**Herätys! Linux-laitteiden haittaohjelma SpeakUp yleistyi nopeasti tammikuussa – pahempaa voi olla tulossa**

*Tietoturvayhtiö Check Pointin ylläpitämälle haittaohjelmalistalle kohosi tammikuussa uusi nimi: Linux-palvelimia tartuttava SpeakUp, joka levittää XMRig-kryptolouhijaa.*

**ESPOO – 15. helmikuuta 2019 –** Linux-palvelimia tartuttava troijalainen [SpeakUp](https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/) nousi tammikuussa ensi kertaa tietoturvayhtiö Check Pointin globaalin haittaohjelmatilaston kymmenen kärkeen. Haittaohjelma on toiminut takaovena levittäen XMRig-kryptolouhijaa, mutta sen kautta voi syöttää kohdelaitteelle minkä tahansa muunkin haittaohjelman ja käynnistää sen.

Uusi troijalainen pystyy tällä hetkellä harhauttamaan kaikkien tietoturvatoimittajien virustorjuntaohjelmia. Sitä on levitetty hyödyntämällä useita tunnettuja haavoittuvuuksia. Check Pointin tutkijoiden mielestä SpeakUpista tekee vaarallisen nimenomaan kyky levittää muita haittaohjelmia.

Kymmenen kärjessä -listan haittaohjelmista peräti puolet pystyy lataamaan tartuttamalleen laitteelle lisää haittaohjelmia. Check Pointin tietoturvatutkijoiden tiimiä vetävä **Maya Horowitz** toteaa, että lähes muuttumattomana pysynyt haittaohjelmatilaston kryptolouhijakärki kätkee alleen vähittäisen muutoksen haittaohjelmien levittämisen tavassa.

”SpeakUpin tapaiset haittaohjelmat ovat vahva varoitusmerkki. Niiden yleisyydestä voi päätellä, että jotakin pahempaa on tulossa. Koska Linux-käyttöjärjestelmää käytetään paljon yrityspalvelimissa, uskomme, että SpeakUp kasvaa vuoden mittaan nykyistä levinneemmäksi ja entistä vakavammaksi uhaksi, Horowitz sanoo.

Suomen haittaohjelmatilaston kolmen kärjessä oli samat ohjelmat kuin joulukuussa. XMRig ja Coinhive olivat vain vaihtaneet paikkaa keskenään. SpeakUp ei meillä yltänyt kymmenen levinneimmän haittaohjelman joukkoon, mutta myös Suomen listalta löytyvät Cridex, Emotet ja Smokeloader pystyvät valmistelemaan tietä muille haittaohjelmilla.

**Suomen yleisimmät haittaohjelmat tammikuussa 2019 Top 3:**

XMRig – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017. Esiintyvyys 16 % organisaatioista.

Coinhive – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla. Esiintyvyys 15 %.

Cridex – Windows-mato, joka yrittää anastaa esimerkiksi luottokorttitietoja. Voi ladata laitteelle myös muita haittaohjelmia. Leviää internet-jakojen ja ulkoisten muistien avulla. Esiintyvyys 10 %.

**Maailman yleisimmät haittaohjelmat tammikuussa 2019 Top 3:**

*\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna*

↔ Coinhive – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla. Käyttää runsaasti laitteen prosessoritehoa.

↑ XMRig – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017.

↑ Cryptoloot – Coinhiven kilpailija kryptolouhinnassa.

Mobiilihaittaohjelmien globaalilla listalla Android-laitteiden takaovi Hiddad syrjäytti samantyyppisen Triadan kärkipaikalta. Kakkossijan vei Lotoor, ja Triada jäi tällä kertaa kolmanneksi.

Check Pointin tutkijat listasivat myös käytetyimmät haavoittuvuudet. Suosituimpana jatkoi Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow CVE-2017-7269, jonka globaali esiintyvyys oli 47 %. Toiseksi hyödynnetyin haavoittuvuus oli Web Server Exposed Git Repository Information Disclosure, esiintyvyys 46 %, ja kolmanneksi jäi OpenSSL TLS DTLS Heartbeat Information Disclosure, esiintyvyys 45 % organisaatioista globaalisti.

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 osoitteesta

<http://blog.checkpoint.com/2019/02/13/january-2019s-most-wanted-malware-a-new-threat-speakup-linux-crypto-cryptomining/>

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa <http://www.checkpoint.com/threat-prevention-resources/index.html>

**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>

Blog: <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.