Tästä syystä kyberrikolliset suosivat kiristysohjelmia

*Kiristyshaittaohjelmat ovat juuri nyt yleisimpiä tietoturvan uhkia niin Suomessa kuin kansainvälisestikin. Check Pointin tietoturvaseminaarissa Helsingissä selvisi, minkä takia: 70 prosenttia uhreista maksaa lunnaat, vaikka niin ei virallisten ohjeiden mukaan pitäisi missään tapauksessa tehdä.*

**Espoo — 30. lokakuuta 2017.** Jos tietoturva-asiantuntija **Magnus Sköld** Check Pointin Euroopan organisaatiosta olisi kyberrikollinen, myös hän valitsisi työkalukseen kiristyshaittaohjelmat. Ne ovat konnien kannalta monin tavoin käytännöllisempiä kuin muut haittaohjelmatyypit.

”Madoilla, pankkitroijalaisilla, näppäintoimintojen tallentajilla ja bottiverkoilla saa saaliiksi vain dataa, jonka myyminen on vaivalloista ja kallista. On huomattavasti helpompaa ja tuottoisampaa myydä data takaisin sen omistajalle. Usein uhri on erittäin motivoitunut saamaan tietonsa takaisin”, Sköld kertoo.

Vuosi 2016 oli kiristäjille erityisen hyvä. Sköldin mukaan kyberrikolliset onnistuivat syöttämään kiristyshaittaohjelman 40 prosenttiin yritysverkoista, ja 70 prosenttia kiristyksen kohteeksi joutuneista maksoi lunnaat. Yli puolet Yhdysvalloissa kiristetyistä maksoi yli 10 000 dollaria ja joka viides yli 40 000 dollaria saadakseen tietonsa takaisin. Niin FBI kuin Suomen Viestintävirastokin ohjeistavat, ettei kiristäjille pidä missään tapauksessa maksaa.

Tänä vuonna kiristäjien tahti ei ole ainakaan hiljentynyt. WannaCry aiheutti ongelmia muun muassa Iso-Britannian terveydenhuollossa. NotPetya tuli kalliiksi esimerkiksi konttialuksistaan tunnetulle logistiikkayhtiö Maerskille. Uusimpana on liikkeellä BadRabbit, joka levisi etenkin Itä-Euroopassa ennen viime viikolla raportoitua pysähtymistään.

Check Pointin laskujen mukaan kiristysohjelmien osuus suomalaisissa yritysverkoissa tavatuista haittaohjelmista oli tämän vuoden alkupuoliskolla 48 prosenttia. Mobiilihaittaohjelmien osuus oli 26 prosenttia, sama kuin pankkitroijalaisten. Koko EMEAssa vastaavat luvut olivat 56, 16 ja 28 prosenttia.

**Harva ilmoittaa poliisille**

”Kiristysohjelmien suosio rikollisten keskuudessa johtuu myös heidän kannaltaan turvallisen maksutavan kehittymisestä. Bitcoin-maksujen vastaanottajaa ei pystytä jäljittämään. Maksaminen onnistuu helposti verkossa, eikä myöskään uhrin tarvitse kertoa siitä kenellekään. Harva ilmoittaa poliisille, koska asialle ei haluta julkisuutta”, Sköld sanoi.

Uusia kiristyshaittaohjelmia lähtee liikkeelle Check Pointin tietojen mukaan päivittäin. Kehittyneimmät uudet kiristyshaittaohjelmat osaavat salata uhrin tietokoneen sisällön lisäksi myös hänen pilvipalveluissa sijaitsevat varmuuskopionsa.

Turvassa eivät ole edes IoT-kodinkoneet. Niillä ei toki säilytetä dataa, mutta kiristyshaittaohjelma voi jumittaa laitteen. Kamera tai termostaatti käynnistyy jälleen, kun uhri on maksanut lunnaat. Sköld kertoo, että valvontakamera on kätevä kiristykseen toisellakin tapaa: kameran hallinnan hankkinut rikollinen voi kuvata, mitä uhrin tiloissa tapahtuu ja uhata julkistaa nauhan, ellei lunnaita makseta.

**Ehkäise kiristys näin**

Mitä sitten on tehtävissä? Magnus Sköldin mukaan paljonkin:

”Esimerkiksi WannaCry iski vain laitteisiin, joiden ohjelmisto oli vanhentunut. Ohjelmistojen pitäminen aina ajan tasalla on perusasia. Yritysten tulee myös jatkuvasti kouluttaa henkilöstöään, jotta nämä osaavat varoa epäilyttäviä linkkejä. Kaikkea ei ole pakko klikata”, hän sanoo.

”Varmuuskopioiden tekeminen on yleinen neuvo, mutta sen toteuttaminen tarpeeksi kattavasti on vaikeaa. Harva varmuuskopioi tarpeeksi usein – kerran päivässä ei yleensä riitä. Paras keino on ehkäistä hyökkäykset ennalta. Yritysten käyttöön on markkinoilla tehokkaita menetelmiä, kuten Check Pointin Anti-Ransomware-teknologia”, Sköld toteaa.

Check Pontin Anti-Ransomware-ratkaisu pystyy palauttamaan tiedot, vaikka ne olisi jo salattu. Se havaitsee ja pysäyttää uudet ja ennestään tunnetut hyökkääjät 99,3 prosentin varmuudella. Esimerkiksi WannaCry ja NotPetya jäivät kiinni tämän ohjelmiston suojaamissa organisaatioissa tuoreeltaan ennen kuin ne pääsivät aiheuttamaan tuhoa.

--

Tiedot haittaohjelmien yleisyydestä perustuvat Check Pointin vuoden 2017 ensimmäistä vuosipuoliskoa koskeavaan raporttiin: [Cyber Attack Trends Report](https://www.checkpoint.com/downloads/resources/2017-cyber-attack-trends.pdf). Sen tiedot perustuvat ThreatCloudinTM keräämään dataan. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä yli 250 miljoonasta verkko-osoitteesta. Check Pointin uhkakartta näyttää kyberhyökkäykset reaaliaikaisesti: [ThreatCloud World Cyber Threat Map](https://www.threat-cloud.com/ThreatPortal/#/map)

Tieto lunnaat maksaneiden osuudesta perustuu IBM:n teettämään tutkimukseen:

<https://www-03.ibm.com/press/us/en/pressrelease/51230.wss>

**Lisätietoja ja raportteja kiristyshaittaohjelmista ja niiltä suojautumisesta Check Pointin verkkosivuilta:**

<http://pages.checkpoint.com/anti-ransomware.html>

**Lisätietoja myös:**

Maajohtaja **Robert Lindqvist**, Check Point Software Technologies, [robertl@checkpoint.com](mailto:robertl@checkpoint.com), p. 050 368 4912

OSG Viestintä, **Maija Rauha**, [maija.rauha@osg.fi](mailto: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.