****Check Pointin haittaohjelmakatsaus 4/2016****

Mobiilihaittaohjelma HummingBad kiipeää kohti listakärkeä

*Mobiililaitteiden haittaohjelma HummingBad jatkaa yleistymistään. Se nousi maaliskuussa jo sijalle 6 maailman levinneimpien haittaohjelmaperheiden listalla. Suomen tilastossa se ei vielä näy.*

**Espoo, torstaina 28. huhtikuuta 2016 –** Android-laitteidenhaittaohjelma HummingBad tunnistettiin vasta helmikuussa, mutta se sijoittuu heti vuoden ensimmäisen neljänneksen top 10 -listalle. Maaliskuun listalla se on kuudes. Check Pointin listaukset kuvavat haittaohjelmaperheiden yleisyyttä yritysverkoissa ja yrityskäytössä olevissa mobiililaitteissa kautta maailman.

– HummingBad näyttää olevan erityisen nopea leviämään. Tilanne ei varsinaisesti yllätä, sillä arvioimme jo tämän vuoden tietoturvaennusteessamme, että puhelimet ovat entistä suositumpi hyökkäysten kohde. Uhka on todellinen ja kasvava siitä huolimatta, ettei HummingBad vielä näy Suomen tilastoissa, kommentoi Check Pointin Suomen maajohtaja **Petri Sonkeri.**

Mobiililaitteiden tietoturva yltää harvoin samalle tasolle kuin muun yritysverkon turva. Silti yritysten riippuvuus mukana pidettävistä laitteista kasvaa edelleen. Sonkerin mukaan tarve ulottaa tehokas tietoturva myös älypuhelimiin ja tablet-laitteisiin on polttavampi kuin koskaan.

Suomen listan top 3: Angler EK, Cutwail ja Matsnu

HummingBad ei vielä näy Suomen yritysverkkojen haittaohjelmien top 10 -listalla. Sitä hallitsivat maaliskuussa **Angler EK**, **Cutwail** ja **Matsnu**,ilkeitä haittaohjelmia nekin. Ne eivät kuitenkaan tähtää mobiililaitteisiin.

**Angler EK** (exploit kit) on maailman levinnein exploit kit eli tapa levittää haittaohjelmia verkkosivujen kautta. Se ryömii sisään käyttäen hyväkseen uhrin tietokoneella olevien ohjelmien haavoittuvuuksia. Sitä kiinnostavat etenkin Flashin, Javan, Silverlightin ja Acrobatin vanhat versiot. Siksi ohjelmista kannattaa olla käytössä aina uusimmat versiot, mikäli käyttää niitä ollenkaan.

**Cutwail** lähettää uhrin koneelta roskapostia ja raportoi komentokeskukseensa, montako viestiä lähetti ja miten moni lähetys epäonnistui. Se voi myös osallistua DDoS-hyökkäyksiin.

**Matsnu** oli mukana myös helmikuun kolmen kärjessä. Se on viime heinäkuussa tunnistettu haittaohjelma, jonka kautta hyökkääjä voi ladata koneelle mitä tahansa koodia. Matsnu pystynee myös vuotamaan tietoja ja salaamaan koneella olevia tiedostoja.

Kansainvälisen mobiililistan top 3: HummingBad, AndroRAT ja Iop.

Kansainvälisen haittaohjelmalistan top 3 olivat maaliskuussa **Conflicker**, **Sality** ja **Cutwail**. Mobiilihaittaohjelmien kolmen kärki oli **HummingBad**, **AndroRAT** ja **Iop**.

**HummingBad** on erittäin sitkeä ja toimintatavaltaan monipolvinen haittaohjelma, jonka tavoitteena on tuottaa kyberrikollisille mainostuloja. Se asentaa puhelimelle työkalupakin, jonka avulla se voi mahdollisesti tehdä jatkossa paljon muutakin kuin levittää mainoksia.

**AndroRAT** osaa piiloutua viattoman näköisen applikaation sisään ja asentuu mobiililaitteelle käyttäjän huomaamatta. Se antaa rikolliselle täyden määräysvallan puhelimen toimintoihin ja sisältöön.

Myös **Iop** on erityisen ikävä haittaohjelma. Se asentaa puhelimelle ohjelmia, jotka näyttävät käyttäjälle mainoksia. Ohjelmia ja mainoksia on niin paljon, että puhelinta on lähes mahdotonta käyttää.

Check Pointin ThreatCloudTM on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Kuukausittain laadittava haittaohjelmatilasto perustuu ThreatCloudin tietoihin.

--

Lisätietoja HummingBadista löytyy Check Pointin blogista:

<http://blog.checkpoint.com/2016/02/04/hummingbad-a-persistent-mobile-chain-attack/>

Check pointin raportti Matsun toimintatavasta löytyy [täältä](http://blog.checkpoint.com/2015/07/02/matsnu-a-new-malware-discovery/).

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

Tarkempia tietoja haittaohjelmista: [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:**

Check Point Software Technologies Finland, maajohtaja Petri Sonkeri, [petris.@checkpoint.com](mailto:petris.@checkpoint.com), p. 040 5047843

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>

**Check Point Software Technologies Ltd.**  
Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin yksinomaan tietoturvaan keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, jotka torjuvat asiakkaisiin kohdistuvat kyberhyökkäykset havaiten haittaohjelmat ja muut tunkeutujat ainutlaatuisen tehokkaasti. Check Pointin täydellinen tietoturva-arkkitehtuuri suojaa yritysverkot mobiililaitteisiin asti, ja sen ratkaisuja ohjataan kattavan ja intuitiivisen hallintajärjestelmän kautta. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.