**Check Pointin haittaohjelmakatsaus 2/2018**

Tammikuun etsityin: Krypotolouhijat pyrkivät tietokoneille myös Suomessa

*Kryptovaluutan salalouhintaan käytetyt ohjelmat ovat yleistyneet nopeasti myös Suomessa. Tietoturvayhtiö Check Point Software Technologiesin ylläpitämän tilaston mukaan Coinhive oli tammikuussa maan toiseksi levinnein haittaohjelma yritysverkoissa.*

**Espoo — 15. helmikuuta 2018.** Check Pointin tutkijat kertovat raportissaan, että Monero-virtuaalivaluuttaa louhiva Coinhive löytyi maailmanlaajuisesti melkein joka neljännestä (23 %) yritysverkosta tammikuussa. Kymmenen yleisimmän haittaohjelman listalla Coinhive piti kärkipaikkaa, ja mukana oli myös kaksi muuta kryptolouhijaa. Suomessa Coinhive oli toiseksi yleisin yritysverkkojen haittaohjelma Fireballin jälkeen.

Kryptovaluutan louhijoita käyttävät muutkin kuin rikolliset eikä louhinta ole sinänsä laitonta. Kyberrikolliset voivat kuitenkin valjastaa ohjelmien avulla osan uhrien tietokoneiden suorituskyvystä louhimaan kryptovaluuttaa itselleen, mikä voi haitata tietokoneen toimintaa. Louhijan mukana on lisäksi mahdollista ujuttaa koneelle myös varsinaisia haittaohjelmia.

”Kryptolouhijat ovat yleistyneet tasaisesti kolmen viime kuukauden aikana, ja niistä on tullut yritysten kannalta uhka. Niiltä on erityisen haasteellista suojautua, koska ne ovat usein verkkosivuilla kätkettyinä. Uhri ei huomaa eikä tiedä, että hänen laitteellaan louhitaan kryptovaluuttaa rikolliselle. Olisi tärkeää, että yrityksillä olisi käytössä tietoturvaratkaisu, joka suojaa näiltä salakavalilta kyberhyökkäyksiltä”, sanoi **Maya Horowitz** Check Pointin tutkimusryhmästä.

Lisäksi Check Pointin tutkijat havaitsivat, että 21 prosentissa organisaatioista on yhä Fireball-haittaohjelman aiheuttamia ongelmia. Fireballia voi käyttää minkä tahansa muun haitallisen koodin lataamiseen uhrin tietokoneelle. Se löydettiin viime vuoden toukokuussa, ja siitä oli paljon haittaa organisaatioille viime kesänä.

**Haittaohjelmat tammikuussa Top 5, Suomi**

1. Fireball – selainkaappari, jonka kautta voi ladata haittaohjelmia uhrin konelle

2. Coinhive – kryptolouhija, joka louhii Moneroa

3. Roughted – monipuolinen mainosten ja haittaohjelmien levittäjä

4. Rig EK – haittaohjelma, joka valmistelee tietä muille haitakkeille

5. Globeimposter – kiristyshaittaohjelma

**Haittaohjelmat tammikuussa Top 3, koko maailma**

1. Coinhive

2. Fireball

3. Rig EK

**Mobiililaitteiden haittaohjelmat tammikuussa Top 3, koko maailma**

1. Lokibot – Android-laitteiden pankkitroijalainen

2. Triada – Android-laitteiden takaovi

3. Hiddad – Paketoi Android-sovelluksia uudelleen ja julkaisee ne sovelluskaupassa

Kartta kuvaa haittaohjelmatiheyttä eri maiden yritysverkoissa ja näyttää haittaohjelmien hotspotit kautta maailman. vihreä – alhainen riski, punainen – korkea riski, valkoinen – puutteelliset tiedot.



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.

Haittaohjelmien Top 10 -lista kokonaisuudessaan löytyy Check Pointin blogista: <https://blog.checkpoint.com/2018/02/15/januarys-most-wanted-malware-cryptomining-malware-continues-to-cripple-enterprise-cpu-power/>

Lisätietoja Check Pointin uhkientorjuntaresursseista: <http://www.checkpoint.com/threat-prevention-resources/index.html>

Check Pointin uhkakartta näyttää kyberhyökkäykset reaaliaikaisesti: [ThreatCloud World Cyber Threat Map](https://www.threat-cloud.com/ThreatPortal/#/map)

Katso täältä, kun haluat tietää, mitä haittaohjelma tekee: [Check Point ThreatWiki](https://threatwiki.checkpoint.com/threatwiki/public.htm)

**Lisätiedot ja haastattelupyynnöt:**

Maajohtaja Robert Lindqvist, Check Point Software Technologies, robertl@checkpoint.com, p. 050 368 4912

OSG Viestintä, Maija Rauha, maija.rauha@osg.fi, p. 0400 630 065

**Seuraa Check Pointia:**
Twitter: <http://www.twitter.com/checkpointsw>Facebook: <https://www.facebook.com/checkpointsoftware>Blogi: [http://blog.checkpoint.com](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 valtionhallinnon ja yritysten kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat asiakasorganisaatioita kyberhyökkäyksiltä alan parhaalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Point tarjoaa monitasoisen ja kattavan tietoturva-arkkitehtuurin, joka suojaa yritysten pilven, verkon ja mobiililaitteilla olevan informaation, sekä kattavan ja intuitiivisen, yhdestä paikasta johdettavan hallintajärjestelmän. Check Point tarjoaa tietoturvan kaiken kokoisille organisaatioille, joita on sen asiakkaina yhteensä yli 100 000.