**Check Pointin haittaohjelmakatsaus 5/2017**

**Pommitus hyökkäystä valmistelevilla EK-haittaohjelmilla jatkui tavallista voimakkaampana huhtikuussa**

*Slammer-mato kohosi epätoivottujen vieraiden listaykköseksi.*

**CPX MILANO, Italia – keskiviikkona 17. toukokuuta 2017 –** Check Pointin havaintojen mukaan kyberhyökkäysten valmisteluun käytetyt Exploit Kit -haittaohjelmat yleistyivät yritysverkoissa entisestään huhtikuussa. Jo maaliskuussa EK-tartuntoja oli globaalisti poikkeuksellisen paljon. Huhtikuun yleisin haittaohjelma oli Rig EK.

Exploit Kitit on suunniteltu etsimään ja hyödyntämään laitteiden haavoittuvuuksia, jotta niille voidaan ladata muita haittaohjelmia. EK-ohjelmien käyttö oli pitkään laskusuunnassa, kunnes Rig EK ja Terror EK palasivat maaliskuussa listakärkeen. Kolmas uudelleen henkiin herännyt tuttavuus on Slammer-mato, joka nousi kansainvälisen haittaohjelmalistan kolmoseksi.

”Vanhat, mutta tehokkaiksi todetut haittaohjelmat eivät katoa minnekään. Ne palaavat usein takaisin varustettuna jollakin uudella kommervenkillä, joka tekee niistä jälleen vaarallisia. Kolmen vanhan ohjelman uuden nousun tulisi toimia varoituksena yrityksille ja organisaatioille. Niiden tulee pysyä jatkuvasti valppaina ja hyödyntää modernia tietoturvaa, joka antaa suojan laajaa haittaohjelmien kirjoa vastaan”, Check Pointin VP of Emerging Products **Nathan Shuchami** sanoi.

**Yleisimmät haittaohjelmat huhtikuussa top 10, Suomi**

1. Rig EK

2. Zeus

3. Slammer

4. HackerDefender

5. Hiddad

6. Business

7. Darkness

8. Sality

9. Blandabindy

10. Tupym

**Yleisimmät haittaohjelmat huhtikuussa top 3, koko maailma**

1. **Rig EK**: Vuonna 2014 löydetty haittaohjelma, joka etsii haavoittuvuuksia Flash-, Java-, Silverlight- ja Internet Explorer -ohjelmista. Hyökkäys tapahtuu niin, että kyberrikolliset murtavat verkkosivuja ja asentavat niille haitallisen uudelleenohjauksen. Uhri ohjautuu turvalliseksi luulemaltaan sivulta rikollisten sivulle. Tämä sivu sisältää varsinaisen exploit kitin, joka tutkii uhrin koneen ja havaittuaan haavoittuvuuden murtautuu sisään.

**2. HackerDefender:** Windows-ohjelmistojen rootkit-tuholainen, jota voidaan käyttää tiedostojen, prosessien ja rekisteriavainten piilottamiseen. Se osaa myös luoda ohjelmistoon takaoven, jota perinteinen tietoturva ei havaitse.

**3. Slammer:** Alun perinMicrosoft SQL 2000:ta varten kehitetty mato, joka leviää erittäin nopeasti aiheuttaen kohteeseen DDoS-hyökkäyksen kaltaisen tilanteen.

**Yleisimmät mobiililaitteiden haittaohjelmat huhtikuussa top 3, koko maailma**

**1. Hiddad:** Android-haittaohjelma, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia, mutta pystyy myös nappaamaan puhelimen käyttäjätietoja.

**2. HummingBad:** Sitkeä Android-laitteiden rootkit-haittaohjelma, joka asentaa haitallisia sovelluksia ja pystyy pienin muutoksin tekemään paljon muutakin, kuten asentamaan näppäilyntallentimen, varastamaan tilitietoja ja ohittamaan suojatut sähköpostisäiliöt.

**3. Lotoor:** Hakkerityökalu, joka hyödyntää Android-käyttöjärjestelmän haavoittuvuuksia saadakseen pääkäyttäjän oikeudet laitteella.

Koko lista löytyy Check Pointin blogista: [Check Point Blog](http://blog.checkpoint.com)

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.

Check Pointin uhkakartta näyttää kyberhyökkäykset reaaliaikaisesti: [ThreatCloud World Cyber Threat Map](https://www.threat-cloud.com/ThreatPortal/#/map)

Katso täältä, kun haluat tietää, mitä mikäkin haittaohjelma tekee: [Check Point ThreatWiki](https://threatwiki.checkpoint.com/threatwiki/public.htm)

Tietoja Check Pointin uhkientorjuntaresursseista: [Threat-prevention-resources](http://www.checkpoint.com/threat-prevention-resources/index.html)

Check Pointin tietoturvatiimin blogi: [Check Point Blog](http://blog.checkpoint.com)

**Lisätiedot ja haastattelupyynnöt:**

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

**Seuraa Check Pointia:**

Check Pointin blogi: <http://blog.checkpoint.com/>

Twitter: [www.twitter.com/checkpointsw](http://www.twitter.com/checkpointsw)

Facebook: <https://www.facebook.com/checkpointsoftware>

YouTube: <http://www.youtube.com/user/CPGlobal>

**About Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.