**IoT-laitteista kerätään bottiverkkoa uudella haittaohjelmalla – odotettavissa palvelunestohyökkäyksiä ja roskapostikampanjoja**

*Check Pointin tietoturvatutkijat varoittavat uudesta haittaohjelmasta, joka pyrki ahkerasti tartuttamaan IoT-laitteita elokuussa. Echobot on vuonna 2016 Suomessakin ongelmia aiheuttaneen Mirain uusi versio.*

**ESPOO – 13. syyskuuta 2019 –** Tietoturvayhtiö Check Pointin tutkimustoiminnasta vastaava Check Point Research varoittaa uusimmassa haittaohjelmakatsauksessaan Mirai-IoT-bottiverkon uudesta versiosta nimeltä Echobot. Mirai tartutti Suomessa vuonna 2016 arviolta 10 000 modeemia ja sai verkkoyhteydet pätkimään monin paikoin. Bottiverkkoja käytetään yleisimmin palvelunestohyökkäyksiin, joilla pyritään rampauttamaan yritysten ja organisaatioiden verkkopalveluja.

Echobot pyrkii saamaan etähallintaan useita erityyppisiä IoT-latteita ja kokoamaan niistä tuhovoimaisen verkoston. Se on hyödyntänyt tähän mennessä jo yli 50 eri haavoittuvuutta, vaikka se havaittiin ensimmäisen kerran vasta toukokuussa. Useimmin se on pyrkinyt käyttämään haavoittuvuutta nimeltä Command Injection Over HTTP. Tämän portin pitävyyttä on koeteltu 34 prosentissa Check Pointin globaaliin verkostoon kuuluvista yrityksistä ja organisaatioista.

Myös alkuvuoden isoin ja aktiivisin bottiverkko, Emotet, osoitti elokuussa elpymisen merkkejä kahden kuukauden tauon jälkeen. On todennäköistä, että Emotetia käytetään uuteen roskapostikampanjaan lähiaikoina.

”Havaitsimme Echobotin ensimmäisen kerran toukokuun puolivälissä ja aloimme seurata sitä, koska se on pahamaineisen Mirain uusi versio. Echobotista on saatu havaintoja 34 prosentissa yrityksistä kautta maailman. Tämä osoittaa jälleen kerran, miten tärkeää on päivittää kaikki yritysverkot, ohjelmistot ja IoT-laitteet uusimpaan version heti sen ilmestyessä, kommentoi Check Pointin tutkimusjohtaja **Maya Horowitz.**

**Suomen yleisimmät haittaohjelmat elokuussa 2019:**

1. JSecoin – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 13 %.
2. TrickBot – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 6 %.
3. XMRig – Monero-kryptovaluutan louhija. Esiintyvyys 6 %.
4. Emotet – Moderni troijalainen, joka on taitava piiloutumaan. Leviää myös sähköpostien kautta. Esiintyvyys 4 %.
5. Formbook – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 4 %.
6. Shiz – Haittaohjelma, joka kätkeytyy Windows-ohjelmiin ja pyrkii varastamaan käyttäjän tietoja. Esiintyvyys 2 %.
7. Loud Miner – Kryptolouhija. Esiintyvyys 2 %.
8. MobiDash – Esiintyvyys 2 %.
9. Tinba – Pankkitroijalainen. Esiintyvyys 2 %.
10. Dealply, Scar ja DttLoader – Kaikkien esiintyvyys 1 %.

**Maailman yleisimmät haittaohjelmat elokuussa 2019:**

1. XMRig – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan.
2. Jsecoin – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa.
3. Dorkbot – IRC-pohjainen mato, joka mahdollistaa laitteen ottamisen etähallintaan ja muiden haittaohjelmien lataamisen laitteelle.

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli elokuussa **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 mobiilihaittaojelma oli **Triada**, joka antaa tunkeutujalle pääkäyttäjän oikeudet Android-laitteeseen. Järjestys oli sama kuin heinäkuussa.

Check Pointin tutkijat listasivat myös elokuun **käytetyimmät haavoittuvuudet**. **SQL-injektiotekniikka** johti kolmannen kerran peräkkäin hyödynnetyimpien haavoittuvuuksien listaa 39 prosentin esiintyvyydellä yritysverkoissa. **OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)** oli heinäkuun toiseksi hyödynnetyin haavoittuvuus samalla eli 39 prosentin esiintyvyydellä, ja kolmanneksi kohosi **MVPower DVR Remote Code Execution**, jonka esiintyvyys oli 38 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.

Täydellinen Top 10 -haittaohjelmalista löytyy [Check Pointin blogista](https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/).

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 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 tietoturvahteisöllä 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.