**Check Pointin haittaohjelmakatsaus 6/2018**

**Kryptolouhija Coinhive eteni heittämällä Suomen tilastokärkeen**

*Tietoturvayhtiö Check Pointin haittaohjelmatilasto kertoo, että kryptolouhijoiden toiminnalle ei näy loppua. Coinhive nousi tilastokärkeen niin kansainvälisesti kuin Suomessakin. Suomi kohosi lisäksi 136 maan keskinäisessä vertailussa 72 sijaa.*

**ESPOO — 12. kesäkuuta 2018.** Toukokuu oli jo viides peräkkäinen kuukausi, kun louhintaohjelmat hallitsivat Check Pointin haittaohjelmatilaston kärkeä. Kryptolouhija Coinhive vaikutti maailmanlaajuisesti peräti 22 prosenttiin yritysverkoista. Huhtikuun 16 prosenttiin verrattuna tämä tarkoittaa siis lähes 50 prosentin nousua. Toinen kryptolouhija, Cryptoloot, seurasi perässä 11 prosentin vaikutuksella. Toista kertaa peräkkäin kolmannelta sijalta löytyi mainoshaittaohjelma Roughted, jonka vaikutus ylsi kahdeksaan prosenttiin.

Myös Suomessa haittaohjelmatilaston kärkikolmikko näytti samalta. Coinhive nousi viidenneltä sijalta suoraan tilaston kärkeen. Toista paikkaa piti Roughted, ja kolmanneksi sijoittui Cryptoloot. Mainoshaittaohjelma Roughtedin yleisyys oli Suomessa maailmanlaajuiseen tilastoon verrattuna yli kaksinkertainen (18 %).

Suomi nousi toukokuussa maailmanlaajuisessa uhkaindeksilistauksessa sijalle 53, mikä on 72 enemmän kuin edellisen kuun sija 125. Check Pointin Suomen tietoturva-asiantuntijoiden tiimin vetäjä **Rami Rauanmaa** varoittaa kuitenkin hätäisistä tulkinnoista. ”Suuretkin vaihtelut ovat tavanomaisia listan keskivaiheilla, eivätkä ne tavallisesti kerro merkittävästä trendistä”, hän kommentoi.

”Yleisimpiä haittaohjelmia ovat Suomessa olleet tämän vuoden alkupuolella kryptolouhijat ja mobiililaitteiden haittaohjelmat. Pankkihaittaohjelmat ja kiristyshaittaohjelmat ovat olleet selvästi harvinaisempia. Haittaohjelmien keskinäiset suhteet vastaavat karkeasti kansainvälistä linjaa. Suomessa tavataan hieman vähemmän kiristyshaittaohjelmia ja hieman enemmän pankkitietoihin kohdistuvia hyökkäyksiä kuin kansainvälisesti”, Rauanmaa jatkaa.

**Haittaohjelmat toukokuussa Top 5, Suomi:**

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

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

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

**4. Jsecoin** - verkkosivustolle istutettava kryptolouhija.

**5. Nivdort** - troijalainen, joka leviää sähköpostiliitteiden tai haitallisten verkkosivujen avulla.

**Haittaohjelmat toukokuussa Top 3, maailma:**

*\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna*

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

**2. ↔ Cryptoloot** - Kryptolouhija, joka käyttää uhrin prosessoritehoa kryptovaluutan louhimiseen.

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

**Mobiililaitteiden haittaohjelmat toukokuussa 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. **Lotoor** - Hyväksikäyttää Android-laitteiden haavoittuvuuksia saadakseen pääkäyttäjän oikeudet.

**Tietoturvahyökkäysten riski eri valtioissa toukokuussa, Top 10**

1**. Somalia**

2**. Liechtenstein**

3. **Etiopia**

4. **Oman**

5. **Malediivit**

6**. Myanmar**

7. **Dominikaaninen tasavalta**

8. **Intia**

9. **Mosambik**

10. **Pakistan**

**--**

53. **Suomi**

94. **Viro**

97**. Ruotsi**

136. **Islanti**

Kartta kuvaa haittaohjelmatiheyttä eri maiden yritysverkoissa ja näyttää haittaohjelmien

riskialueet ympäri 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.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista osoitteesta <https://blog.checkpoint.com/2018/06/07/mays-wanted-malware/>

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

**Lisätiedot ja haastattelupyynnöt:**

Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, ramira@checkpoint.com

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.