**Emotet-bottiverkko syöksee jälleen roskapostia uhrien laitteille – kolmen kuukauden hiljaisuus päättyi**

*Check Pointin tietoturvatutkijat ovat havainneet, että tunnettu bottiverkko on jälleen voimissaan ja levittää mainoskampanjoja kuin ei olisi koskaan kesälomalla ollutkaan.*

**ESPOO – 11. lokakuuta 2019 –** Tietoturvayhtiö Check Pointin tutkimustoiminnasta vastaava Check Point Research kertoo uusimmassa haittaohjelmakatsauksessaan, että Emotet-bottiverkko oli kolmen kuukauden hiljaisuuden jälkeen jälleen hyvässä vauhdissa syyskuussa. Meneillään oli useita roskapostikampanjoja, joiden toteutuksessa se oli mukana.

Osassa Emotet-kampanjointiin kuuluvista sähköposteista oli linkki, jota klikkaamalla uhrin koneelle latautui haitallinen Word-tekstitiedosto. Osassa viesteistä haitallinen tiedosto oli liitteenä. Kun tiedosto avattiin, se pyysi uhria mahdollistamaan tiedoston makrot, jotka sitten latasivat Emotet-haittaohjelman uhrin tietokoneelle. Emotet oli syyskuussa maailman viidenneksi yleisin haittaohjelma. Suomen listalla se oli kuudes.

”Meille ei ole selvinnyt, miksi Emotet piti lomaa kolmen kuukauden ajan, mutta oletamme, että sen kehittäjät päivittivät sen ominaisuuksia. On tärkeää, että organisaatiot muistuttavat työntekijöitään kalasteluviestien riskeistä ja varoittavat avaamasta epäilyttävistä osoitteista tulevien sähköpostiviestien liitteitä tai klikkaamasta niiden linkkejä. Myös uusimman sukupolven haittaohjelmaratkaisu, joka seuloo epäilyttävät viestit ennen kuin ne lähtevät vastaanottajalle, on hyödyllinen”, kommentoi Check Pointin tutkijaryhmän vetäjä **Maya Horowitz**.

**Suomen yleisimmät haittaohjelmat syyskuussa 2019:**

1. JSecoin – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 13 %.
2. Formbook – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 7 %.
3. XMRig – Monero-kryptovaluutan louhija. Esiintyvyys 7 %.
4. TrickBot – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 5 %.
5. Phoenix – Esiintyvyys 4 %.
6. Emotet – Moderni troijalainen, joka on taitava piiloutumaan. Leviää myös sähköpostien kautta. Esiintyvyys 4 %.
7. Cryptoloot – Kryptolouhija. Esiintyvyys 4 %.
8. Chir – Esiintyvyys 3 %.
9. Loyeetro – Esiintyvyys 3 %.
10. Bonzo – Esiintyvyys 2 %.

Dealply – Esiintyvyys 2 %.

**Maailman yleisimmät haittaohjelmat syyskuussa 2019:**

1. Jsecoin – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa.
2. XMRig – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan.
3. Agentesla – Kehittynyt RAT-haittaohjelma, joka tallentaa näppäintoimintoja ja varastaa salasanoja. Pystyy myös ottamaan kuvakaappauksia.

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli syyskuussa **Lotoor**, joka on Android-laitteiden haavoittuvuuksia hyödyntävä hakkerityökalu. Kakkoseksi kohosi **AdroidBauts**, joka pystyy välittämään eteenpäin monia laitteen tietoja sekä lataamaan laitteelle mainoksia, sovelluksia ja oikoteitä. Kolmanneksi yleisin mobiilihaittaohjelma oli **Hiddad**, joka pakkaa sovelluksia uudelleen ja tarjoaa niitä kolmannen osapuolen sovelluskaupassa. Se levittää pääasiassa mainoksia ja muuta roskapostia, mutta pystyy myös ohittamaan tiettyjä käyttöjärjestelmän turvaportteja, jolloin hyökkääjä voi päästä käsiksi arkaluontoiseen aineistoon.

Check Pointin tutkijat listasivat myös syyskuun **käytetyimmät haavoittuvuudet**. **MVPower DVR Remote Code Execution** johti tällä kertaa listaa 37 prosentin esiintyvyydellä yritysverkoissa. **The Linux System Files Information Disclosure** -haavoittuvuus oli seuraavaksi yleisin, ja kolmanneksi ylsi **Web Server Exposed Git Repository Information Disclosure.** Ero oli hiuksenhieno, ja molempien esiintyvyys oli 35 %.

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/2019/10/10/september-2019s-most-wanted-malware-emotet-botnet-starts-spreading-spam-campaigns-again-after-three-month-silence/).

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](mailto:ramira@checkpoint.com)

Maija Rauha, viestintäkonsultti, OSG Viestintä, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065

**Seuraa Check Point Researchia:**

Blogi: <https://research.checkpoint.com/>

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

**Check Point Research**

Check Point Research 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.