ImageGate: Check Point paljasti uuden tavan levittää haittaohjelmia kuvien kautta

*Tietoturvayhtiö Check Pointin tutkijat selvittivät sosiaalisessa mediassa leviävän virusviestin toiminnan. Facebook Messengerin kautta Suomessakin levinnyt virus on ollut alkusoitto Locky-kiristyshaittaohjelman hyökkäykselle.*

**Espoo, 24. marraskuuta 2016 –** Check Point Software Technologies ilmoitti tänään, että sen tietoturvatutkijat ovat tunnistaneet uuden hyökkäysmenetelmän, ImageGaten, joka upottaa haittaohjelmia valokuva- ja grafiikkatiedostoihin. Lisäksi tutkijat ovat selvittäneet, miten krakkerit ovat käynnistäneet kuvien sisältämän haittakoodin toiminnan sosiaalisen median palveluissa, kuten Facebookissa ja LinkedInissä.

Tutkimuksen mukaan hyökkääjät ovat rakentaneet uuden menetelmän, jolla on mahdollista upottaa haittakoodia kuvatiedostoon ja ladata se onnistuneesti sosiaalisen median sivustolle. Hyökkääjät hyödyntävät sosiaalisen median rakenteellista heikkoutta pakottaakseen uhrit lataamaan kuvatiedoston. Tämä johtaa tartuntaan käyttäjän koneella heti, kun loppukäyttäjä klikkaa ladattua tiedostoa.

Kolmen viime päivän aikana koko tietoturva-ala on seurannut tarkasti Locky-kiristyshaittaohjelman massiivista leviämistä sosiaalisen median, erityisesti Facebookin kautta. Check Pointin tutkijat uskovat vahvasti, että ImageGate-tekniikka selittää, miten hyökkäys on mahdollinen. Asia on tähän asti ollut selvittämättä.

Check Pointin tutkijat pystyivät paljastamaan hyökkäysmenetelmän, joka kohdistuu useisiin isoihin verkkopalveluihin kautta maailman, mukaan lukien Facebook ja LinkedIn. Check Point kertoi Facebookille ja LinkedInille tietonsa menetelmästä jo syyskuun alkupuolella.

Katso demovideo täältä: <https://youtu.be/sGlrLFo43pY>

Locky-kiristyshaittaohjelman tapauksessa käy niin, että kun käyttäjä lataa ja avaa saamansa haitallisen tiedoston, kaikki hänen koneellaan olevat tiedostot enkryptataan automaattisesti, ja käyttäjä saa ne uudelleen käsiinsä vasta maksettuaan lunnaat. Tietoturva-alalla arvioidaan, että kampanja on edelleen käynnissä ja uhrien määrä kasvaa päivä päivältä.

”Yhä useammat kuluttavat aikaa sosiaalisen median sivustoilla. Kyberrikolliset ymmärtävät, että niitä pidetään yleensä turvallisina, ja siksi he etsivät jatkuvasti uusia tekniikoita, joiden avulla he voisivat hyödyntää sosiaalista mediaa rikollisen toimintansa alustana. Check Pointin tehtävä on suojata käyttäjiä tietoturvariskeiltä, ja siksi pyrimme jatkuvasti tunnistamaan, minne rikolliset iskevät seuraavaksi”, kertoo Check Pointin Head of Products Vulnerability Research **Oded Vanunu**.

**Suojaudu näin:**

Check Point suosittelee seuraavia suojaavia toimenpiteitä:

1. Jos olet klikannut kuvaviestiä ja selaimesi alkaa ladata tiedostoa, älä avaa sitä. Sosiaalisen median palveluiden pitäisi näyttää kuvat ilman, että tiedostoa pitää ladata.

2. Älä avaa mitään kuvatiedostoa, jossa on epätavallinen pääte, kuten SVG, JS tai HTA.

**Check Point julkaisee yksityiskohtaisen teknisen selvityksen uudesta hyökkäysmenetelmästä vasta sen jälkeen, kun sen kohteena olevat tärkeimmät verkkosivustot ovat korjanneet haavoittuvuuden. Näin hyökkääjät eivät pääse hyötymään tilanteesta.**

**Haastattelupyynnöt:**

Check Pointin Head of Products Vulnerability Research Oded Vanunu antaa puhelinhaastatteluja tarvittaessa. Ota yhteys ajan sopimiseksi: 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.