**Check Pointin haittaohjelmakatsaus 10/2017**

Tarkkana sähköpostin kanssa: huijausviestejä oli syyskuussa liikkeellä poikkeuksellisen paljon

*Sähköpostin kautta leviävä kiristyshaittaohjelma Locky oli Suomen yritysverkoissa yleisin ja globaalisti toiseksi yleisin haittaohjelma syyskuussa. Edellinen Locky-aalto koettiin viime vuonna.*

**Espoo — 12. lokakuuta 2017.** Locky poistui tietoturvayhtiö Check Pointin ylläpitämältä haittaohjelmien Top 10 -listalta viime vuoden lokakuussa, mutta yleistyi viime kuussa jälleen niin nopeasti, että se saatiin kiinni joka kymmenennestä (11,5 %) yritysverkosta globaalisti. Lockyä levitti Necurs-bottiverkko, joka löytyy itse Top 10 -listan sijalta 10.

Locky alkoi levitä vuoden 2016 helmikuussa, jolloin se nousi nopeasti maailman yleisimpien haittaohjelmien joukkoon. Se leviää pääasiassa sähköposteissa, joissa on liitteenä Word-tekstitiedostoksi tai pakatuksi Zip-tiedostoksi naamioituja komentokoodeja. Viestissä kehotetaan klikkaamaan liitettä, jolloin kiristyshaittaohjelma latautuu tietokoneelle ja salaa sen sisältämät tiedostot. Tämän jälkeen näytölle tuleva viesti neuvoo uhria lataamaan koneelleen Tor-verkon ja käymään sen avulla nettisivulla, jossa esitetään lunnasvaatimus. Lunnaat pyydetään bitcoineina. Kesäkuussa 2016 Lockystä lähti liikkeelle päivitetty versio, joka sisältää paljastumisen estäviä ominaisuuksia.

”Lockyn uusi tuleminen osoittaa, että vanhat haittaohjelmat voivat olla aivan yhtä vaarallisia kuin uudet. Kyberrikolliset pyrkivät koko ajan muuntamaan tuttuja haittaohjelmia tunnistamattomiksi, ja isot bottiverkot voivat antaa potkua niiden globaalille levitykselle. Sähköpostien kanssa on syytä olla koko ajan tarkkana. Tarvitaan vain yksi varomaton klikkaus, ja koko yritysverkon tietoturva vaarantuu”, kommentoi Check Pointin Suomen maajohtaja **Robert Lindqvist**.

**Haittaohjelmat syyskuussa Top 10, Suomi**

1. Locky – kiristyshaittaohjelma

2. Roughted – mainosten ja haittaohjelmien levittäjä

3. Rig EK – hyökkäysten valmistelija

4. Jaff – kiristyshaittaohjelma

5. Globeimposter – kiristyshaittaohjelma

6. Zeus – troijalainen

7. Fireball – selainkaappari

8. Pushdo – troijalainen

9. Emotet –troijalainen

10. Dyre – pankkitroijalainen

**Haittaohjelmat elokuussa Top 3, koko maailma**

1. RoughTed –mainosten ja haittaohjelmien levittäjä

2. Locky – kiristyshaittaohjelma

3. Globeimposter – kiristyshaittaohjelma

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

1. Triada – Android-laitteiden takaovi

2. Hiddad – mainosten levittäjä ja tietovaras Android-laitteissa

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: [//dm-research.us.checkpoint.com/augusts-most-wanted-malware-banking-trojans-and-ransomware-that-want-your-money/](http://dm-research.us.checkpoint.com/?p=17702&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.