**Check Pointin haittaohjelmakatsaus 4/2018**

**Jälleen uusi kryptolouhija nousi haittaohjelmalistalle**

*Tietoturvayhtiö Check Pointin globaali uhkaindeksi kertoo, että hakkerit käyttävät yhä enenevässä määrin kryptolouhintaa, joka voi toimia myös ilman aktiivista verkkoselainkäyttöä. Lähelle listakärkeä on jälleen noussut uusi louhintaohjelma.*

**Espoo — 20. huhtikuuta 2018.** Check Pointin maaliskuun haittaohjelmatilaston mukaan eritoten XMRig-varianttina tunnettu kryptolouhintaohjelma on yleistynyt. Ensimmäistä kertaa toukokuussa 2017 havaittu XMRig nousi maaliskuussa Check Pointin haittaohjelmakatsauksen sijalle 8. Globaalisti havainnoissa nousua oli 70 prosenttia. XMRig, joka toimii itse päätelaitteella ilman verkkoselainta, louhii kryptovaluutta Moneroa.

”Kryptovaluutan louhiminen on ollut kyberrikollisille sangen kannattavaa, ja XMRigin nousu osoittaa heidän panostavan keinojensa muokkaamiseen ja parantamiseen. Paitsi että kryptolouhinta hidastaa PC:itä ja servereitä, nämä haittaohjelmat voivat kerran yrityksen verkkoon päästyään levitä siellä horisontaalisesti. On siksi tärkeää, että yritykset käyttävät monitasoista kyberturvallisuusstrategiaa suojautuakseen niin jo vakiintuneelta haittaohjelmakannalta kuin uusiltakin uhkilta”, sanoo Check Pointin tietoturvatutkijoiden ryhmää vetävä **Maya Horowitz.**

Coinhive säilytti maaliskuussa maailmanlaajuisen johtoasemansa neljättä kuukautta peräkkäin. Se löytyi 18 prosentista mukana olleita organisaatioita, perässään Rig EK Exploit Kit 17 prosentilla ja Cryptoloot-louhija kolmantena 15 prosentilla. XMRig oli kahdeksanneksi yleisin haittaohjelmavariantti ja se iski viiteen prosenttiin organisaatioista.

**Haittaohjelmat maaliskuussa Top 3, maailma:**

 *\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuuhun verrattuna*

**1. ↔ Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.

**2. ↑** **Rig EK** - Iskee Flashin, Javan, Silverlightin ja Internet Explorerin kautta ja valmistelee uhrin konetta myöhempiä hyökkäyksiä varten.

**3. ↑ Cryptoloot** - Kryptolouhija, joka käyttää uhrin prosessoritehoa kryptovaluutan louhimiseen.

**Haittaohjelmat maaliskuussa Top 5, Suomi:**

**1. Rig EK** - Iskee Flashin, Javan, Silverlightin ja Internet Explorerin kautta kautta ja valmistelee uhrin konetta myöhempiä hyökkäyksiä varten.

**2. Cryptoloot** - Kryptovaluuttalouhija, Coinhiven kilpailija.

**3. Coinhive** - Kryptovaluutta Monerolle suunniteltu louhija.

**4. Roughted** - Laajan skaalan haittamainosohjelma, voi tarjota reitin myös kiristysohjelmille.

**5. Fireball** - Selainkaappari.

Yleisin mobiilihaittaohjelma oli Lokibot, Android-laitteiden pankkitroijalainen, joka myöntää rikollisille superkäyttäjäoikeudet haittaohjelmien lataukseen.

**Mobiililaitteiden haittaohjelmat maaliskuussa Top 3, maailma:**

1. **Lokibot** - Android-laitteiden pankkitroijalainen, joka voi myös muuntua kiristysohjelmaksi lukiten puhelimen.
2. **Triada** - Android-laitteiden takaovi, joka myöntää superkäyttäjäoikeudet haittaohjelmien lataamiseen.
3. **Hiddad** - Paketoi Android-sovelluksia uudelleen ja julkaisee ne sovelluskaupassa.

Ensimmäistä kertaa Check Pointin tutkijat analysoivat myös levinneimpiä haavoittuvuuksia. CVE-2017-10271 sijoittui kärkeen 26 prosentin globaalilla vaikutuksella, toisena tuli SQL Injection -haavoittuvuus 19 prosentilla ja kolmanneksi CVE-2015-1635, jota oli hyödynnetty 12 prosentissa organisaatioista globaalisti.

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 lista Top 10 -uhkaohjelmista maaliskuussa löytyy Check Pointin blogista osoitteessa:<http://blog.checkpoint.com/2018/04/16/marchs-wanted-malware-cryptomining-malware-works-even-outside-web-browser-rise/>

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

**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>

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 maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yrityksen verkot, pilvipalvelut kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.