Kesäkuun haittaohjelmakatsaus: Emotetin hiljaiseloon ei kannata tuudittautua

Check Pointin tietoturvatutkijat kertovat, että Emotet-bottiverkko vietti hiljaiseloa suurimman osan kesäkuusta, mutta saattaa palata takaisin uusien haittaominaisuuksien kera.

ESPOO – 15. heinäkuuta 2019 -- Tietoturvayhtiö Check Pointin tutkijaryhmä kertoo, että suurin toiminnassa oleva bottiverkko Emotet pysyi kesäkuussa pääosin passiivisena eikä sen tekemiä hyökkäyksiä juurikaan tavattu. Koko vuoden ensimmäisen puoliskon Emotet pysyi globaalin haittaohjelmalistauksen viiden kärjessä massiivisten roskapostikampanjoidensa myötä.

Check Pointin tutkijat uskovat, että Emotet on laitettu telakalle huolto- ja päivitystoimenpiteiden ajaksi, mutta on jälleen aktivoituessaan entistä suurempi uhkatekijä.

“Emotet on vuodesta 2014 tullut laajalti tutuksi pankkitroijalaisena, mutta viime vuodesta lähtien sitä on käytetty myös bottiverkkona laajoissa roskapostikampanjoissa sekä muiden haittaohjelmien jakamisessa. Vaikka Emotet olikin kesäkuussa pääosin passiivisena, se oli silti viidentenä globaalissa haittaohjelmalistauksessamme, mikä kertoo sen yleisyydestä. On hyvin todennäköistä, että Emotet palaa vielä uusien haittaominaisuuksien kera”, sanoo Check Pointin Threat Intelligence and Research Director **Maya Horowitz**.

“Kun Emotet on kerran asennettu koneelle, se kykenee levittämään itseään roskapostikampanjoiden kautta, lataamaan koneelle muita haittaohjelmia (kuten Trickbotin, joka puolestaan saastuttaa koko isäntäverkon pahamaineisella Ryuk-kiristyshaittaohjelmalla) sekä tunkeutumaan verkon muihinkin jäseniin.”

Suomen yleisimmät haittaohjelmat kesäkuussa 2019:

1. Jsecoin – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa. Esiintyvyys 6 % organisaatioista.
2. Emotet – Kehittynyt, itsemonistuva ja modulaarinen troijalainen. Tullut laajalti tutuksi pankkitroijalaisena, mutta viime vuodesta lähtien sitä on käytetty myös bottiverkkona laajoissa roskapostikampanjoissa sekä muiden haittaohjelmien jakamisessa. Esiintyvyys 6 %.
3. Formbook – Windows-käyttöjärjestelmiin kohdistuva InfoStealer, joka tunnistettiin ensi kertaa vuonna 2016. Muun muassa kerää verkkoselainten kirjautumistietoja, ruutukaappauksia ja näppäimistön painalluksia. Esiintyvyys 5 %.
4. Cryptoloot – Kryptovaluutan louhija, joka käyttää hyödykseen uhrin suorittimen ja näytönohjaimen tehoja. Esiintyvyys 4 %.
5. XMRig – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017. Esiintyvyys 4 %.
6. Bundler, 7. Scar, 8. Ramnit, 9. Babilon 10. Trickbot, Gandcrab ja Typum

Maailman yleisimmät haittaohjelmat kesäkuussa 2019 Top 3:

1. XMRig – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017.
2. Jsecoin – Louhintaohjelma, joka on mahdollista upottaa verkkosivulle. Sivuston käyttäjä voi halutessaan esimerkiksi ostaa pelirahaa louhimalla kryptovaluuttaa.
3. Cryptoloot – Kryptovaluutan louhija, joka käyttää hyödykseen uhrin suorittimen ja näytönohjaimen tehoja.
4. Dorkbot, 5. Emotet, 6. Ramnit, 7. Hawkeye, 8. Nanocore, 9. Formbook, 10. Trickbot

Mobiilihaittaohjelmien globaalilla listalla ykkösenä oli **Lotoor**, joka on Android-laitteiden haavoittuvuuksia hyödyntävä hakkerityökalu. Kakkoseksi kohosi **Triada**, Android-laitteiden takaovi, jonka avulla hyökkääjä saa laitteen pääkäyttäjäoikeudet. Kolmanneksi yleisin mobiilihaittaojelma **Ztorg** taas on troijalainen, joka hankkii Android-laitteella laajat käyttäjäoikeudet ja kykenee asentamaan itsenä lisäksi myös muita sovelluksia laitteelle.

Check Pointin tutkijat listasivat myös käytetyimmät haavoittuvuudet. Kesäkuussa kärkipaikkaa piti edelleen **SQL-injektiotekniikka** 52 prosentin esiintyvyydellä. **OpenSSL TLS DTLS Heartbeat Information Disclosure** oli kesäkuun toiseksi hyödynnetyin haavoittuvuus 43 prosentin esiintyvyydellä, ja kolmanneksi kohosi **Joomla Object Injection Remote Command Execution**, jonka esiintyvyys oli 41 prosenttia organisaatioista kautta maailman.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin™ 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 osoitteesta:
https://blog.checkpoint.com/2019/07/09/june-2019s-most-wanted-malware-emotet-crypto-malware-mining-xmrig/

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) 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.

