille. Esiintyvyys 1,40 %.

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

1. **XMRig** – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan. Esiintyvyys 5 %.
2. **Jsecoin** – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 4 %.
3. **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 3 %.

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli maaliskuussa **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-käyttäjiin kohdistuva mainosohjelma **AndroidBauts.** Kolmannella sijalla oli Android-laitteiden haavoittuvuuksia hyödyntävä hakkerityökalu **Lotoor**.

Check Pointin tutkijat listasivat myös maaliskuun käytetyimmät **haavoittuvuudet**. Luettelon kärjessä oli **“MVPower DVR Remote Code Execution”**, jota yritettiin hyödyntää 30 prosentissa yritysverkoista maailmanlaajuisesti. Toiseksi yleisin oli **“PHP php-cgi Query String Parameter Code Execution”**, esiintyvyys 29 prosenttia. Kolmannella sijalla oli **“OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)”**, esiintyvyys 27 prosenttia.

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/2020/04/09/march-2020s-most-wanted-malware-dridex-banking-trojan-ranks-on-top-malware-list-for-first-time/).

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](mailto:ramira@checkpoint.com).  
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, [paivi.savolainen@osg.fi](mailto: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.