# Uusi puhelinten haittaohjelma SpinOK yleistyy vauhdikkaasti – Nämä olivat kesäkuun 2023 yleisimmät haittaohjelmat Suomessa ja maailmalla

*Check Point Softwaren kesäkuun haittaohjelmakatsaus kertoo, että alkuvuoden yleisin haittaohjelma on ollut monikäyttöinen Qbot, joka oli kesäkuussa myös Suomen yleisin haittaohjelma. Mobiililaitteiden troijalainen SpinOK nappasi kesäkuussa ensi kertaa puhelinten haittaohjelmien Top 10 -listan kärkipaikan.*

**ESPOO – 11. heinäkuuta 2023 –** Maailman johtava tietoturvayhtiö Check Point Software Technologies on julkaissut kesäkuun 2023 haittaohjelmakatsauksensa. Check Pointin tutkijoiden mukaan alkuvuoden yleisin haittaohjelma on ollut Qbot-troijalainen, joka on pitänyt globaalin haittaohjelmien listan kärkipaikkaa viitenä kuukautena kuudesta. Qbot oli kesäkuussa myös Suomen yleisin haittaohjelma. Android-laitteiden troijalainen SpinOK nappasi puhelinhaittaohjelmien listan ykköspaikan, vaikka se havaittiin ensi kertaa vasta toukokuussa. Kiristysohjelmat nousivat jälleen otsikoihin sen jälkeen, kun MOVEit-tiedostonjakopalvelusta löytyi nollapäivähaavoittuvuus, jota on käytetty hyökkäyksissä niin ulkomailla kuin Suomessakin.

Ensimmäiset havainnot Qbotista tehtiin vuonna 2018, jolloin se oli pelkkä pankkitroijalainen. Sitä on sittemmin kehitetty jatkuvasti, ja sen lisätoiminnot mahdollistavat muun muassa salasanojen, sähköpostiviestien ja luottokorttitietojen urkkimisen. Sitä levitetään yleensä sähköpostiviestien avulla, ja sillä on käytössä useita eri tekniikoita havaituksi tulemisen välttämiseksi. Tällä hetkellä sitä käytetään pääasiassa muiden haittaohjelmien lataamiseen uhrien laitteille, ja sen läsnäolo yrityksen tietoverkossa voi tarjota ponnahduslaudan kiristysohjelmahyökkäyksille.

Mobiilitietoturvan touko-kesäkuun isoin uutinen oli SpinOK-haittaohjelma, joka on kerännyt tähän mennessä 421 miljoonaa latausta. Se oli kesäkuun yleisin mobiilihaitake globaalisti. Levinneisyyden takana on haittaohjelman soluttautuminen sovelluskehitystyökaluun (SDK) ja sitä kautta useisiin Android-laitteissa paljon käytettyihin sovelluksiin ja peleihin, joista osa on ladattavissa Google Play Storesta. SpinOK pystyy pitämään silmällä laitteen leikepöytää ja varastamaan laitteelta arkaluontoisia tietoja. Se muodostaa näin ollen vakavan uhan puhelinten käyttäjien yksityisyydelle ja turvallisuudelle, mikä korostaa tarvetta suojata mobiililaitteet ja niiden sisältämät henkilötiedot. Haittaohjelman nopea yleistyminen on myös tarpeellinen muistutus ohjelmistokehityksen toimitusketjuihin liittyvästä hyökkäysriskistä, joka voi olla toteutuessaan tuhoisa.

Kesäkuussa käynnistyi myös laajamittainen kiristyshaittaohjelmakampanja, joka näkyi yrityksissä ja organisaatioissa kautta maailman. Progress Software Corporation havaitsi toukokuussa MOVEit Transfer -tiedostonjako-ohjelmassa ja -pilvipalvelussa nollapäivähaavoittuvuuden, joka mahdollisti luvattoman pääsyn palveluympäristöön. Vaikka haavoittuvuus paikattiin 48 tunnin sisällä, venäläiseen Clop-ryhmään yhdistetyt kyberrikolliset ehtivät käyttää sitä hyväkseen ja käynnistää toimitusketjuhyökkäyksen MOVEit-käyttäjiä vastaan. Tähän mennessä 108 organisaatiota on ilmoittanut joutuneensa hyökkäyksen kohteeksi, mukana seitsemän yhdysvaltalaista yliopistoa. Haavoittuvuuden hyväksikäyttöä on havaittu myös Suomessa.

 

”MOVEit-hyökkäys osoittaa, että vuodesta 2023 on tulossa kiristyshaittaohjelmien kannalta iso vuosi. Clapin tapaiset rikollisryhmät eivät vaivaudu taktisiin operaatioihin yksittäisten uhrien takia vaan tehostavat toimintaansa hyödyntämällä ohjelmistoja, joita käytetään yritysympäristössä laajasti. Näin ne tavoittavat satoja uhreja samalla hyökkäyksellä. Tässä tilanteessa korostuu monikerroksinen kyberturvallisuusstrategian merkitys yrityksille. On myös tärkeää korjata haavoittuvuudet viivyttelemättä niiden paljastuttua”, sanoo Check Point Softwaren tutkimusjohtaja **Maya Horowitz**.

**Suomen yleisimmät haittaohjelmat kesäkuussa 2023:**

1. **Qbot** (eli Qakbot) – Ensimmäisen kerran vuonna 2008 havaittu pankkitroijalainen, joka varastaa uhrin pankkitunnuksia ja tallentaa näppäinpainalluksia. Qbotia levitetään yleensä roskapostiviestien välityksellä. Esiintyvyys 4,37 %.
2. **Remcos** – Etähallintaohjelma (RAT), joka havaittiin ensimmäisen kerran vuonna 2016. Se leviää roskapostien liitteinä olevien Office -tiedostojen avulla ja se on suunniteltu välttämään Microsoftin virustutkat. Esiintyvyys 3,93 %.
3. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 2,62 %.
4. **XMRig** – Monero-kryptovaluutan louhija. Kyberkonnat väärinkäyttävät usein tätä avoimen lähdekoodin ohjelmistoa ja integroivat sen haittaohjelmiin louhiakseen laittomasti uhrien laitteilla. Esiintyvyys 2,18 %.

5.–10. **Injuke**, **NJRat**, **GhOst**, **Formbook**, **Esfury** ja **Zegost** – Kaikkien esiintyvyys 1,31 %.

**Maailman yleisimmät haittaohjelmat kesäkuussa 2023:**

1. **Qbot** (eli **Qakbot**) – Ensimmäisen kerran vuonna 2008 havaittu pankkitroijalainen, joka varastaa uhrin pankkitunnuksia ja tallentaa näppäinpainalluksia. Qbotia levitetään yleensä roskapostiviestien välityksellä. Esiintyvyys 7 %.
2. **Formbook** – Windows-järjestelmien haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 4 %.
3. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 3 %.

**Maailman yleisimmät mobiililaitteiden haittaohjelmat kesäkuussa 2023:**

1. **SpinOk** – Android-laitteiden ohjelmamoduli, joka on koodattu vakoiluohjelmaksi. Se kerää tietoja laitteelle tallennetuista tiedostoista ja pystyy välittämään niitä kyberrikollisille. Toukokuun 23. päivään mennessä haittaohjelma oli löydetty jo yli sadasta Android-sovelluksesta ja se oli ladattu laitteille 421 000 000 kertaa.
2. **Anubis** – Android-laitteille suunnattu Anubis on varustettu kiristysominaisuuksilla, ja se kykenee tallentamaan myös ääntä ja näppäinpainalluksia. Sitä on havaittu sadoissa Google Storen sovelluksissa.

 

3. **AhMyth** – RAT eli etäkäyttötroijalainen havaittiin vuonna 2017. Sitä levitetään sovelluskaupoista ja useilta sivustoilta löytyvissä Android-sovelluksissa. Haittaohjelma pystyy keräämään uhrin laitteelta henkilötietoja sekä tallentamaan näppäilyjä, ottamaan ruutukaappauksia, lähettämään tekstiviestejä ja käyttämään kameraa.

Check Pointin tutkijat listasivat myös kesäkuun käytetyimmät **haavoittuvuudet**. Yleisin haavoittuvuus oli **Web Servers Malicious URL Directory Traversal,** jota on yritetty hyödyntää 51 prosentissa yritysverkoista maailmanlaajuisesti. Toiseksi yleisin oli **Apache Log4j Remote Code Execution (CVE-2021-44228)**, jonka esiintyvyys oli 46 %. Kolmannella sijalla oli **HTTP Headers Remote Code Execution (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756)**, jonka esiintyvyys oli 44 prosenttia.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin tietoihin. ThreatCloud-verkosto kerää reaaliaikaisia tietoja kyberhyökkäyksistä kautta maailman sadoilta miljoonilta antureilta tietoverkoista, päätelaitteista ja puhelimista. Kerätyn tiedon käsittelyssä hyödynnetään tekoälyä ja Check Point Researchin ainutlaatuista tutkimusdataa. Check Point Research on Check Pointin kyberturvatutkimuksesta vastaava osa.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista: June 23's Most Wanted Malware

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa https://www.checkpoint.com/.

**Lisätiedot:**
Viivi Tynjälä, Country Manager, Finland and Baltics, Check Point Software Technologies, viivit@checkpoint.com, p. 0400 411 530.

**Haastattelu- ja kuvapyynnöt:**
Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065.

**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

**Check Point Research**
Check Point Research (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. (https://www.checkpoint.com/) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Check Point Infinityn ratkaisuportfolio suojaa yrityksiä ja julkisia organisaatioita 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Infinity koostuu neljästä peruspilarista: Check Point Harmony etäkäyttäjille; Check Point CloudGuard pilven automaattiseen suojaamiseen; ja Check Point Quantum tietoverkkojen ja datakeskusten suojaamiseen. Näitä kaikkia hallitaan alan kattavimmalla ja intuitiivisimmalla yhtenäisellä hallintajärjestelmällä; Check Point Horizonilla, joka on

 

tietoturvapoikkeamien ennaltaehkäisyyn tähtäävä ohjelmisto- ja palvelukokonaisuus. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

 