Tietoturvayhtiö varoittaa mobiilikäyttäjiä: QR-koodihuijaukset nousussa

QR-koodien käyttö, esimerkiksi tapahtumiin kirjautumiseen ja yhteystietojen selvittämiseen, on koronapandemian aikana lisääntynyt huomattavasti. Tämä houkuttelee huijareita, joiden tavoitteena on varastaa käyttäjätunnuksia sekä levittää haitallisia ohjelmia ja sovelluksia käyttäjien puhelimiin.

ESPOO – 27. marraskuuta 2020 – Maailman johtava tietoturvayhtiö Check Point® Software Technologies varoittaa mobiilikäyttäjiä QR-koodien turvallisuusriskeistä, sillä niiden käyttö on lisääntynyt räjähdysmäisesti Covid-19-pandemian aikana. Esimerkiksi ravintolat ovat aiempaa enemmän ottaneet käyttöön QR-koodeja, jotta asiakkaat voivat selata ruokalistaa puhelimeltaan ja maksaa ilman kontaktia.

Hakkerit pyrkivät hyötymään QR-koodien uudesta suosiosta ja korvaavat aitoja QR-koodeja koodeilla, jotka käynnistävät haitallisen URL-osoitteen tai yrittävät ladata haittaohjelmia. Aiemmin vuonna 2020 Belgian liittovaltion poliisi antoi varoituksen QR-koodeihin liittyvästä verkkopetoksesta. Haitallinen koodi yrittää skannattaessa varastaa kirjautumistunnuksia, joita käytetään puhelimen muissa, esimerkiksi pankki- ja vähittäiskaupan sovelluksissa. Alankomaiden ING Bank on myös varoittanut vilpillisistä QR-koodeista, jotka yrittävät yhdistää asiakkaiden ING-tileihin mobiilisovelluksen kautta toisen henkilön ING-pankin.

MobileIronin äskettäin tekemän tutkimuksen vastaajista 38 % oli skannannut QR-koodin ravintolassa, baarissa tai kahvilassa ja 37 % oli skannannut koodin vähittäiskaupassa maalis-syyskuussa 2020. Yli puolet (51 %) vastaajista ilmoitti, ettei heillä ole puhelimessaan tietoturvaohjelmistoa tai että he eivät tiedä, onko sitä. Usein puhelimissa on sekä henkilökohtaisia että työnantajan tietoja ja sovelluksia, mikä lisää organisaatioiden kyberriskiä. Check Pointin vuoden 2020 kyberturvallisuusraportti osoitti, että mobiililaitteisiin liittyvät kyberhyökkäykset vaikuttivat 27 prosenttiin organisaatioista maailmanlaajuisesti, ja 34 % organisaatioista kärsi mobiililaitteiden haittaohjelmista.

”On muistettava, ettei QR-koodi ole muuta kuin nopea ja kätevä tapa käyttää nettipalveluja. Emme voi olla varmoja, että koodi on aito ennen kuin olemme jo skannanneet sen – ja silloin hyökkäys on jo voinut käynnistyä”, toteaa Check Point Softwaren Suomen maajohtaja **Sampo Vehkaoja**.

”QR-koodit eivät ole luonnostaan turvallisia tai luotettavia, ja hakkerit tietävät, että suurimmalla osalla ihmisistä on vain vähän tai ei lainkaan suojausta kännykässään. Suosittelemme kaikkia käyttämään mobiilitietoturvaratkaisua laitteidensa ja tietojensa suojaamiseksi verkkourkinnalta sekä haitallisilta ohjelmilta ja sovelluksilta”.

Check Pointilla on tietoturvaratkaisuja sekä henkilökohtaisille että yritysten mobiililaitteille. SandBlast Mobile pitää yritystoiminnot ja mobiililaitteiden arkaluontoiset tiedot suojassa kyberhyökkäyksiltä ainutlaatuisella, laitteen sisäisellä verkkosuojauksella. Se sisältää haittaohjelmien, tietojenkalastelun ja bottien torjunnan sekä turvallisen selaamisen ja tarjoaa reaaliaikaisen suojan kehittyneimmiltäkin uhilta. ZoneAlarm Mobile Security suojaa henkilökohtaisia mobiililaitteita kiristysohjelmilta, data- ja tunnistevarkauksilta sekä kaapatuilta Wi-Fi-verkoilta.

Lisätiedot:
Sampo Vehkaoja, Country Manager, Finland and Baltics, Check Point Software Technologies, sampov@checkpoint.com. Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

©2020 Check Point Software Technologies Ltd. All rights reserved

Seuraa Check Pointia:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Check Point Research
Check Point Research (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) 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.

©2020 Check Point Software Technologies Ltd. All rights reserved