Check Point
SOFTWARE TECHNOLOGIES LTD.

WE SECURE THE FUTURE

Haittaohjelmakatsaus 5/2017 – Fireball levisi kulovalkean tavoin

Keskiviikkona 21. kesäkuuta 2017 – Check Pointin havaintojen mukaan kulovalkean tavoin maailmalla keväällä levinnyt Fireball-haittaohjelma nousi toukokuussa yleisemmät haittaohjelmat top 10 -tilaston kärkeen Suomessa ja maailmalla.

Check Point kertoi aiemmin tässä kuussa, että Fireball oli saastuttanut yli 250 miljoonaa konetta ja peräti viidenneksen maailman yritysverkoista ja leviäminen on sittemmin jatkunut. Fireball kaappaa haltuunsa kohde-selaimet ja muuttaa ne zombeiksi, joita se käyttää muun muassa lisähaittaohjelmien lataamiseen ja arvokkaiden tunnistetietojen varastamiseen.

Toukokuun listauksen toisella sijalla Suomessa ja maailmalla oli RoughTed. Kyseessä on laajamittainen malvertising-kampanja, jota on käytetty erilaisten haitallisten sivustojen, adwaren, exploit kittien ja muiden haitakkeiden levittämiseen. Sitä voidaan käyttää kaikentyyppisiin alustoihin ja käyttöjärjestelmiin kohdistuvissa hyökkäyksissä.

Kolmanneksi yleisin haittaohjelma Suomessa oli pitkään listan kärkisijoilla lymyillyt Rig ek, Exploit Kit -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.

Yleisimmät haittaohjelmat toukokuussa 2017 top 10, Suomi

1. Fireball
2. RoughTed
3. Rig ek
4. Slammer

5. Zeus
6. Nivdort
7. HackerDefender
8. BadJoke
9. Tupym
10. Emotet

Yleisimmät haittaohjelmat toukokuussa 2017 top 3, koko maailma

1. ↑ **Fireball – Selainkaappausohjelma, joka voi muuntautua malware downloader -ohjelmaksi.** Fireball kaappaa haltuunsa kohde-selaimet ja muuttaa ne zombeiksi, joita se käyttää muun muassa lisähaittaohjelmien lataamiseen ja arvokkaiden tunnistetietojen varastamiseen

2. ↑ **RoughTed** – Laajamittainen malvertising-kampanja, jota on käytetty erilaisten haitallisten sivustojen, adwaren, exploit kittien ja muiden haitakkeiden levittämiseen.

3. ↑ **WannaCry** – on historian levinnein kiristyshaittaohjelma, joka saastutti miljoonia koneita toukokuun aikana. WannaCry höydyntää Windows SMB -haavoittuvuutta, nimeltään EternalBlue, levittäytyäkseen verkosta toiseen.

Yleisimmät mobiililaitteiden haittaohjelmat toukokuussa top 3, koko maailma

1. **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.

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

3. **Triada** – Android-haittaohjelma, joka auttaa myöhemmin laitteelle ladattavia haittaohjelmia sulautumaan älypuhelimen prosesseihin ja hankkii niille pääkäyttäjän oikeudet. Se on siis tyypiltään takaovi ja suunniteltu Android-laitteita varten.

Koko lista löytyy Check Pointin blogista: Check Point Blog

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.

Check Pointin uhkakartta näyttää kyberhyökkäykset reaaliaikaisesti: ThreatCloud World Cyber Threat Map

Tietoja siitä, mitä mikäkin haittaohjelma tekee: Check Point ThreatWiki
Tietoja Check Pointin uhkientorjuntaresursseista: Threat-prevention-resources
Check Pointin tietoturvatiimin blogi: Check Point Blog

Lisätiedot, tulokset täydellisinä ja haastattelupyynnöt:

Maajohtaja Robert Lindqvist, Check Point Software Technologies,
robertl@checkpoint.com, p. 050 368 4912
OSG Viestintä, Lasse Pulkkinen, lasse.pulkkinen@osg.fi , p. 0400 630 049 tai 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
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) 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.

