**Joker-haittaohjelma livahti jälleen Google Play -kauppaan**

*Joker-haittaohjelma tunnetaan kyvystään piiloutua Google Play -kaupassa myynnissä oleviin puhelinsovelluksiin. Check Pointin tietoturvatutkijat ovat löytäneet jälleen uuden Joker-version, joka tilaa palveluja uhrin nimissä.*

**ESPOO — 9.7.2020** – Tietoturvayhtiö Check Point Software Technologies tutkijat ovat löytäneet Joker-haittaohjelmasta uuden version. Joker tunnetaan erittäin muuntautumiskykyisenä puhelinsovellusten haittaohjelmana, jonka havaitseminen on vaikeaa. Siksi Google Play -kaupasta on toistuvasti löydetty ja poistettu sovelluksia, jotka sisältävät Jokerin. Haitake havaittiin ensimmäisen kerran jo vuona 2017.

Uusin Joker tulee laitteelle vaarattoman näköisessä sovelluksessa, kuten taustakuvakirjaston mukana. Google on poistanut sovelluskaupastaan 11 uuden Joker-version sisältänyttä sovellusta. Puhelimeen päästyään haittaohjelma lataa laitteelle toisen haittaohjelman. Se kirjautuu käyttäjän tietämättä maksullisiin palveluihin, jotka alkavat laskuttaa uhria. Siten kyseessä on tilausansa.

Check Pointin tutkija **Aviran Hazum** huomasi, että uusin Joker piiloutuu ”Android Manifest” -tiedostoon, joka jokaisessa Android-sovelluksessa pitää olla, jotta se toimisi laitteessa. Siinä vaiheessa, kun Google arvioi sovellusta, Joker pysyy hiljaa ja piilossa. Varsinaisen työn tekevä haittaohjelma ladataan Jokeriin vasta, kun sovellus on jo myynnissä.

”Nämä sovellukset on nyt poistettu markkinoilta, mutta on erittäin todennäköistä, että uusia Joker-versoita tulee jatkossakin. Siksi jokaisen on hyvä ymmärtää, mikä Joker on ja miten siltä voi suojautua”, Aviran Hazum sanoo.

**Näin suojaudut**

Jos epäilet, että puhelimessasi on Joker-tartunnan saanut sovellus, toimi näin:

* Poista epäilyttävä sovellus
* Tarkista luottokortti- ja puhelinlaskustasi, onko nimissäsi tilattu maksullisia palveluja. Peruuta tilaus, jos mahdollista.
* Asenna laitteellesi tietoturvaohjelmisto, jotta vältyt tartunnoilta jatkossa.

Tarkemmat tiedot uuden Jokerin toiminnasta ja lista poistetusta sovelluksista löytyvät Check Point Researchin blogista täältä:  <https://research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/>

**Lisätiedot ja haastattelupyynnöt:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com.

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

**Seuraa Check Point Researchia:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**Check Point Research**

Check Point Research ([research.checkpoint.com](https://research.checkpoint.com)) huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvayhteisöllä on käytettävissään paras mahdollinen tieto kyberturvallisuuden riskeistä. Tutkijaryhmä kerää ja analysoi ThreatCloud-verkkopalvelun tallentamat maailmanlaajuiset kyberhyökkäystiedot, jotta hakkerit pysyvät kurissa ja kaikki Check Pointin tuotteet pystytään päivittämään uusimmilla suojauksilla. Tutkijaryhmä koostuu yli 100 analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvayhtiöiden ja viranomaisten kanssa.

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.