**Check Pointin haittaohjelmakatsaus 5/2018**

**Kryptolouhijat hyödyntävät nyt päivittämättömiä palvelimia**

*Tietoturvayhtiö Check Point muistuttaa, että myös palvelimet kannattaa päivittää. Hakkerit käyttävät nyt hyväkseen paikkaamattomia palvelinten tietoturva-aukkoja louhiakseen kryptovaluuttaa.*

**ESPOO — 15. toukokuuta 2018.** Huhtikuussa louhintaohjelmat hallitsivat Check Pointin haittaohjelmatilaston kärkeä jo neljättä kertaa peräkkäin. Yritysverkoista 16 prosentista löytyi Coinhive-tartunta, joten se säilytti maailmanlaajuisen johtoasemansa. Toinen kryptolouhija, Cryptoloot, seurasi täpärästi perässä 14 prosentilla, kun Roughted-mainoshaittaohjelma ylsi kolmannelle sijalle 11 prosentilla.

Suomessa viiden yleisimmän haittaohjelman joukossa oli kolme kryptolouhijaa, yleisimpänä Cryptoloot. Sen yleisyys oli lähes 23 prosenttia. Suomessa Coinhive oli sijalla viisi 11 prosentin vaikuttavuudella.

Check Pointin tietoturvatutkijat havaitsivat jo alkuvuonna, että kyberrikolliset hyödyntävät Microsoft Windows Server 2003 -palvelimen ja Oracle Web Logic -palvelimen paikkaamattomia haavoittuvuuksia kryptovaluutan salalouhintaan. Huhtikuussa tämä toiminta yleistyi merkittävästi. Kaikkiaan 46 prosentissa organisaatioista havaittiin louhintaan liittyvä hyökkäys, jonka kohteena oli Microsoft Windows Server 2003 -haavoittuvuus, ja Oracle Web Logicia pyrittiin hyödyntämään louhintaan 40 prosentissa yrityksistä.

”Salalouhinnan yleistyessä kyberrikolliset kehittävät jatkuvasti uusia ansaintamuotoja. Päivittämättömiin palvelimiin kohdistuvat hyökkäykset ovat tärkeä muistutus yrityksille. Tietoverkkojen suojaamisessa ei pidä unohtaa perusasioita, kuten ohjelmistojen paikkausta ja päivityksiä”, kiteyttää Check Pointin tietoturvatutkijoiden ryhmää vetävä **Maya Horowitz**.

Viimeisin päivitys kumpaankin palvelimeen on ollut saatavilla jo puolen vuoden ajan. Horowitzin mielestä on huolestuttavaa, että siitä huolimatta niinkin moneen serveriin pystyttiin tunkeutumaan. ”On tärkeää, että yritykset käyttävät monitasoista kyberturvallisuusstrategiaa suojautuakseen niin vakiintuneelta haittaohjelmakannalta kuin uusiltakin uhkilta”, täydentää Horowitz.

**Haittaohjelmat huhtikuussa Top 3, maailma:**

*\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna*

**1. ↔ Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.

**2. ↑ Cryptoloot** - Kryptolouhija, joka käyttää uhrin prosessoritehoa kryptovaluutan louhimiseen.

**3. ↑** **Roughted** - Laajan skaalan haittamainosohjelma, voi tarjota reitin myös kiristysohjelmille.

**Haittaohjelmat huhtikuussa Top 5, Suomi:**

**1. Cryptoloot** - Kryptovaluuttalouhija, Coinhiven kilpailija.

**2. Roughted** - Laajan skaalan haittamainosohjelma, voi tarjota reitin myös kiristysohjelmille.

**3. Fireball** - Selainkaappari.

**4. Jsecoin** - verkkosivustolle istutettava kryptolouhija.

**5. Coinhive** - Kryptovaluutta Monerolle suunniteltu louhija.

Yleisimpänä mobiilihaittaohjelmana jatkoi maaliskuun tapaan Lokibot, Android-laitteiden pankkitroijalainen, joka myöntää rikollisille superkäyttäjäoikeudet haittaohjelmien lataukseen. Seuraavana listalla jatkoivat niin ikään Triada ja Hiddad.

**Mobiililaitteiden haittaohjelmat huhtikuussa Top 3, maailma:**

1. **Lokibot** - Android-laitteiden pankkitroijalainen, joka voi myös muuntua kiristysohjelmaksi lukiten puhelimen.
2. **Triada** - Android-laitteiden takaovi, joka myöntää superkäyttäjäoikeudet haittaohjelmien lataamiseen.
3. **Hiddad** - Paketoi Android-sovelluksia uudelleen ja julkaisee ne sovelluskaupassa.

Check Pointin tutkijat analysoivat myös levinneimpiä haavoittuvuuksia. Ensimmäiselle sijalle tuli CVE-2017-7269 46 prosentin globaalilla vaikutuksella ja toiseksi ylsi CVE-2017-10271, jota oli hyödynnetty 40 prosentissa organisaatioista maailmanlaajuisesti. Kolmantena listalla oli SQL Injection -haavoittuvuus 16 prosentilla.

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/2018/05/14/aprils-wanted-malware-cryptomining-malware-targeting-unpatched-server-vulnerabilities/>

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](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>

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 maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yrityksen verkot, pilvipalvelut kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.