**Kryptolouhijat ahkeroivat viime vuonna 37 prosentissa yrityksistä, kertoo Check Pointin uusi tietoturvaraportti**

*Kryptolouhijan hyökkäyksen kohteena on edelleen 20 prosenttia yrityksistä joka viikko. Kolmasosassa yrityksistä saatiin viime vuonna kiinni jokin mobiilihaittaohjelma, mutta kiristyshaittaohjelma löytyi vain 4 prosentista.*

**ESPOO — 28. tammikuuta 2019** – Tietoturvayhtiö Check Point® Software Technologies on julkistanut ennakkotietoja uusimmasta tietoturvaraportistaan. Check Point Security Report 2019 valaisee menetelmiä, joita kyberrikolliset viime vuonna yleisimmin käyttivät ja antaa yritysten tietoturvasta vastaaville viitteitä siitä, millaisilta uhilta tänä vuonna pitää suojautua.

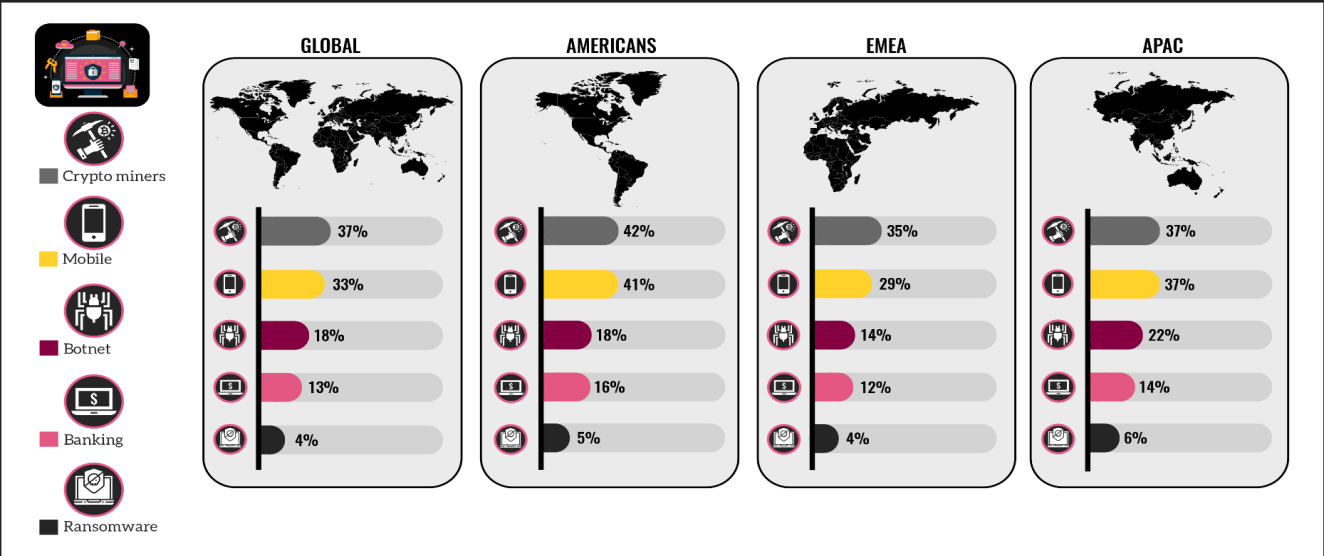
Viime vuoden havainnosta nousevat tärkeimmät kyberhyökkäystrendit ovat:

* **Kryptolouhijat hallitsevat haittaohjelmakenttää:** Neljä globaalisti runsaimmin liikkeellä ollutta haittaohjelmaa olivat kaikki kryptolouhijoita, joiden esiintyvyys organisaatioissa oli yhteensä 37 prosenttia vuonna 2018. Vaikka kaikkien kryptovaluuttojen arvo on laskenut, 20 prosenttia yrityksistä joutuu edelleen louhijahyökkäyksen kohteeksi joka viikko. Louhintaohjelmat ovat viime aikoina myös kehittyneet. Osa ohjelmista osaa hyödyntää ohjelmistojen haavoittuvuuksia ja välttää joutumista tietoturvaratkaisun hiekkalaatikkoon.
* **Mobiililaitteet ovat liikkuva maali:** 33 prosenttia organisaatioista koki vuoden aikana yhden tai useampia mobiilihaittaohjelmien hyökkäyksiä. Viime vuoden kolme yleisintä mobiililaitteiden haittaohjelmaa oli suunnattu Android-laitteille. Mobiilihaittaohjelma oli muutamissa esiin tulleissa tapauksissa asennettu laitteelle jo ennen sen käyttöönottoa, ja sovelluskaupoista löytyi sovellukseksi naamioituja haittaohjelmia.
* **Bottiverkot käynnistävät monenlaisia hyökkäyksiä:** Botit olivat kolmanneksi yleisin haittaohjelmatyyppi, jonka esiintyvyys oli 18 prosenttia organisaatioista. Botteja käytetään käynnistämään palvelunestohyökkäyksiä ja levittämään muita haittaohjelmia. Bottitartunta löytyi vuonna 2018 melkein joka toisesta (49 %) organisaatiosta, joka koki palvelunestohyökkäyksen.

* **Kiristyshaittaohjelmia on liikkeellä entistä vähemmän:** Kiristyshaittaohjelmien käyttö väheni viime vuonna radikaalisti. Niiden esiintyvyys oli vain 4 prosenttia organisaatioista globaalisti.

”Kyberhyökkäyksistä ei ollut viime vuonna mitään pulaa. Siitä pitivät huolen kryptolouhinnan räjähdysmäinen yleistyminen sekä massiiviset tietovuodot ja palvelunestohyökkäykset. Kyberrikollisilla on käytössään laaja valikoima keinoja, jotka ovat kehittyneet entistäkin salavihkaisemmiksi ja vaikeammiksi havaita”, kommentoi Check Pointin Chief Marketing Officer **Peter Alexander**.

”Useita eri keinoja käyttävät, nopeasti liikkuvat ja laajat viidennen sukupolven (Gen V) hyökkäykset yleistyvät koko ajan. Organisaatioiden pitää ottaa käyttöön monikerroksinen kyberturvallisuusstrategia, joka estää hyökkääjiä pääsemästä käsiksi niiden verkkoihin ja dataan. Uusi tietoturvaraporttimme tarjoaa myös tietoa ja suosituksia hyökkäysten ehkäisemisen keinoista”, Alexander jatkoi.



*Kyberhyökkäykset tyypeittäin globaalisti ja alueittain.*

Suomi ei esiinny Check Pointin raportissa erityisenä lintukotona. Maailman ja Euroopan yleisimmät haittaohjelmat olivat yleisimpiä myös Suomessa, ja niiden keskinäiset voimasuhteet olivat lähes samat kuin muualla. Niiden esiintyvyys oli kuitenkin Suomessa hieman korkeampi kuin Euroopassa keskimäärin.

Coinhiven esiintyvyys oli Suomessa 31 ja EMEAssa 23 %, Cryptolootin 25/14 %, Jsecoinin 16/12 %, Nivdortin 15/6 %, Necursin 13/7 %, Ramnitin 12/6 %, Fireballin 10/5 %, Dorkbotin 10/5 %, XMRigin 9/6 % ja Authedminen 9/4 %.

Miksi tietyt haittaohjelmat olivat Suomessa yleisempiä kuin muualla? Tietoturva-asiantuntija **Rami Rauanmaa** Check Pointin Suomen toimistolta vastaa, että täsmällistä syytä on vaikea sanoa. ”Haittaohjelmatilanne vaihtelee kuukaudesta toiseen. Yleensä ottaen Suomessa tavataan vähemmän bottiverkkoja kuin muualla maailmassa, kun taas kryptolouhijoita on meillä liikkeellä enemmän kuin muualla”, Rauanmaa sanoo.

Check Pointin Security Report 2019 perustuu Check Pointin globaalin ThreatCloud-verkoston ajantasaisesti keräämiin hyökkäystietoihin, Check Pointin viime vuoden aikana tekemiin tutkimuksiin sekä kyselyyn, jonka Check Point teetti IT-ammattilaisten ja yritysjohtajien parissa. Raportti kertoo, millaisia ovat uusimmat uhat eri toimialoilla ja käy perusteellisesti läpi haittaohjelmien, tietovuotojen ja valtiollisten kyberhyökkäysten trendit. Check Pointin omat ajatusjohtajat analysoivat raportissa tämän hetken ja huomisen monitahoista uhkamaisemaa, jotta se tulisi ymmärretyksi yrityksissä ja organisaatioissa.

Täydellinen raportti: <https://pages.checkpoint.com/cyber-security-report-2019-trends.html>

Liitteenä olevassa taulukossa ovat tiedot yleisimpien haittaohjelmien esiintyvyydestä Suomessa, Ruotsissa, Venäjällä ja EMEA-alueella.

**Lisätiedot ja haastattelupyynnöt:**

OSG Viestintä, Maija Rauha, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065

Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, [ramira@checkpoint.com](mailto:ramira@checkpoint.com)

**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 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.