**Check Pointin haittaohjelmakatsaus 11/2018**

**Etäohjattava troijalainen nousi ensi kertaa haittaohjelmien Top 10 -listalle**

*Tietoturvayhtiö Check Pointin haittaohjelmaseuranta havaitsi lokakuussa laajan kampanjan, joka levitti etäohjattavaa RAT-haittaohjelmaa. Listan kärkisijoja pitivät kuitenkin edelleen kryptovaluutan louhijat.*

**ESPOO — 15. marraskuuta 2018.** Etäohjattava troijalainen eli RAT (Remote Access Trojan) nousi lokakuussa ensi kertaa tietoturvayhtiö Check Point Software Technologiesin globaalille haittaohjelmien Top 10 -listalle. FlawedAmmyy-nimisen haittaohjelman avulla hyökkääjä saa halutessaan täyteen hallintaansa kohdelaitteen ja sen sisältämät tiedostot. Hän voi hallita laitteen kameraa ja mikrofonia, ottaa ruutukaappauksia, napata tunnistetietoja, varastaa tiedostoja ja tarkkailla uhrin toimintaa.

FlawedAmmyy on lokakuun globaalilla listalla sijalla 10. Suomen kymmenen yleisimmän haittaohjelman listalla se ei ole.

Check Pointin tietoturvatutkijoiden ryhmää vetävä Threat Intelligence Group Manager **Maya Horowitz** kertoo, että FlawedAmmyyn yleistyminen on jatkunut jo useita kuukausia. Lokakuun kampanja oli kuitenkin laajin tähän asti. ”Tämä osoittaa, että salasanojen, salassapidettävien tiedostojen sekä pankkiyhteyksiä ja maksamista koskevien tietojen tapainen data ei ole menettänyt houkuttelevuuttaan kyberrikollisten silmissä. Näin siitä huolimatta, että kryptolouhijat jatkavat käytetyimpinä haittaohjelmina”, Horowitz tulkitsee.

Kryptolouhijat pitävät edelleen haittaohjelmatilaston kärkisijoja niin Suomessa kuin globaalistikin. Lokakuun levinnein haittaohjelma oli Coinhive, joka löytyi 18 prosentista Check Pointin globaaliin verkostoon kuuluvista yritysverkoista. Cryptolootin esiintyvyys oli 8 prosenttia. Suomessa Coinhive oli suhteellisesti vielä hieman yleisempi 23 prosentin esiintyvyydellä, ja Cryptoloot löytyi 11 prosentista suomalaisia yritysverkkoja.

**Suomen yleisimmät haittaohjelmat lokakuussa Top 5:**

1. **Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla. Esiintyvyys 23 % organisaatioista.
2. **Roughted** – Laajan skaalan haittamainosohjelma, voi tarjota reitin myös kiristysohjelmille. Esiintyvyys 13 %.
3. **Cryptoloot.** Coinhiven kilpailija kryptolouhinnassa. Esiintyvyys 12 %.
4. **Cridex** – Windows-mato, joka yrittää anastaa esimerkiksi luottokorttitietoja. Leviää internet-jakojen ja ulkoisten muistien avulla. Esiintyvyys 9 %.
5. **Dorkbot** – Pankkitroijalainen, joka urkkii uhrin tietoja ja jota käytetään usein myös palvelunestohyökkäysten toteuttamiseen. Esiintyvyys 8 %.

**Maailman yleisimmät haittaohjelmat lokakuussa Top 3:**

*\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna*

1. **↔ Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. **↑ Cryptoloot** – Coinhiven kilpailija kryptolouhinnassa**.**
3. **↔** **Dorkbot** – IRC-pohjainen mato, joka sallii koodin lataamisen ja suorittamisen tartunnan saaneelle laitteelle etänä ja toimii usein muiden haittaohjelmien levitystapana.

**Maailman yleisimmät mobiililaitteiden haittaohjelmat lokakuussa Top 3:**

1. **Triada** – Android-laitteiden takaovi, joka myöntää pääkäyttäjäoikeudet haittaohjelmien lataamiseen. Sen on havaittu myös urkkivan, millä verkkosivuilla uhri käy.
2. **Lokibot** – Android-laitteiden pankkitroijalainen, joka voi myös muuntua kiristysohjelmaksi lukiten puhelimen.
3. **Hiddad** – Android-laitteiden haittaohjelma, joka kaappaa sovelluksia, paketoi niiden mukaan mainoksia levittävää koodia ja panee ne uudelleen tarjolle sovelluskauppaan. Se pääsee myös käsiksi laitteen tietoturvaominaisuuksiin, mitä kautta hyökkääjä voi saada haltuunsa arkaluontoista tietoa.

**Maailman hyödynnetyimmät haavoittuvuudet syyskuussa Top 3:**

1. ↔ Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow (CVE-2017-7269). Esiintyvyys 48 % organisaatioista.
2. ↑ OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)Esiintyvyys 46 %.
3. ↑ Web servers PHPMyAdmin Misconfiguration Code Injection. Esiintyvyys 42%.

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/2018/11/13/october-2018s-most-wanted-malware-for-the-first-time-remote-access-trojan-reaches-top-threats-cryptomining/>

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 johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden kohdistettujen hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri käsittää uuden 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen kaikkia verkko-, pilvi- ja mobiilitoimintoja kaikilta tunnetuilta hyökkäyksiltä, ja sitä hallitaan alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän kautta. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.