**Tietoturvan vuosi: Kybervarustelu kiihtyi
– kryptolouhijat, bottiverkot ja kiristysohjelmat iskussa**

*Kukaan ei ole turvassa kyberhyökkäyksiltä, osoittaa Check Point Researchin vuoden 2020 tietoturvaraportti. Hyökkäykset ovat kehittyneempiä, ovelampia ja kohdennetumpia kuin koskaan ennen.*

**ESPOO – 15. tammikuuta 2020** -- Maailman johtava tietoturvaratkaisujen toimittaja [Check Point Software Technologies](https://www.checkpoint.com/) on julkaissut vuosittaisen tietoturvaraporttinsa. Check Point Security Report 2020 valottaa menetelmiä, joilla kyberrikolliset hyökkäävät organisaatioihin eri toimialoilla ympäri maailmaa. Raportti antaa tietoturva-ammattilaisille ja yritysjohtajille eväitä viidennen sukupolven kyberuhkilta suojautumiseksi.

Check Pointin tutkijat ovat havainnoineet kyberrikollisuuden ilmiöitä kuluneen vuoden aikana. Niistä merkittävimpiä ovat:

* **Kryptolouhijat yhä hallitsevia haittaohjelmia** – Vaikka kryptovaluutan louhinta väheni vuonna 2019 johtuen kryptovaluutan arvon laskusta ja CoinHiven toiminnan päättymisestä maaliskuussa, louhijoita löytyi 38 prosentista yrityksistä maailmanlaajuisesti (37 % vuonna 2018). Louhinta on rikollisille yhä kannattavaa, alhaisen riskin toimintaa.
* **Bottiarmeijoiden koko kasvaa** – bottiverkot levittäytyivät viime vuonna 28 prosenttiin organisaatioista ympäri maailmaa. Kasvua oli yli 50 prosenttia vuoteen 2018 verrattuna. Käytetyin bottihaittaohjelma oli Emotet, muun muassa sen roskapostin jakelun monipuolisuuden vuoksi. Myös esimerkiksi pornokiristykset ja DDoS-hyökkäykset lisääntyivät huomattavasti.
* **Kohdennetut kiristysyritykset aiempaa vakavampia** – Vaikka kiristyksen kohteeksi joutuneita organisaatioita on suhteellisen vähän, hyökkäykset ovat entistä vakavampia. Rikolliset valitsevat kohteensa huolellisesti tavoitteenaan kiristää mahdollisimman suuria summia. Suosituimpia kohteita ovat ohjelmistopalvelut, terveydenhuolto ja julkinen sektori.
* **Mobiilihyökkäykset vähenevät** – Mobiililaitteita koskevia kyberhyökkäyksiä esiintyi viime vuonna 27 prosentissa organisaatioista, luvun ollessa 33 prosenttia vuonna 2018. Mobiiliuhat ovat kehittyneet, mutta organisaatiot ovat niistä tietoisempia ja suojaavat laitteensa paremmin.
* **Magecart-hyökkäykset ylsivät epidemiaksi** – Rajusti lisääntyneet Magecart-hyökkäykset syöttävät haittakoodia verkkokauppasivustoille asiakkaiden maksutietojen varastamiseksi. Niiden uhreja olivat viime vuonna sadat verkkosivut hotelliketjuista ja myymäläjäteistä pieniin ja keskisuuriin yrityksiin, kaikilla alustoilla.
* **Pilvihyökkäykset lisääntyvät** – Nykyään yli [90 prosenttia](https://media.flexera.com/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf) yrityksistä käyttää pilvipalveluita, mutta 67 prosenttia tietoturvatiimeistä valittaa niiden infrastruktuurin ja tietoturvan puutteellisuutta. Pilvihyökkäysten määrä on jatkanut kasvuaan vuonna 2019. Tähän suurimpana syynä on pilviresurssien virheellinen konfigurointi, mutta myös suoraan pilvipalveluntarjoajiin kohdistuvat hyökkäykset ovat lisääntyneet.

"Vuoden 2019 kybermaailma oli monimutkainen. Kansallisvaltiot, kyberrikollisorganisaatiot ja yksityiset tahot kiihdyttivät kyberasevarustelua hälyttävällä tahdilla. Tämä jatkuu vuoteen 2020", kertoo Major Intelligence Officer **Lotem Finkelsteen** Check Point Software Technologiesilta.

”Vaikka organisaatio olisi varustettu parhailla mahdollisilla tietoturvatuotteilla, rikkomusten riskiä ei voida täysin eliminoida. Organisaatioiden tulisi olla proaktiivisia ja tehdä ennakoivat suunnitelmat hyökkäysten estämiseksi eikä keskittyä havaitsemaan ja korjaamaan jo sattuneita vahinkoja. Näin ne pysyvät askeleen edellä hyökkääjiä. Check Pointin vuoden 2020 tietoturvaraportti kertoo, mihin organisaatioiden on kiinnitettävä huomiota ja miten ne voivat voittaa sodan kyberhyökkäyksiä vastaan parhaiden käytäntöjen avulla."

Check Pointin Security Report 2020 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 asiantuntijat analysoivat raportissa tämän hetken ja huomisen monitahoista uhkamaisemaa, jotta se tulisi ymmärretyksi yrityksissä ja organisaatioissa.

*Lataa* [***koko raportti***](https://pages.checkpoint.com/cyber-security-report-2020.html) *ja lue* [***blogi***](https://blog.checkpoint.com/2020/01/15/the-2020-check-point-cyber-security-annual-report-is-available/) *Check Pointin sivustolla.*

**Lisätietoja:**Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, ramira@checkpoint.com.
Haastattelupyynnöt: Viestintäkonsultti Päivi Savolainen, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

**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>

**Julkaisijasta:**

**Check Point Research**

Check Point Research ([research.checkpoint.com](https://research.checkpoint.com)) huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvayhteisöllä on käytettävissään paras mahdollinen tieto kyberturvallisuuden riskeistä. Tutkijaryhmä kerää ja analysoi ThreatCloud-verkkopalvelun tallentamat maailmanlaajuiset kyberhyökkäystiedot, jotta hakkerit pysyvät kurissa ja kaikki Check Pointin tuotteet pystytään päivittämään uusimmilla suojauksilla. Tutkijaryhmä koostuu yli 100 analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvayhtiöiden ja viranomaisten 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 hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.