**Check Pointin haittaohjelmakatsaus 4/2017**

Hyökkäystä valmistelevat haittaohjelmat yleistyivät räjähdysmäisesti

*Exploit Kit (EK) on monikäyttöinen haittaohjelmatyyppi, jolla kyberrikolliset valmistelevat esimerkiksi kiristyshaittaohjelmien hyökkäyksiä. Haitaketyyppi yleistyi maaliskuussa voimakkaasti sekä maailmalla että Suomessa.*

**Espoo, 20. huhtikuuta 2017 –** Tietoturvayhtiö Check Pointin kansainvälisellä haittaohjelmien listalla EK-tartunnat nousivat pitkän tauon jälkeen sijoille 2 ja 11. Suomessa Rig EK oli maaliskuun yleisin ja Terror EK toiseksi yleisin yritysverkoista tavattu haittaohjelma.

Exploit Kit valmistelee tietä muille haittaohjelmille etsimällä laitteilta haavoittuvuuksia. Rig etsii ja hyödyntää Flash-, Java- ja Silverlight-ohjelmien sekä Internet Explorer -selaimen haavoittuvuuksia. Terror on uusi, vasta viime joulukuussa löydetty haittaohjelma. Molempien on havaittu levittävän laajaa haitakevalikoimaa roskapostin lähettäjistä ja bitcoin-louhijoista lähtien pankkitroijalaisiin ja kiristyshaittaohjelmiin asti.

Check Pointin tietoturvatutkijat arvioivat, että kiristyshaittaohjelmat olivat viime vuonna yksi kyberrikollisten tuottoisimmista työvälineistä. Hyökkäykset ovat tuskin ainakaan vähenemään päin, kun niitä nyt valmistellaan Exploit Kiteillä.

”EK-haittaohjelmatyypin dramaattinen uusi sisääntulo osoittaa, etteivät vanhatkaan tietoturvan uhat katoa lopullisesti näyttämöltä, vaan kyberrikolliset hyödyntävät niitä kehittäessään uusia työvälineitä. Onhan se nopeampaa kuin haittaohjelman luominen alusta asti. Exploit Kit on erityisen joustava haittaohjelmatyyppi, jota on helppo muokata”, kommentoi Check Pointin VP of Emerging Products **Nathan Shuchami.**

Rigiltä, Terrorilta ja muilta EK-ohjelmilta suojautumiseen vaaditaan perinteistä laajempi ja kehittyneempi tietoturvaratkaisu, joka pitää koko yritysverkon turvassa mobiililaitteet mukaan lukien. Hyvä valinta on Check Pointin SandBlast™ Zero-Day Protection täydennettynä Mobile Threat Prevention -ratkaisulla.

**Yleisimmät haittaohjelmat helmikuussa top 10, Suomi**

1. Rig EK

2. Terror EK

3. Hiddad

4. Zeus

5. Redkit

6. HackerDefender

7. BadJoke

8. Slammer

9. Tupym

10. Hancitor

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

1. HackerDefender

2. Rig EK

3. Conficker

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

1. Hiddad

2. HummingBad

3. Ztorg

Koko lista löytyy Check Pointin blogista: <http://blog.checkpoint.com/2017/04/13/marchs-wanted-malware-list-exploit-kits-rise-popularity/>

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, 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>

**Check Point Software Technologies Ltd.**
Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin yksinomaan kyberturvallisuustuotteisiin keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, joiden kyky havaita haittaohjelmat ja muut tunkeutujat sekä suojata asiakkaat kyberhyökkäyksiltä on ainutlaatuisen tehokas. Check Pointin täydellisen kattava tietoturva-arkkitehtuuri suojaa niin yritysverkot kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava sekä intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.