**Koronavirus hakkereiden täkynä – Lisätietoja epidemiasta tarjoava roskaposti levittää haittaohjelmaa**

*Koronaviruspelon lisäksi kyberrikolliset hyödynsivät tammikuussa ahkerasti haavoittuvuutta, jota esiintyy jo 45 prosentissa maailman yritysverkoista, kertovat tietoturvayhtiö Check Pointin tutkijat.*

**ESPOO – 12. helmikuuta 2020 –** Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research kertoo haittaohjelmakatsauksessaan, että Emotet oli maailman yleisin haittaohjelmauhka jo neljättä kuukautta peräkkäin. Tammikuussa sitä levitettiin koronavirusaiheisen roskapostikampanjan avulla.

Tutkijoiden mukaan haitalliset sähköpostit näyttävät ilmoittavan, missä koronavirus leviää, tai tarjoavan lisätietoja viruksesta. Ne rohkaisevat sähköpostin saajaa avaamaan liitteet tai napsauttamaan viestin linkkejä, jotka avattaessa yrittävät ladata uhrin koneelle Emotet-haittaohjelman. Emotet-sovellusta käytetään ensisijaisesti kiristys- ja muiden haittaohjelmien jakeluun.

Valtaosa koronavirusaiheisista roskapostikampanjoista on suuntautunut Japaniin ja Indonesiaan. Niiden rinnalle on noussut koronavirusta verkkotunnuksissaan käyttäviä huijaussivustoja, jotka väittävät myyvänsä rokotuksia virusta vastaan.

Tammikuussa lisääntyivät myös yritykset hyödyntää niin kutsuttua ”MVPower DVR Remote Code Execution” -haavoittuvuutta. Se nousi joulukuun kolmannelta sijalta maailman käytetyimmäksi. Haavoittuvuutta esiintyy jo 45 prosentissa organisaatioista maailmanlaajuisesti. Hyökkäyksen onnistuessa pahantekijä pystyy suorittamaan haitallisen koodin valitulla koneella.

"Yleisimmät yritysverkkoihin kohdistuvat uhat ovat edelleen monipuolisia haittaohjelmia, kuten Emotet, XMRig ja Trickbot. Ne ovat levinneet yhteensä jo yli 30 prosenttiin organisaatioista ympäri maailmaa", kertoo Check Pointin Threat Intelligence & Research, Products -ryhmän johtaja **Maya Horowitz**.

"Yritysten tulisi opastaa työntekijöitään tunnistamaan ajankohtaisiin aiheisiin liittyviä ​​roskaposteja, jotka yleensä levittävät haittaohjelmia. Myös yritysten tietoturvan tulisi olla ajan tasalla, jotta ne pystyvät torjumaan verkkouhkia ja estämään kiristysyritykset ja tietovarkaudet", hän muistuttaa.

Suomessa tammikuun yleisin haittaohjelma oli kryptolouhija XMRig, jota esiintyi noin joka kymmenennessä yritysverkossa. Toista sijaa piti pankkihuijari TrickBot. Koronaviruksella ratsastava Emotet ei ehtinyt Suomen listalle tammikuussa.

**Suomen yleisimmät haittaohjelmat tammikuussa 2020:**

1. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 9,73 %.
2. **TrickBot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 6.19 %.
3. **IsErIk**. Esiintyvyys 3,54 %.

4. **RigEK**. Esiintyvyys 2.65%.

5. **Formbook** – Windows OS -järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 2,65 %.

6. **NJRat** – Etäyhteystroijalainen, suunnattu lähinnä Lähi-idän valtion virastoihin ja järjestöihin. Tallentaa uhrin näppäinpainalluksia, käyttää kameraa, varastaa selaimiin tallennettuja tietoja sekä lataa ja lähettää tiedostoja. Esiintyvyys 1,77 %.

7. **Guerrilla** – Troijalainen, joka lataa muita haittaohjelmia Android-puhelimille ja on onnistuttu upottamaan useisiin sovelluksiin. Tuottaa vilpillisiä mainostuloja sovelluskehittäjille. Esiintyvyys 1,33 %.

8. **Vidar** – Windows-käyttöjärjestelmien haittaohjelma, joka varastaa salasanoja, luottokorttitietoja ja muuta arkaluontoista tietoa useista selaimista ja digitaalisista lompakoista. Esiintyvyys 1,33 %.
9. **Lotoor** – Hakkerointityökalu, joka hyödyntää Android-käyttöjärjestelmän haavoittuvuuksia juurioikeuksien saamiseksi vaarantuneista mobiililaitteista. Esiintyvyys 1,33 %.
10. **Domen**. Esiintyvyys 1,33 %.
11. **Remcos** – Jakaa haittaohjelmia roskaposteihin liitettyjen Microsoft Office -asiakirjojen kautta. Esiintyvyys 1,33 %.

**Maailman yleisimmät haittaohjelmat ja haavoittuvuudet tammikuussa 2020:**

1. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään nykyään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 13 %.
2. **XMRig** – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan. Esiintyvyys 10 %.
3. **Trickbot** – Pankkitroijalainen, jota päivitetään jatkuvasti uusilla ominaisuuksilla. Joustava ja räätälöitävä haittaohjelma, jota voidaan käyttää monikärkisten kampanjoiden osana. Esiintyvyys 7 %.

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli tammikuussa **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta ja asentamaan itsensä uudelleen, jos käyttäjä poistaa sen. Toisella sijalla oli muita haittaohjelmia Android-puhelimille lataava **Guerrilla**, joka on onnistuttu upottamaan useisiin sovelluksiin. Troijalainen tuottaa vilpillisiä mainostuloja sovelluskehittäjille. Kolmanneksi yleisin oli Android-käyttäjiin kohdistuva mainosohjelma **AndroidBauts**.

Check Pointin tutkijat listasivat myös tammikuun käytetyimmät **haavoittuvuudet**. Luettelon kärjessä oli **“MVPower DVR Remote Code Execution”**, jota esiintyi 45 prosentissa yritysverkoista maailmanlaajuisesti. Toiseksi yleisin oli **“Web Server Exposed Git Repository Information Disclosure”**, esiintyvyys 44 prosenttia. Kolmannella sijalla oli **“PHP DIESCAN information disclosure”**, esiintyvyys 42 prosenttia.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Täydellinen Top 10 -haittaohjelmalista löytyy [Check Pointin blogista](https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-malicious-emotet-malware/).

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa [www.checkpoint.com](http://www.checkpoint.com).

**Lisätiedot:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com.
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

**Seuraa Check Point Researchia:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**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.