Yli miljoona Google-tiliä murrettu - asialla uusi Android-haittaohjelma Gooligan

*Tietoturvayhtiö Check Point on paljastanut ison Google-tilien tietomurron. Sen aiheuttaja on uusi Android-haittaohjelma, joka tartuttaa yli 13 000 laitetta vuorokaudessa.*

**San Carlos, CA 30. marraskuuta 2016 –** Check Point Software Technologies ilmoitti tänään, että se on löytänyt uuden Android-haittaohjelmavariantin, joka on jo murtanut yli miljoonan Google-tilin tietoturvan.

Gooliganiksi nimetty haittaohjelma murtaa Android-laitteen suojaukset ja ottaa pääkäyttäjän oikeudet eli roottaa puhelimen tai tabletin sekä varastaa laitteelle varastoidut sähköpostiosoitteet ja tunnistusavaimet. Niiden avulla hyökkääjät pääsevät käsiksi käyttäjien Gmail-, Google Photos-, Google Docs-, Google Play- ja G Suite -tileihin ja niiden sisältämiin arkaluontoisiin tietoihin.

”Yli miljoonan Google-tilin tietojen joutuminen vääriin käsiin on huolestuttavaa, ja tapaus edustaa kyberhyökkäysten seuraavaa aaltoa. Todistamme parhaillaan krakkereiden toimintatavan strategista murrosta, jossa he ottavat kohteeksi älypuhelimet ja niille varastoidut sensitiiviset tiedot”, sanoo Check Pointin mobiilista tietoturvasta vastaava johtaja **Michael Shaulov**.

**Gooligan pähkinänkuoressa:**

* Kampanja tartuttaa **13 000 mobiililaitetta joka päivä** ja se on ensimmäinen haittaohjelma, joka on onnistunut murtamaan yli miljoona laitetta.
* Vääriin käsiin on joutunut satoja yritysten sähköpostiosoitteita kautta maailman.
* Gooligan tarttuu laitteisiin, joissa on Android 4-(Jelly Bean, KitKat) tai 5 (Lollipop) -käyttöjärjestelmä. **Melkein 74 prosentissa käytössä olevista Android-laitteista** on jompikumpi.
* Saatuaan laitteen komentoonsa hyökkääjät hankkivat tuloja lataamalla vilpillisesti sovelluksia Google Play -kaupasta uhrin laitteelle ja arvioimalla niitä uhrin puolesta.
* Gooligan asentaa murtamilleen laitteille yhteensä **vähintään 30 000 sovellusta** päivässä. Kampanjan alusta laskien latauksia on ollut jo yli kaksi miljoonaa.

Check Point kertoi tietonsa kampanjasta Googlen tietoturvatiimille välittömästi. ”Yhteistyö Check Pointin kanssa on meille arvokasta, ja olemme tehneet töitä yhdessä tämän tapauksen ratkaisemiseksi. Osana toimenpiteitämme käyttäjiemme suojaamiseksi Ghost Push -haittaohjelmaperheeltä olemme parantaneet Android-ekosysteemin yleistä turvallisuutta ja käyttäjiemme tietoturvaa useilla eri tavoilla”, toteaa Googlen Android-tietoturvasta vastaava johtaja **Adrian Ludwig**.

Check Pointin mobiilitietoturvan tutkijatiimi törmäsi Gooliganin koodiin ensi kertaa haitallisen SnapPea -sovelluksen yhteydessä viime vuonna. Elokuussa 2016 haittaohjelmasta havaittiin uusi muoto, joka on siitä lähtien tartuttanut ainakin 13 000 laitetta päivässä. Noin 57 % tartunnoista on sattunut Aasiassa ja noin 9 % Euroopassa. 15.11. tartuntoja oli Suomessa 70, Ruotsissa 177 ja Venäjällä 33 949.

Infektio alkaa, kun käyttäjä lataa ja asentaa Gooligan-tartunnan saaneen sovelluksen laitteelleen tai klikkaa kalasteluviestissä olevaa haitallista linkkiä.

Check Point tarjoaa yleisön käyttöön [ilmaisen verkkotyökalun](https://gooligan.checkpoint.com), jonka avulla Android-käyttäjät voivat tarkistaa, onko heidän tilinsä murrettu.

”Jos tili on murrettu, laitteelle pitää asentaa puhdas käyttöjärjestelmä. Monimutkaista operaatiota kutsutaan flashaukseksi (flashing). Suosittelemme, että laitteesta suljetaan virta ja se viedään sertifioituun huoltoon flashausta varten”, Shaulov lisää.

**Lisätietoja** Check Pointin blogista: <http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan>

**Haastattelupyynnöt:**

OSG Viestintä, Maija Rauha, maija.rauha@osg.fi, p. 0400 630 065.

Puhelinhaastatteluja antaa Michael Shaulov, Check Pointinmobiilista tietoturvasta vastaava johtaja (head of product management and product marketing)

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.