**Kyberrikolliset keräsivät heinäkuussa bottiverkkoja digibokseista ja videotallentimista**

*Check Pointin tietoturvatutkijat kertovat, että vasta löydetty haavoittuvuus Open DreamBox 2.0.0. Web Admin -laajennuksessa oli erittäin hyödynnetty heinäkuussa. Peräti 32 prosentissa Check Pointin globaaliin verkostoon kuuluvista yrityksistä koettiin hyökkäysyritys tätä kautta.*

**ESPOO – 14. elokuuta 2019 –** Tietoturvayhtiö Check Pointin tutkijaryhmä varoittaa Dream Multimedian DreamBox-digiboksien ohjelmistosta löytyneestä haavoittuvuudesta, joka mahdollistaa hyökkääjälle laitteen etähallinnan ja esimerkiksi sen liittämisen bottiverkkoon. Haavoittuvuus nousi heinäkuussa useimmin hyödynnettyjen haavoittuvuuksien Top 10 -listalla sijalle 8.

Vaaravyöhykkeessä olivat myös muut IoT-laitteet. Kuukauden kolmanneksi hyödynnetyin haavoittuvuus, MVPower DVR Remote Code Execution, sijaitsee digitaalisen videotallentimen ohjelmistossa. Tiedetään, että laitteita on liitetty pahamaineiseen Mirai-bottiverkkoon tätä haavoittuvuutta hyödyntämällä.

”Hyökkääjät ovat nopeita hyödyntämään haavoittuvuuksia heti niiden löytämisen jälkeen. Heillä on tavoitteena ehtiä ennen kuin käyttäjät päivittävät ohjelmistonsa uuteen, korjattuun versioon. Siltikin on yllättävää, että kolmannes yrityksistä joutui heti hyökkäyksen kohteeksi. Haavoittuvuuksien nopea paikkaaminen ja ohjelmistojen päivitys on yrityksille ja organisaatioille hyvin tärkeä tapa suojata itseään”, sanoi Check Pointin tutkimusjohtaja **Maya Horowitz**.

Toinen tärkeä heinäkuun tapahtuma oli Cryptoloot-louhintaohjelman putoaminen haittaohjelmien 10 kärjessä -listan sijalle 10. Vielä kesäkuussa se oli listakolmonen.

”Ilmiö on mielenkiintoinen. Cryptoloot on hallinnut haittaohjelmien listaa puolentoista vuoden ajan, ja tämän vuoden ensimmäisellä puoliskolla se oli maailman toiseksi yleisin haittaohjelma. Cryptolootin tärkein kilpailija, Coinhive, lopetti toimintansa alkuvuonna, ja uskomme, että nämä asiat liittyvät yhteen. Kyberrikolliset luottavat nyt enemmän XMRigin ja Jsecoinin kaltaisiin kryptolouhijoihin”, Horowitz kommentoi.

**Suomen yleisimmät haittaohjelmat heinäkuussa 2019:**

1. Jacksbot – Troijalainen, jonka avulla laite voidaan ottaa etähallintaan ja liittää bottiverkkoon. Tunnetaan myös nimellä JRat. Esiintyvyys 8 %.
2. AgentTesla – Verkossa myynnissä oleva haittaohjelma, jonka avulla voi muun muassa seurata ja tallentaa uhrin näppäintoimintoja ja leikepöytää sekä ottaa näyttökaappauksia. Esiintyvyys 6 %.
3. Lokibot– Pääasiassa kalastelusähköpostien kautta levitettävä salasanakaappari. Esiintyvyys 6 %.
4. Emotet – Moderni troijalainen, joka on taitava piiloutumaan. Leviää myös sähköpostien kautta. Esiintyvyys 6 %.
5. Nanocore – Troijalainen, jonka tavoitteena on uhrin laitteen luovuttaminen etähallintaan. Esiintyvyys 6 %.
6. Formbook 7. Jsecoin 8. XMRig, 9. Trickbot, 10. Scar

**Maailman yleisimmät haittaohjelmat heinäkuussa 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 heinäkuussa **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 mainoshaittaohjelma **Piom**, joka seuraa käyttäjän selaintoimintoja ja lähettää sen perusteella valitsemiaan mainoksia laitteelle.

Check Pointin tutkijat listasivat myös heinäkuun **käytetyimmät haavoittuvuudet**. **SQL-injektiotekniikka** johti toisen kerran peräkkäin hyödynnetyimpien haavoittuvuuksien listaa 46 prosentin esiintyvyydellä yritysverkoissa. **OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)** oli heinäkuun toiseksi hyödynnetyin haavoittuvuus 41 prosentin esiintyvyydellä, ja kolmanneksi kohosi **MVPower DVR Remote Code Execution**, jonka esiintyvyys oli 40 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/2019/08/08/july-2019s-most-wanted-malware-vulnerability-in-opendreambox-2-0-0-webadmin-plugin-enables-attackers-to-execute-commands-remotely/>

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 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](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.