**Kryptolouhijoiden esiintyvyys yrityksissä oli kymmenkertainen kiristyshaittaohjelmiin verrattuna, mutta vain yksi viidestä ammattilaisesta havaitsi tartunnan, kertoo Check Pointin Security Report 2019**

*Tietoturvaraportin nyt julkaistu toinen luku tuo esiin kyberrikollisuuden demokratisoitumisen, kun kuka tahansa voi ostaa haittaohjelmia palveluna.*

**ESPOO – 7. helmikuuta 2019 –** Maailman johtava tietoturvaratkaisujen toimittaja Check Point on julkaissut toisen osan vuoden 2019 tietoturvaraportistaan. Sen mukaan kyberrikollisuus on demokratisoitunut, kun haittaohjelmien myymisestä palveluna (malware as a service) on tullut ansaintamuoto, ja kehittyneitä hyökkäysmenetelmiä on tarjolla kaikille, jotka ovat halukkaita maksamaan niistä.

Raportti paljastaa myös Check Pointin tietoturvatutkijoiden vuoden 2108 aikana havaitsemat keskeiset kyberhyökkäysten trendit. Kasvusuunnassa olivat etenkin useita erilaisia tekniikoita hyödyntävät hyökkäykset, jotka pyrkivät välttämään yritysten tietoturvatutkat. Raportissa kerrotaan myös, minkä tyyppisiä hyökkäyksiä yritysten IT- ja tietoturvatiimit pitivät isoimpina uhkina organisaatioilleen. Raportin kohokohtia:

* **Kryptolouhijat jäävät usein huomaamatta:** kryptolouhintaohjelmat tartuttivat vuonna 2018 kymmenkertaisen määrän organisaatioita kiristyshaittaohjelmiin verrattuna, mutta vain yksi viidestä IT-ammattilaisesta oli tietoinen siitä, että oman organisaation tietoverkko oli saanut tartunnan. Kryptolouhijoiden globaali esiintyvyys oli 37 % organisaatioista vuonna 2018, ja 20 % yrityksistä kokee edelleen louhijahyökkäyksen joka viikko, vaikka kryptovaluuttojen arvo on laskenut 80 %.
* **Kryptolouhijoiden riski aliarvioidaan organisaatioissa:** Kun yritysten IT- ja tietoturvavastaavilta kysyttiin, mitkä olivat tärkeimpiä tietoturvan uhkia heidän organisaatiossaan, vain 16 % mainitsi kryptolouhijat. Palvelunestohyökkäykset (34 %), tietovuodot (53%), kiristysohjelmat (54 %) ja kalastelu (66 %) mainittiin useammin. Tämä on huolestuttavaa, koska kryptolouhijat voivat toimia muiden haittaohjelmien kulkua helpottavina takaovina.
* **Haittaohjelmia voi ostaa palveluna:** Amatööritkin pystyvät nykyään käärimään rahaa kiristyshaittaohjelmien avulla, kuten GandCrab -kumppanuusohjelman tapaus osoitti. Yhteistyökumppanit pitävät noin 60 % uhreilta kootuista lunnaista, ja haittaohjelman kehittäjät saavat loput noin 40 %. GandCrabilla on yli 80 aktiivista levittäjää, jotka tartuttivat kahden kuukauden aikana 50 000 uhria ja perivät lunnaita arviolta 300 000 ja 600 000 dollarin välillä liikkuvan summan.

”Kyberrikolliset kehittävät jatkuvasti uusia liiketoimintamalleja, kuten haittaohjelmien kumppanuusohjelmia, maksimoidakseen laittomat tulonsa mahdollisimman riskittömästi. Mutta vaikka uhat ovat poissa silmistä, ne eivät saisi olla poissa mielestä: vaikka kyberhyökkäyksistä tuli vuonna 2018 entistä huomaamattomampia, ne ovat silti yhä tuhovoimaisia ja vaarallisia. Tietoturvaraporttimme auttaa organisaatioita ymmärtämään paremmin tietoturvan uhkia, joille ne altistuvat”, sanoi Check Pointin Chief Marketing Officer **Peter Alexander**, kun raportti julkistettiin Check Pointin CPX 2019 -tapahtumassa Las Vegasissa keskiviikkona.

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.

**Lataa raportti täältä:** <https://research.checkpoint.com/2019-security-report-vol-2-under-the-hood-of-cyber-crime>

**Lisätiedot ja haastattelupyynnöt:**

Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, ramira@checkpoint.com

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 Research**

Check Point Research tarjoaa Check Point Software Technologiesin asiakkaille ja laajemmalle tiedusteluyhteisölle johtavan kybertiedustelutiedon. Tutkimustiimi kerää ja analysoi ThreatCloudin globaalia kyberhyökkäysdataa huolehtien samalla siitä, että kaikki Check POIntin tietoturvatuotteet päivitetään uusimmilla suojauksilla. Tutkimustiimi koostuu yli sadasta analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvatoimittajien, poliisiviranomaisten ja CERT-toimijoiden kanssa.

**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.