**Check Pointin haittaohjelmakatsaus 9/2018**

**Pankkitroijalaiset liikkuivat vilkkaasti loppukesän lämmössä**

*Tietoturvayhtiö Check Pointin uusin haittaohjelmatilasto kertoo, että laajamittainen Ramnit-matojen hyökkäysaalto nosti pankkitroijalaisten esiintyvyyden tavallista korkeammaksi elokuussa.*

**ESPOO — 13. elokuuta 2018.** Check Pointin laskujen mukaan Ramnit-pankkitroijalaisia oli liikkeellä yritysverkoissa selvästi tavallista enemmän elokuussa. Ramnit-hyökkäysten määrä kaksinkertaistui loppukesän aikana kevään lukemista. Suuri osa Ramnit-liikenteestä liittyi kampanjaan, joka pyrki ottamaan uhrien tietokoneita kyberrikollisten käyttöön välityspalvelimiksi. Check Point on kertonut kampanjasta tarkemmin [tutkimusblogissaan.](https://research.checkpoint.com/ramnits-network-proxy-servers/)

Ramnit nousi elokuussa globaalin haittaohjelmatilaston sijalle 6, mutta myös muita pankkitroijalaisia havaittiin tavallista enemmän. Niitä oli kaikkiaan liikkeellä elokuussa yli kaksinkertainen määrä kesäkuuhun verrattuna. Check Pointin tietoturvatutkijoiden tiimin vetäjä **Maya Horowitz** kertoo, että tämä oli jo toinen peräkkäinen kesä, jolloin kyberrikolliset hyödynsivät helpon rahan toivossa nimenomaan pankkitroijalaisia.

”Tällaisia trendejä ei kannata vähätellä, koska kyberrikolliset tietävät, mitä tekevät. He pyrkivät valitsemaan hyökkäyskeinot, jotka tuottavat todennäköisimmin tulosta kunakin ajankohtana. Nähtävästi verkossa liikkuvien selainkäytös on kesäkuukausina sellaista, että se tekee heistä alttiita pankkitroijalaisille”, Horowitz jatkaa.

Horowitzin mukaan pankkitroijalaisten ja muidenkin ei-toivottujen vieraiden pääsy yritysverkkoihin on mahdollista estää monikerroksisella kyberturvallisuusstrategialla, joka suojaa sekä tunnetuilta haittaohjelmaperheiltä että täysin uusilta uhilta.

Globaalin haittaohjelmatilaston ykkösenä jatkoi elokuussa kryptovaluutan louhija Coinhive, joka oli läsnä 17 prosentissa yritysverkoista. Suomessa Coinhive oli niin ikään listaykkönen 16 prosentin levinneisyydellä. Dorkbotin ja Andormedan globaali levinneisyys oli kummankin kuusi prosenttia. Suomessa sijoilla kaksi ja kolme olivat Roughted 12 prosentin ja Sality 11 prosentin levinneisyydellä.

**Suomen yleisimmät haittaohjelmat elokuussa Top 5:**

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. **Sality** – Leviää tartunnan saaneiden tiedostojen, ulkoisten muistien ja verkkojakojen kautta ja käytetään yleensä roskapostituksiin.
4. **Cridex** – Windows-mato, joka yrittää anastaa esimerkiksi luottokorttitietoja. Leviää internet-jakojen ja ulkoisten muistien avulla.
5. **Ramnit** – FTP-palvelimia hyödyntävä mato, joka valmistaa itsestään kopion ja levittää sen eteenpäin. Voi toimia myös takaovena.

**Maailman yleisimmät haittaohjelmat elokuussa Top 3:**

*\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna*

1. **↔ Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. **↑** **Dorkbot** – Pankkitroijalainen, joka urkkii uhrin tietoja ja jota käytetään usein myös palvelunestohyökkäysten toteuttamiseen.
3. **↑ Andromeda** – Haittaohjelma, jota käytetään pääasiassa takaovena muiden haittaohjelmien välittämiseksi laitteille, mutta sen avulla on mahdollista myös koota bottiverkkoja**.**

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

1. **Lokibot** – Android-laitteiden pankkitroijalainen, joka voi myös muuntua kiristysohjelmaksi lukiten puhelimen.
2. **Lotoor** – Hakkerityökalu, joka hyödyntää Android-käyttöjärjestelmän haavoittuvuuksia saadakseen itselleen pääkäyttäjän oikeudet.
3. **Triada** – Android-laitteiden takaovi, joka myöntää pääkäyttäjäoikeudet haittaohjelmien lataamiseen. Sen on havaittu myös urkkivan, millä verkkosivuilla uhri käy.

**Maailman hyödynnetyimmät haavoittuvuudet elokuussa Top 3:**

1. ↔ Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow (CVE-2017-7269).
2. ↑ OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346).
3. ↑ D-link DSL-2750B Remote Command Execution.

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/2018/09/11/augusts-most-wanted-malware-banking-trojan-attacks-turn-up-the-heat/>

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.