**Espoo, 17. marraskuuta 2016**

Kyberkonnien 5 vaarallisinta Android-ideaa

*Android-puhelinten suuren suosion takia kyberrikolliset pitävät haittaohjelmien räätälöintiä Androidille erityisen tuottoisana liiketoimena. Check Pointin tietoturvatutkijat paljastavat haittakoodinikkareiden viisi innovatiivista ideaa, jotka ovat yleistyneet trendeiksi asti.*

**1. Naamiointi**

Tietoturvayhtiöt tekevät kaikkensa kehittääkseen ratkaisuja, joilla haittakoodit saadaan kiinni, ja samaan aikaan kyberrikolliset kehittävät uusia keinoja niiden naamioimiseksi ja salaamiseksi. Moni tietoturvaratkaisu, kuten Google Play -sovelluskauppaa vartioiva Bouncer, menee halpaan, kun ohjelman haitallinen osuus muutetaan salakieliseksi.

**2. Tippa**

Haittaohjelmia ujutetaan Google Play -kauppaan myös tiputtamalla. Tippa asennetaan lataamalla sovelluskauppaan vaaraton sovellus. Google hyväksyy sen, koska se ei sisällä haittakoodia. Kun käyttäjä lataa sovelluksen puhelimeensa, se ottaa yhteyden hyökkääjän palvelimelle ja lataa sieltä haitallisen koodikomponentin käyttäjän laitteelle.

**3. Palikat**

Haittaohjelma sisältää monesti erillisiä, eri tavoin toimivia osia. Kaksi komponenttia voi toteuttaa samaa tavoitetta eri suunnista. Jos yksi palikka paljastuu ja tehdään vaarattomaksi, hyökkäys voi jatkua toisen komponentin turvin. Hyökkääjälle on helpompaa korvata tehottomaksi tehty osa uudella kuin koodata koko haittaohjelma alusta asti uudestaan.

**4. Pitkäikäisyys**

Haittakoodien tekijät käyttävät useita tekniikoita varmistaakseen, että haittaohjelma pysyy kohdelaitteella sitkeästi. Esimerkiksi sovelluksen ikoni voidaan kätkeä, haitallinen toiminta voidaan ohjelmoida käynnistymään vasta viikkojen tai kuukausien kuluttua, sovellus voidaan naamioida toiseksi tai sille voidaan hankkia niin korkean tason käyttöoikeudet, ettei käyttäjä pysty poistamaan sitä. Tavoite on aina sama: pitää ohjelma riittävän kauan laitteella, että se ehtii toteuttaa rikolliset aikeensa.

**5. Laajennetut oikeudet**

Kyberrikollisilla on useita tekniikoita laajojen käyttöoikeuksien hankkimiseksi haittaohjelmille. Joskus oikeuksia pyydetään suoraan käyttäjältä, joskus hyödynnetään ohjelmistojen aukkoja. Koska Androidista on käytössä useita eri versioita, joista kussakin on omat haavoittuvuutensa, kestää usein kuukausia ennen kuin tietoturvapaikat saapuvat perille, jos käyttäjä ylipäätään lataa niitä. Laitteet voivat olla kuukausikaupalla ovet auki odottamassa hyökkääjiä.

Kyberkonnat ovat yhtä nokkelia kuin sinnikkäitäkin, ja on varmaa, että heillä on jo kehitteillä vielä uudempia tekniikoita. Vain käyttämällä edistyneitä tietoturvaratkaisuja on mahdollista pysyä heitä edellä.

*Lähde: 2016 Check Point Security Report*, joka on ladattavissa täältä: <http://www.checkpoint.com/securityreport/>

--

**Lisätiedot:**

Check Point Software Technologies Finland, maajohtaja Petri Sonkeri, petris.@checkpoint.com, p. 040 5047843

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.