**Toukokuun haittaohjelmakatsaus: Päivitä nyt, älä odota BlueKeep-iskua**

*Check Pointin tietoturvatutkijat ovat havainneet useita yrityksiä paikantaa laitteita, jotka ovat alttiita Bluekeep-haavoittuvuuden hyödyntämiselle. Kyseessä on todennäköisesti ollut haittaohjelmahyökkäysten valmistelu.*

**ESPOO – 13. kesäkuuta 2019 –** Tietoturvayhtiö Check Pointin tutkijaryhmä kehottaa yrityksiä ja organisaatioita tarkistamaan ja päivittämään välittömästi kaikki Windows 7- ja Windows Server 2008 -järjestelmiä käyttävät laitteensa ja palvelimensa hiljattain havaitun BlueKeep-haavoittuvuuden ([CVE-2019-0708](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708)) paikkaamiseksi. Päivitys pienenentää riskiä joutua kiristyshaittaohjelma- ja kryptolouhijahyökkäyksien kohteeksi.

Haavoittuvuus sijaitsee Windowsin Remote Desktop Service -etätyöpöytäyhteydessä. Vaarassa olevia verkkoon kytkettyjä laitteita on lähes miljoona, ja niiden lisäksi riski koskee yritysten ja organisaatioiden omien verkkojen laitteita, joissa on käytössä vanhempia Windows-versioita ja etätyöpöytäyhteys. Haavoittuvuus on kriittinen, koska sen hyödyntäminen on mahdollista ilman käyttäjän myötävaikutusta. Etätyöpöytäyhteyden kautta on aikaisemmin levitetty esimerkiksi [Samsam](https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=malwarefamily&threatId=14666)- ja [Dharma](https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=malwarefamily&threatId=306866) -kiristyshaittaohjelmia.

Check Pointin tutkijaryhmä on viime päivinä havainnut useita verkon skannauksia, joiden tavoitteena on ollut tunnistaa laitteita, joissa on paikkaamaton BlueKeep-haavoittuvuus. Skannausyrityksiä on tehty globaalisti eri maista. Niiden tavoitteena on mahdollisesti ollut haittaohjelmahyökkäyksen valmistelu. [Microsoftin](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708) julkistamien paikkausten ohella Check Point tarjoaa sekä [verkko- että laitekohtaisen suojauksen](https://blog.checkpoint.com/2019/05/20/critical-vulnerability-in-windows-os-security-threat-patch-how-to-protect-yourself/) näiltä hyökkäyksiltä.

Check Pointin Threat Intelligence and Research Director **Maya Horowitzin** mukaan BlueKeep on viime kuukausien merkittävin tietoturvauhka.

”Haavoittuvuutta ei ole tiettävästi vielä käytetty, mutta julkisuudessa on esitetty useita mahdollisia hyödyntämisen tapoja. Olemme samaa mieltä Microsoftin ja muiden tietoturva-alan toimijoiden kanssa siinä, että BlueKeepiä on mahdollista käyttää yhtä suuriin hyökkäyksiin kuin vuoden 2017 massiiviset WannaCry- ja NotPetya -kampanjat. Yksikin tietokone, jossa on paikkaamaton vika, voi toimia porttina, jonka kautta koko yritysverkko saa haittaohjelmatartunnan. Kaikki tartunnan saaneet tietokoneet, jotka ovat yhteydessä internetiin, voivat sitten tartuttaa muita haavoittuvuuden sisältäviä laitteita, jolloin hyökkäys voi levitä eksponentiaalisesti ja nopeudella, johon on vaikea puuttua. Tästä syystä on kriittistä, että yritykset ja organisaatiot suojaavat itseään ja muita paikkaamalla haavoittuvuuden nyt, ennen kuin se on myöhäistä”, Horowitz jatkoi.

Kiristyshaittaohjelmaa palveluna tarjonneen [GandCrab Ransomware-as-a-Service](https://research.checkpoint.com/gandcrab-ransomware-mindset/) -yhteistyöohjelman kehittäjät ilmoittivat toukokuun viimeisenä päivänä toimintansa päättymisestä ja kehottivat yhteistyökumppaneitaan lopettamaan GandCrabin levittämisen 20 päivän sisällä. Haittaohjelmapalvelu on ollut toiminnassa tammikuusta 2018 lähtien, ja uhreja kertyi jo kahden ensimmäisen kuukauden aikana 50 000. Palvelun kehittäjien ja yhteistyökumppanien keräämien tulojen sanotaan kohoavan miljardeihin dollareihin. Gandcrab nousi säännöllisesti kuukauden 10 yleisimmän haittaohjelman joukkoon, koska sitä päivitettiin jatkuvasti tavoilla, jotka auttoivat sitä kätkeytymään tietoturvaohjelmistoilta.

**Suomen yleisimmät haittaohjelmat toukokuussa 2019:**

1. Jsecoin– Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa. Esiintyvyys 9 % organisaatioista.
2. Vidar – esiintyvyys 7 %.
3. XMRig – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017. Esiintyvyys 6 %.
4. Cryptoloot – Kryptovaluutan louhija, joka louhii Moneroa. Esiintyvyys 6 %.
5. Nivdort – Troijalainen, joka kerää salasanoja ja tietoa käyttäjän asetuksista. Esiintyvyys 6 %.
6. Ramnit, 7. Formbook, 8. Neshta, 9. Emotet 10. Badrabbit, PrizeRAT ja Tofsee

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

1. Cryptoloot – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. XMRig – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan.
3. Jsecoin – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa.
4. Emotet, 5. Ramnit, 6. Emotet, 7. Dorkbot, 8. Trickbot, 9. Nivdort, 10. Agentesla

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli **Lotoor**, joka on Android-laitteiden haavoittuvuuksia hyödyntävä hakkerityökalu. Kakkoseksi kohosi **Hiddad**, jonka tärkein toimintamuoto on mainosten levittäminen. Se pystyy kuitenkin myös nappaamaan käyttäjätietoja Android-puhelimelta ja välittämään ne eteenpäin vääriin käsiin. Kolmanneksi yleisin mobiilihaittaojelma oli **Triada**, Android-laitteiden takaovi, jonka avulla hyökkääjä saa laitteen pääkäyttäjäoikeudet.

Check Pointin tutkijat listasivat myös käytetyimmät haavoittuvuudet. Perinteiset hyökkäyskeinot kokivat toukokuussa uuden tulemisen, todennäköisesti kryptolouhijoiden tuottoisuuden ehtymisen takia. **SQL-injektiotekniikka** johti hyödynnetyimpien haavoittuvuuksien listaa 49 prosentin esiintyvyydellä yritysverkoissa. **Web Server Exposed Git Repository Information Disclosure** oli toukokuun toiseksi hyödynnetyin haavoittuvuus 44 prosentin esiintyvyydellä, ja kolmanneksi kohosi **OpenSSL TLS DTLS Heartbeat Information Disclosure**, jonka esiintyvyys oli 41 prosenttia organisaatioista kautta maailman.

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.

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

**Lisätiedot ja haastattelupyynnöt:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com

Maija Rauha, viestintäkonsultti, OSG Viestintä, 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.