**Check Pointin haittaohjelmakatsaus 11/2017**

Check Point: Kryptovaluutan salalouhiminen on nouseva tietoturvauhka

*Check Pointin uusimmasta haittaohjelmatilastosta selviää, että kryptovaluutan louhimiseen tarkoitetut haittaohjelmat ovat yleistyneet voimakkaasti. CoinHive oli lokakuussa maailman kuudenneksi käytetyin haittaohjelma, ja Suomessa se oli Top 10 -listan kymmenes.*

**Espoo — 14. marraskuuta 2017.** Tietoturvayhtiö Check Pointin lokakuun haittaohjelmatiedot kertovat, että kryptovaluutan salalouhiminen uhrien koneilla on huolestuttavasti lisääntynyt. Check Pointin tuoreen [raportin](https://blog.checkpoint.com/2017/10/23/crypto-miners-the-silent-cpu-killer-of-2017/) mukaan louhintaohjelma voi viedä jopa 65 % uhrin tietokoneen prosessoritehosta ilman, että tämä on antanut asiaan suostumustaan.

Yleisin louhintahaittaohjelma, CoinHive, lataa laitteelle JavaScriptin, joka sitten käyttää suuren osan sen prosessoritehosta.

RoughTed ja Locky säilyttivät kärkipaikkansa haittaohjelmien Top 3:ssa, mutta kansainvälisen listan kolmoseksi ja Suomen listan neloseksi kiilasi uusi yrittäjä, Seamless, joka on tyypiltään liikenteenohjaaja. Se ohjaa uhrinsa haitalliselle verkkosivulle, minkä seurauksena laitteelle latautuu toinen, EK-tyyppinen haittaohjelma. EK:t eli Exploit Kitit valmistelevat uhrin koneen lisälatauksille.

”Kryptovaluutan louhijat ovat uusi, hiljainen uhka. Kyberrikolliset jauhavat niiden avulla tuloja samalla, kun uhrien päätelaitteiden ja verkkojen suorituskyky laskee. Monitasoinen, ennakoivan uhkientorjunnan sisältävä tietoturvaratkaisu on välttämätön, jotta CoinHiven ja Seamlessin kaltaiset uudet haittaohjelmat eivät pääse tuottamaan yllättäviä vahinkoja yritysverkoissa”, kommentoi Check Pointin Suomen maajohtaja **Robert Lindqvist**.

**Haittaohjelmat syyskuussa Top 10, Suomi**

1. Roughted – mainosten ja haittaohjelmien levittäjä

2. Locky – kiristyshaittaohjelma

3. Jaff – kiristyshaittaohjelma

4. Seamless – liikenteenohjaaja (TDS), joka ohjaa verkkoliikennettä haitallisille sivuille

5. Zeus – troijalainen

6. Pushdo – troijalainen

7. Fireball – selainkaappari

8. Emotet – troijalainen

9. Triada – Android-laitteiden takaovi

10. Coin Hive – Louhii Monero-kryptovaluuttaa ja heikentää tietokoneen suorituskykyä

**Haittaohjelmat elokuussa Top 3, koko maailma**

1. RoughTed –mainosten ja haittaohjelmien levittäjä

2. Locky – kiristyshaittaohjelma

3. Seamless – liikenteenohjaaja

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

1. Triada – Android-laitteiden takaovi

2. LeakerLocker – Android-laitteiden kiristyshaittaohjelma, joka uhkaa julkaista käyttäjän tietoja, ellei lunnaita makseta.

3. Lotoor – Android-laitteiden hakkerityökalu, hyödyntää haavoittuvuuksia

Check Point uskoo monikerroksisen tietoturvan voimaan haittaohjelmien torjunnassa. Tehokkaat tietoturvaohjelmistot pitävät yritysverkot puhtaina tarkkailemalla tietynlaista käyttäytymistä ja ominaisuuksia, jolloin ne saavat kiinni sekä uudet että ennestään tutut tunkeutujat. Tällaisia ratkaisuja ovat Check Pointin SandBlast™ Zero-Day Protection ja Mobile Threat Prevention.

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: http://blog.checkpoint.com/2017/11/13/[octobers-wanted-malware-cryptocurrency-mining-presents-new-threat/](http://wcms.us.checkpoint.com/?p=159698&preview=true)

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.