Tietoturvaennuste 2019: Kuusi kehittyvää trendiä

**ESPOO – 19. joulukuuta 2018** – Tietoturvayhtiö Check Pointin tietoturvaennuste 2019 listaa nousevat trendit, joiden kanssa yritysten tietoturvavastaavat todennäköisesti painiskelevat ensi vuoden aikana.

**1. Digitaalista kultaa kaivetaan yhä syvemmältä**

Kryptovaluutan louhijat ohittivat kiristyshaittaohjelmat kyberrikollisten suosikkiansaintamuotona ja dominoivat haittaohjelmamaisemaa koko vuoden 2018 ajan. Check Pointin haittaohjelmakirjanpidon mukaan louhijoiden esiintyvyys yritysverkoissa nousi globaalisti 42 prosenttiin, kun edellisen syksyn lukema oli 20,5 prosenttia. Kryptolouhijoiden suosion syyt ovat yksinkertaiset: ne ovat helppoja levittää ja hankalia havaita. Louhija saattaa jauhaa kuukausien ajan tuloja rikollisille ennen kuin se huomataan.

Näin tehokkaat haittaohjelmat tuskin jäävät pois käytöstä vuonna 2019. Päinvastoin ne kaivautuvat todennäköisesti entistäkin syvemmälle yritysten tietoverkkoihin. Niiden parannellut versiot ottanevat kohteekseen skaalattavat pilviympäristöt ja suojaamattomat mobiiliympäristöt, jolloin ne pääsevät käsiksi massiivisiin tietokoneresursseihin.

**2. Mobiililaitteiden tietoturvan vähättely jatkuu**

Vaikka älypuhelimet muodostavat suuren osan yritysten hyökkäyksille alttiista pinnasta, niiden tietoturvan vähättely jatkuu. Häijy Android-laitteiden pankkitroijalainen [Lokibot](https://blog.checkpoint.com/2018/09/11/augusts-most-wanted-malware-banking-trojan-attacks-turn-up-the-heat/) oli vuonna 2018 kolmen levinneimmän mobiilihaittaohjelman joukossa. Lokibot anastaa tietoja ja järjestää hyökkääjille oikeuden ladata laitteelle lisää haittaohjelmia. [Syyskuussa 2018](https://blog.checkpoint.com/2018/10/15/september-2018s-most-wanted-malware-cryptomining-attacks-against-apple-devices-on-the-rise/) kryptolouhijat usutettiin joukolla iPhone- ja iOS-laitteiden kimppuun. Louhijoiden määrä kasvoi tuolloin nopeasti 400 prosenttia aiempaan verrattuna.

Check Point ennustaa, että mobiilihaittaohjelmien määrä kasvaa vuonna 2019. Uutena on tulossa all-in-one-haittaohjelmia, joissa yhdistyvät pankkitroijalaisten, näppäilyn tallentajien ja kiristyshaittaohjelmien ominaisuudet. Ne antavat rikollisille mukavasti valinnanvaraa hyökkäysten kehittelyyn. Laitteiden käyttöjärjestelmistä löytynee uusia haavoittuvuuksia, jotka tarjoavat helppoja reittejä suojaamattomien laitteiden sisuksiin.

**3. Pilven tietoturva rakoilee**

Pilven skaalattavuus ja joustavuus vetoaa yrityskäyttäjiin, mutta palveluja kehitettäessä ajatellaan harvoin tietoturvaa alusta asti. Marraskuussa 2018 Check Point kertoi löytämistään [haavoittuvuuksista bisneskäytössä suosittujen kuvauskopterien pilvipalvelualustassa](https://blog.checkpoint.com/2018/11/08/the-spy-drone-in-your-cloud/). Haavoittuvuus oli tuolloin jo korjattu, mutta se jätti kopterien lentoreitit, kuvat, paikkatiedot ja käyttäjien luottokorttitiedot ulkopuolisten armoille. Näin voi käydä, kun ensin kehitetään palvelu ja vasta sitten mietitään tietoturvaa.

Vuonna 2019 on odotettavissa, että pilvessä sijaitsevien käyttäjätilien kaappaukset ja hakkerointiyritykset lisääntyvät, kun yhä useammat yritykset käyttävät SaaS-sovelluksia ja pilvipohjaista sähköpostia (esimerkiksi Office 365, GSuite ja One Drive). Kalasteluyritykset tulevat tämän myötä yleistymään vielä nykyisestä.

**4. Koneoppiminen yleistyy hyvässä ja pahassa**

Koneoppiminen ja tekoälytekniikat ovat [parantaneet dramaattisesti uusien haittaohjelmien tunnistamista](https://blog.checkpoint.com/2018/08/30/ai-and-cybersecurity-combining-data-with-human-expertise/) ja niihin reagoimista 18 viime kuukauden aikana. Uudet uhat on pystytty tekemään vaarattomiksi jo ennen kuin ne ovat levinneet laajalti. Toisaalta myös kyberrikolliset alkavat hyödyntää koneoppimisen tekniikoita yritysverkkojen heikkojen kohtien etsimiseen, haavoittuvuuksien löytämiseen ja paremmin piiloutuvien haittaohjelmien kehittämiseen.

**5. Viranomaisilla on sormensa pelissä**

Valtiolliset toimijat eivät välty tietoturvahuolilta. Viime vuosina viranomaisia ovat huolettaneet etenkin kriittisiin infrastruktuurikohteisiin kuten sähköverkkoihin kohdistuvat hyökkäysriskit. Monissa maissa on perustettu erityisiä kansallisen kyberturvallisuuden toimielimiä, joiden tehtävä on varautua tämäntyyppisiin hyökkäyksiin.

Samaan aikaan valtiolliset toimijat käyttävät haittaohjelmia myös itse, joskus jopa vakoillakseen omia kansalaisiaan. Vuonna 2018 tällainen tapaus havaittiin Iranissa, jossa kansalaisia valvottiin älypuhelinten avulla [Domestic Kitten](https://www.scmagazineuk.com/domestic-kitten-malware-campaign-targets-iranians/article/1492352) -kampanjassa. Sadat ihmiset latasivat puhelimilleen vaarattomaksi naamioidun sovelluksen, joka vakoili heitä.

Hyökkäyksillä infrakohteisiin ei ole toistaiseksi saatu aikaan massiivisia tuhoja. On kuitenkin varsin todennäköistä, että valtiot käyttävät kybersodankäynnin keinoja jatkossakin. Kybervakoilusta ja kansalaisten yksityisyyden suojasta tulee nykyistäkin kuumempi puheenaihe etenkin, kun vaalituloksiin vaikuttamisesta [on jo saatu todisteita](https://www.theguardian.com/commentisfree/2017/mar/06/big-data-cambridge-analytica-democracy).

**6. Nanotietoturva yleistyy globaalisti**

Yhä useammassa laitteessa on verkkoyhteys. Yrityksissä [ei ole onnistuttu](https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/) luomaan kunnollisia käytäntöjä verkkojen ja laitteiden suojaamiseksi turvattomien IoT-laitteiden aiheuttamilta tietoturvariskeiltä. IoT-laitteiden ja niiden pilvipalveluyhteyksien tietoturva on edelleen heikko. Seuraavien kahden vuoden aikana fyysiset rakenteet katoavat enenevässä määrin pilveen, jonka etuna on palvelujen nopea skaalattavuus. Pilvipalvelut hoitavat yhteyksiä puhelimiin, robottiautoihin, IoT-antureihin, lääkinnällisiin laitteisiin tai mihin tahansa muuhun, jolla on yhteys internetiin. Tämän laiteverkoston suojaaminen tietoturvan riskeiltä on kriittistä, jotta pilvessä lymyävien ja sieltä laajalle levittäytyvien uusien uhkien leviäminen voidaan estää.

Uuden sukupolven tietoturva vastaa haasteeseen käyttämällä nanoteknologiaa soveltavia tietoturva-agentteja. Erittäin pienikokoinen lisäosa toimii missä laitteessa ja ympäristössä tahansa. Nanoagentti pystyy kontrolloimaan kaikkea laitteeseen tulevaa ja siltä lähtevää liikennettä, ja se pitää yhteyttä tekoälypohjaiseen, globaaliin tietoturvajärjestelmään, joka ohjaa tietoturvaa ja tekee ratkaisut reaaliajassa.

--

**Lisätiedot ja haastattelupyynnöt:**

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

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>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.