Google, Amazon ja WhatsApp ohittivat Applen eniten jäljiteltyinä brändeinä – mobiilissa kyberkonnat teeskentelevät olevansa Facebook

Check Pointin tietoturvatutkijat paljastavat uusimmassa brändiväärennösraportissaan, että Google ja Amazon olivat huhti-kesäkuussa maailmanlaajuisesti jäljitellyimmät tuotemerkit. Kun uhreja lähestyttiin älypuhelinten kautta, hakkerit teeskentelivät useimmin olevansa Facebook.

Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut vuoden 2020 toista kvartaalia koskevan Brand Phishing -raporttinsa. Raportista selviää, mitä tuotemerkkejä kyberrikolliset useimmin hyödynsivät yrittäessään napata uhrien henkilö- tai pankkitietoja. Raportissa on myös esimerkkejä Apple iCloudia ja PayPalia jäljittelevistä tietojenkalasteluhyökkäyksistä.

Brand Phishing -hyökkäyksestä on kysymys, kun rikolliset yrittävät jäljitellä tunnetun tuotemerkin verkkosivuja käyttämällä samaa domain-nimeä tai URL-osoitetta ja samantyyppistä sivuston ulkoasua. Väärennetylle sivustolle voidaan houkutella uhreja sähköpostilla tai tekstiviestillä, mobiilisovelluksen avulla tai verkkoselaimessa. Väärennetty sivusto sisältää usein lomakkeen, jonka avulla kyberrikolliset keräävät uhrien henkilö- ja maksutietoja.

Huhti-kesäkuun useimmin kaapatut brändit olivat Google ja Amazon, joiden nimet olivat tavalla tai toisella mukana 13 prosentissa huijausyrityksistä. Kyberkonnat pyrkivät näin hyödyntämään niiden hyvää tunnettuutta. Kolmannelle sijalle ylsi WhatsApp.

Sähköpostihuijaushyökkäykset lisääntyvät verrattuna kolmeen edelliseen kuukauteen. Niitä oli lähes neljännes (24 %) kaikista tietojenkalasteluhyökkäyksistä. Syynä tähän muutokseen voi olla Covid-19:ään liittyvien globaalien rajoitusten lieventäminen, kun yritykset ovat avautuneet uudelleen ja työntekijät ovat palanneet töihin.

Lähes 15 % tietojenkalasteluhyökkäyksistä kohdistuu mobiililaitteisiin. Niissä jäljitellyimmät tuotemerkit ovat Facebook, WhatsApp ja PayPal.

Apple (Q1:n jäljitellyin brändi) putosi 7. sijalle Q1:n kärkipaikalta. Brändiväärennöshavaintojen kokonaismäärä pysyi vakaana vuoden 2020 ensimmäiseen neljännekseen verrattuna.

Väärennetyimmät brändit, Q2 2020

1. Google (mukana 13 prosentissa kaikista brand phishing -yrityksistä globaalisti)
2. Amazon (13 %)
3. WhatsApp (9 %)
4. Facebook (9 %)
5. Microsoft (7 %)
6. Outlook (3 %)
7. Apple (2 %)
8. Netflix (2 %)
9. Huawei (2 %)
10. PayPal (2 %)

”Kyberrikolliset keskittyvät edelleen huijaamaan meitä luotettavien nimien, kuten Googlen, Amazonin ja WhatsAppin kautta. Kuluneella vuosineljänneksellä tietoja kalasteltiin kuitenkin tavallista enemmän

sähköpostitse. Koska meidän on ollut välttämätöntä työskennellä kotona, sähköposti on ollut hakkereiden tärkein hyökkäysmenetelmä. Miettisin toisenkin kerran sähköpostitse lähetetyn dokumentin avaamista, varsinkin jos lähettäjä väittää olevansa Google tai Amazon. Odotan sähköpostitse tehtyjen tietojenkalasteluhyökkäysten lisääntyvän entisestään vuoden 2020 jälkipuoliskolla", sanoo **Lotem Finkelsteen**, Manager of Threat Intelligence Check Pointilta.

Kuinka pysyä turvassa:
1. Käytä aitoja verkkosivustoja. Älä klikkaa mainoslinkkejä sähköpostissa. Sen sijaan googlaa haluamasi jälleenmyyjä ja napsauta linkkiä Googlen tulossivulta.
2. Varo “erikoistarjouksia”. 80 prosentin alennus uudesta iPhonesta ei yleensä ole luotettava ostomahdollisuus.
3. Varo alkuperäistä jäljittelevi domain-nimiä. Tarkkaile sähköpostiviestien tai verkkosivustojen oikeinkirjoitusvirheitä ja tuntemattomia sähköpostin lähettäjiä.

Check Point kerää brändiväärennösraportin tiedot ThreatCloud-verkostonsa kautta. ThreatCloud on maailman laajin kyberrikollisuuden paljastamiseen tähtäävä verkosto, joka kerää tiedot hyökkäyksistä Check Pointin tietoturvalaitteilta kautta maailman. Verkosto tunnistaa päivittäin yli 11 miljoonaa haittaohjelmaa ja yli 5,5 miljoonaa tartunnan saanutta verkkosivua analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Lue lisää aiheesta Check Pointin blogista.

Lisätiedot:
Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com. Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

Seuraa Check Point Researchia:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_
Podcast: https://research.checkpoint.com/category/cpradio/
Facebook: https://www.facebook.com/checkpointresearch

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.

