**Kyberuhkien alkuvuoden trendit – Hyökkääjät ratsastivat koronaviruksella verkkoihin, pilveen ja mobiiliin**

*Check Pointin “Cyber Attack Trends: 2020 Mid-Year Report” -raportti paljastaa koronavirusaiheisten kyberhyökkäysten kohdistuneen kaikkiin ympäristöihin. Check Point korostaa puolivuotiskatsauksessaan myös kansallisvaltioiden kyberaktiivisuuden nousua.*

**SAN CARLOS, CA — 22. heinäkuuta 2020** – Tietoturvayhtiö [Check Point® Software Technologies](https://www.checkpoint.com/) on julkaissut puolivuotiskatsauksensa kyberhyökkäysten trendeistä. “Cyber Attack Trends: 2020 Mid-Year Report” paljastaa, kuinka rikolliset, poliittiset ja kansallisvaltioiden uhkatoimijat ovat hyödyntäneet COVID-19-pandemiaa hyökkäyksissään organisaatioihin kaikilla aloilla, mukaan lukien hallitukset, teollisuus, terveydenhuolto, palveluntarjoajat, kriittinen infrastruktuuri ja kuluttajat.

Koronavirukseen liittyvät tietojenkalastelu- ja haittaohjelmahyökkäykset lisääntyivät dramaattisesti helmikuun alle 5 000:stä viikossa huhtikuun lopun yli 200 000:een viikoittain. Maiden purkaessa rajoituksiaan touko-kesäkuussa hyökkääjät aktivoituivat hyödyntämään myös muita aiheita. Tämä lisäsi kaiken tyyppisiä kyberhyökkäyksiä kesäkuun lopussa 34 prosentilla maalis-huhtikuuhun verrattuna maailmanlaajuisesti.

**Vuoden 2020 alkupuolen keskeisiä suuntauksia:**

* **Kybersodankäynti yltyy**: Kansallisvaltioiden kyberhyökkäykset lisääntyivät voimakkaasti vuoden 2020 alkupuolella, kun valtiot pyrkivät saamaan tiedustelutietoa pandemian käsittelyyn liittyen. Hyökkäykset kohdistuivat myös terveydenhuoltoon ja humanitaarisiin järjestöihin, esimerkiksi Maailman terveysjärjestö [WHO ilmoitti hyökkäysten lisääntyneen 500 prosentilla](https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance).
* **Kaksinkertainen kiristys**: Vuonna 2020 on käytetty laajasti uutta kiristyshyökkäyksen muotoa, jossa hyökkääjät keräävät suuria määriä tietoja ennen salausta. Uhreja, jotka kieltäytyvät maksamasta lunnaita, uhataan tietojen vuotamisella, mikä painostaa heitä suostumaan rikollisten vaatimuksiin.
* **Mobiilihyökkäykset**: Uhkatoimijat ovat etsineet uusia mobiilihyökkäysvektoreita ja kehittäneet tekniikoitaan tietoturvajärjestelmien ohittamiseksi ja haitallisten sovellusten ujuttamiseksi virallisiin sovelluskauppoihin. Toisessa [innovatiivisessa hyökkäyksessä](https://research.checkpoint.com/2020/mobile-as-attack-vector-using-mdm/) rikolliset käyttivät suuren kansainvälisen yrityksen mobiililaitehallintajärjestelmää levittäen haittaohjelmia yli 75 prosenttiin hallituista mobiililaitteista.
* **Pilvihyökkäykset**: Pandemian aikainen nopea siirtyminen julkisiin pilviympäristöihin on lisännyt niihin varastoituihin tietoresursseihin ja arkaluontoiseen dataan kohdistuvia hyökkäyksiä. Uhkatoimijat käyttävät myös pilvi-infrastruktuuria [varastoidakseen haittaohjelmahyökkäysten haitallisia hyötykuormia](https://research.checkpoint.com/2020/threat-actors-migrating-to-the-cloud/). Check Pointin tutkijat havaitsivat tammikuussa Microsoft Azuressa alan ensimmäisen [kriittisen haavoittuvuuden](https://blog.checkpoint.com/2020/01/30/check-point-research-partners-with-microsoft-azure-to-create-a-safer-better-secured-cloud-infrastructure/), joka olisi antanut hakkereille mahdollisuuden vaarantaa muiden Azure-vuokralaisten tietoja ja sovelluksia. Tämä osoittaa, että julkiset pilvet eivät automaattisesti ole turvallisia.

”Maailmanlaajuinen reagointi pandemiaan on muuttanut ja nopeuttanut uhkatoimijoiden tavanomaista hyökkäysmallia tämän vuoden ensimmäisellä puoliskolla. Hyökkääjät ovat hyödyntäneet COVID-19:n ympärillä olevia pelkoja ja suojanneet niillä toimintaansa. Olemme myös havainneet uusia merkittäviä haavoittuvuuksia ja hyökkäysvektoreita, jotka uhkaavat organisaatioiden turvallisuutta kaikilla aloilla. Tietoturva-asiantuntijoiden on oltava tietoisia näistä nopeasti kehittyvistä uhista, jotta he voivat varmistaa organisaatioidensa parhaan mahdollisen suojaustason loppuvuoden 2020 aikana,” kommentoi Check Pointin tietoturvatutkijaryhmän johtaja **Maya Horowitz**.

**Yleisimmät haittaohjelmat, vuoden 2020 alkupuoli:**

1. **Emotet (esiintyvyys 9 % yritysverkoista maailmanlaajuisesti) –**Kehittynyt, itsemonistuva ja modulaarinen troijalainen. Tullut laajalti tutuksi pankkitroijalaisena, mutta sitä on käytetty myös bottiverkkona laajoissa roskapostikampanjoissa sekä muiden haittaohjelmien jakamisessa.  Hyödyntää useita eri keinoja pysyäkseen elinvoimaisena ja kiertotekniikoita ollakseen huomaamaton. Pystyy leviämään haitallisia liitetiedostoja tai linkkejä sisältävien kalastelusähköpostien kautta.
2. **XMRig (8 %)** – Avoimen lähdekoodin laitteille tarkoitettu Monero-kryptovaluutan louhija.
3. **Agent Tesla (7 %)** – Edistyksellinen etäkäyttötroijalainen (RAT), joka on ollut aktiivinen vuodesta 2014. Se pystyy esimerkiksi uhrinsa näppäinten painalluksia seuraamalla ja kuvakaappauksia ottamalla pääsemään käsiksi WiFi-salasanoihin ja muihin kohdelaitteen tietoihin (esimerkiksi Google Chrome, Mozilla Firefox ja Microsoft Outlook -sähköpostiohjelma).

**Yleisimmät kryptolouhijat, vuoden 2020 alkupuoli:**

1. **XMRig (46 % kaikesta kryptolouhinnasta maailmanlaajuisesti)** – Avoimen lähdekoodin laitteille tarkoitettu Monero-kryptovaluutan louhija, joka tunnistettiin ensimmäistä kertaa vuonna 2017.
2. **Jsecoin (28 %)** – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. JSEcoin lopetti toimintansa huhtikuussa 2020.
3. **Wannamine (6 %)** – Kryptovaluutta Moneroa louhiva haitta­ohjelma, joka levittäytyy verkkomadon tavoin.

 **Yleisimmät mobiilihaittaohjelmat, vuoden 2020 alkupuoli**

1. **xHelper (24 % kaikista mobiilihaittaohjelmahyökkäyksistä)** – Android-haittaohjelma, joka voi ladata muita haitallisia sovelluksia sekä näyttää haitallisia mainoksia. Se myös kykenee asentamaan itsensä uudelleen, vaikka uhri olisi poistanut sen. Ensimmäisen kerran marraskuussa 2019 havaittu xHelper on tartuttanut yli 45 000 laitetta.
2. **PreAMo (19 %)** – Huhtikuussa 2019 tunnistettu Android-haittaohjelma, joka jäljittelee käyttäjää klikkaamalla bannereita. Google Playsta löydetty haittaohjelma on ladattu yli 90 miljoonaa kertaa kuuteen eri mobiilisovellukseen.
3. **Necro (14 %)** – Android-laitteiden haittaohjelma, joka levittää muita haittaohjelmia, mutta pystyy myös näyttämään mainoksia ja anastamaan rahaa väärennettyjen tilausten avulla.

**Yleisimmät pankkihaittaohjelmat, vuoden 2020 alkupuoli:**

1. **Dridex (27 % kaikista pankkihaittaohjelmahyökkäyksistä)** – Pankkitroijalainen, jonka kohteena ovat Windows PC:t. Dridex ohjaa uhrin pankkitiedot hyökkääjän hallitsemaan palvelimeen. Se ottaa yhteyttä etäpalvelimeen, lähettää tietoja tartunnan saaneesta järjestelmästä ja voi myös ladata ja suorittaa lisämoduuleja kauko-ohjausta varten.
2. **Trickbot (20 %)** – Modulaarinen pankkitroijalainen, joka kohdistuu Windows-alustaan ja levittäytyy useimmiten roskapostikampanjoiden tai muiden haittaohjelmien välityksellä.
3. **Ramnit (15 %)** – Vuonna 2010 tunnistettu modulaarinen pankkitroijalainen, joka varastaa verkkoistuntojen tietoja.

Check Pointin kyberhyökkäyksiin pureutuva puolivuotisraportti tarjoaa yksityiskohtaisen katsauksen kyberuhkien maailmaan. Raportti perustuu Check Point ThreatCloudinTM keräämiin tietoihin tammikuun ja kesäkuun 2020 välisenä aikana. Se nostaa esiin hakkereiden eniten suosimat tavat hyökätä yrityksiä vastaan.

Raportin täysversio on saatavissa [täällä](https://pages.checkpoint.com/cyber-attack-2020-trends.html).

**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 Point Researchia:**Blog: <https://research.checkpoint.com/>

Twitter: <https://twitter.com/_cpresearch_>

Podcast: <https://research.checkpoint.com/category/cpradio/>

Facebook: <https://www.facebook.com/checkpointresearch>

**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.