**Bottiverkon lonkerot leviävät IoT-laitteisiin**

*Tietoturvayhtiö Check Pointin tutkijat kertovat myös uudesta SMS-tietojenkalastelukampanjasta, joka levittää haittaohjelma Emotetia.*

**ESPOO – 11. maaliskuuta 2020 –** Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research kertoo haittaohjelmakatsauksessaan, että hyökkäykset Mirai-bottiverkolle alttiisiin haavoittuvuuksiin lisääntyivät helmikuussa huomattavasti.

Mirai-bottiverkko on tunnettu IoT (Internet of Things) -laitteiden tartuttamisesta ja massiivisista DDoS-hyökkäyksistä. Haavoittuvuus, joka tunnetaan nimellä “PHP php-cgi Query String Parameter Code Execution”, oli helmikuun kuudenneksi hyödynnetyin. Se vaikutti 20 prosenttiin organisaatioista ympäri maailmaa, luvun ollessa tammikuussa kaksi prosenttia.

Tutkijat varoittavat organisaatioita myös Emotetista, joka oli kuukauden toiseksi käytetyin haittaohjelma ja tällä hetkellä yleisin bottiverkko. Se on levinnyt helmikuussa kahdella uudella vektorilla. Näistä ensimmäinen oli amerikkalaiskäyttäjille suunnattu SMS-tietojenkalastelukampanja. Siinä tekstiviesti jäljittelee tunnettujen pankkien viestejä ja houkuttaa uhrit klikkaamaan haitallista linkkiä, joka lataa laitteeseen Emotet-haittaohjelman. Toinen vektori oli Emotet, joka havaitsee ja hyödyntää lähellä olevia Wi-Fi-verkkoja. Se pyrkii leviämään väsytyshyökkäyksillä, joissa kokeillaan erilaisia ​​yleisesti käytettyjä Wi-Fi-salasanoja. Sovellusta käytetään ensisijaisesti kiristys- ja muiden haittaohjelmien jakeluun.

Emotet esiintyi helmikuussa seitsemässä prosentissa organisaatioista maailmanlaajuisesti, määrän ollessa tammikuussa 13 prosenttia. Silloin sitä levitettiin esimerkiksi koronavirusaiheisten roskapostikampanjoiden kautta. Tämä osoittaa, kuinka nopeasti kyberrikolliset muuttavat hyökkäystensä aiheita ja yrittävät näin maksimoida tartuntojen määrän.

”Helmikuun merkittävimmät uhat olivat monipuolisia haittaohjelmia, kuten XMRig ja Emotet. Rikolliset pyrkivät rakentamaan mahdollisimman laajan tartunnan saaneiden laitteiden verkoston. He hyödyntävät sitä ansaintatarkoituksessa monin tavoin kiristysohjelmista DDoS-hyökkäyksiin”, kertoo Check Pointin Threat Intelligence & Research, Products -ryhmän johtaja **Maya Horowitz**.

 "Koska tärkeimmät tartunnanlevittäjät ovat sähköpostiviestit ja tekstiviestit, organisaatioiden tulisi opastaa työntekijöitään tunnistamaan erityyppiset haitalliset roskapostit. Niiden tulisi myös ottaa käyttöön tietoturva, joka estää aktiivisesti näitä uhkia tarttumasta verkkoon”, hän jatkaa.

Suomessa helmikuun yleisin haittaohjelma oli RiGEK, jota esiintyi noin yhdeksässä prosentissa yritysverkoista. RigEK käyttää Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksia. Tartuntaketju alkaa uudelleenohjauksella aloitussivulle, joka sisältää haavoittuvat plug-init tarkistavan JavaScriptin.

Toisella sijalla oli kryptovaluutan louhija XMRig.

**Suomen yleisimmät haittaohjelmat helmikuussa 2020:**

1. **RigEK** – Haittaohjelmien lataaja Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksissa. Esiintyvyys 8,93 %.
2. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 8.48 %.
3. **Jsecoin** – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 4,91 %.
4. **TrickBot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 4,91 %.
5. **Hiddad** – Android-haittaohjelma, joka pakkaa sovelluksia uudelleen ja laittaa ne tarjolle kolmannen osapuolen sovelluskauppaan. Esiintyvyys 3,57 %.
6. **Bonzo.** Esiintyvyys 2,23 %.
7. **Remcos** – Jakaa haittaohjelmia roskaposteihin liitettyjen Microsoft Office -asiakirjojen kautta. Esiintyvyys 1,79 %.
8. **Scar**. Troijalainen, joka varastaa käyttäjän kirjautumistiedot eri verkkosivustoilta ja lataa lisää haittaohjelmia. Esiintyvyys 1,79 %.
9. **Ewind**. Esiintyvyys 1,34 %.
10. **Ramnit**. – Mato, joka leviää pääasiassa ulkoisten kovalevyjen ja avoimien FTP-palvelinten kautta. Mato luo itsestään kopion ja tartuttaa laitteen ulkoiset ja sisäiset muistit. Esiintyvyys 1,34 %.

**Maailman yleisimmät haittaohjelmat ja haavoittuvuudet helmikuussa 2020:**

1. **XMRig** – Avoimen lähdekoodin louhintaohjelma, jota käytetään Moneron louhintaan. Esiintyvyys 7 %.
2. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään nykyään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 6 %.
3. **Jsecoin** – Verkkosivuille upotettava kryptovaluutan louhintaohjelma. Esiintyvyys 5 %.

**Mobiilihaittaohjelmien** globaalilla listalla ykkösenä oli helmikuussa **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta ja asentamaan itsensä uudelleen, jos käyttäjä poistaa sen. Toiseksi yleisin oli Android-haittaohjelma **Hiddad**, joka pakkaa sovelluksia uudelleen ja laittaa ne tarjolle kolmannen osapuolen sovelluskauppaan. Kolmannella sijalla oli muita haittaohjelmia Android-puhelimille lataava **Guerrilla**, joka on onnistuttu upottamaan useisiin sovelluksiin. Troijalainen tuottaa vilpillisiä mainostuloja sovelluskehittäjille.

Check Pointin tutkijat listasivat myös helmikuun käytetyimmät **haavoittuvuudet**. Luettelon kärjessä oli **“MVPower DVR Remote Code Execution”**, jota esiintyi 31 prosentissa yritysverkoista maailmanlaajuisesti. Toiseksi yleisin oli **“OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)”**, esiintyvyys 28 prosenttia. Kolmannella sijalla oli **“PHP DIESCAN information disclosure”**, esiintyvyys 27 prosenttia.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. ThreatCloud-tietokanta tarkastaa yli 2,5 miljardia verkkosivustoa ja 500 miljoonaa tiedostoa sekä tunnistaa yli 250 miljoonaa haittaohjelmatoimintaa päivittäin.

Täydellinen Top 10 -haittaohjelmalista löytyy [Check Pointin blogista](https://blog.checkpoint.com/2020/03/11/february-2020s-most-wanted-malware-increase-in-exploits-spreading-the-mirai-botnet-to-iot-devices/).

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa [www.checkpoint.com](http://www.checkpoint.com).

**Lisätiedot:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com.
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

**Seuraa Check Point Researchia:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**Check Point Research**

Check Point Research ([research.checkpoint.com](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. ([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.