DHL kiihdytti Microsoftin ohi kyberkonnien suosikkisyöttinä – ”On aivan liian helppoa olla huomaamatta epäilyttäviä yksityiskohtia”

Check Pointin tietoturvatutkijat kertovat uusimmassa brändiväärennösraportissaan, että kyberrikollisten tietojenkalastelussa jäljittelemien brändien kärkikolmikossa olivat loka-joulukuussa DHL, Microsoft ja WhatsApp.

ESPOO – 18. tammikuuta 2022 - Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut vuoden 2021 neljättä kvartaalia koskevan Brand Phishing -raporttinsa. Raportista selviää, mitä tuotemerkkejä kyberrikolliset useimmin hyödynsivät kalastellessaan uhrien henkilö- tai pankkitietoja.

Useimmin jäljitellyksi brändiksi kiri loka-joulukuussa 2021 ensimmäistä kertaa logistiikkayhtiö DHL, jota koski 23 prosenttia kaikista brändiväärennöksistä. Rikolliset hyödynsivät tällä tavoin verkkokaupan kasvua. Ykkösenä oli yhä Microsoft 20 prosentin osuudellaan. Ensimmäistä kertaa kärkikymmenikköön ylsi myös kuljetus- ja logistiikkayhtiö FedEx.

Sosiaalinen media vahvisti viime vuoden viimeisellä neljänneksellä asemaansa tietojenkalasteluyrityksissä eniten imitoitujen sektoreiden joukossa. Vaikka Facebook on poistunut listalta, WhatsApp on noussut kolmanneksi eniten jäljitellyksi brändiksi. Sen osuus on nyt 11 prosenttia kaikista tietojenkalasteluyrityksistä. LinkedIn on sijalla viisi ja sen osuus on nyt 8 prosenttia kaikista tietojenkalasteluihin liittyvistä hyökkäyksistä.

”On hyvä muistaa, että kyberrikolliset ovat ennen kaikkea opportunisteja. Yrittäessään varastaa ihmisten henkilötietoja tai levittää haittaohjelmia käyttäjän koneelle he pyrkivät usein hyödyntämään kuluttajatrendejä ja jäljittelevät johtavia brändejä”, sanoo Data Research Group Manager **Omer Dembinsky** Check Point Softwarelta.

”Viime vuosineljänneksellä globaali logistiikkayhtiö DHL nousi ensimmäistä kertaa useimmin jäljiteltyjen brändien top 10 -listan kärkeen. Hakkerit pyrkivät oletettavasti hyötymään uusien ja mahdollisesti varomattomien verkko-ostajien huimasta määrästä vuoden vilkkaimman ostossesongin aikana. Iäkkäämmillä käyttäjillä saattaa olla puutteellisemmat teknologiataidot kuin nuoremmilla sukupolvilla. Tehdessään ostoksia verkossa kenties ensimmäistä kertaa he eivät välttämättä erota väärennettyjä vahvistusviestejä tai seurantapäivityksiä aidoista”, Dembinsky jatkaa.

”Ei tullut yllätyksenä, että etätyöskentelyn ja muiden pandemian seurausten myötä hakkerit hyödyntävät yhä useammin sosiaalisen median kanavia, kuten WhatsAppia, Facebookia ja LinkedIniä. Valitettavasti väärennetyt brändit eivät voi tehdä paljoakaan tietojenkalasteluyritysten torjumiseksi. Oven lisävahingoille avaa inhimillinen tekijä: On aivan liian helppoa olla huomaamatta epäilyttäviä yksityiskohtia, kuten väärin kirjoitettuja verkkotunnuksia ja muita kirjoitusvirheitä tai virheellisiä päivämääriä. Kehotamme kaikkia käyttäjiä kiinnittämään huomiota tällaisiin yksityiskohtiin, kun he ovat tekemisissä DHL:n kaltaisten yritysten kanssa tulevina kuukausina”, kommentoi Check Pointin Suomen ja Baltian maajohtaja **Sampo Vehkaoja**.

Brand Phishing -hyökkäyksestä on kysymys, kun rikolliset yrittävät jäljitellä tunnetun tuotemerkin verkkosivuja käyttämällä samaa tai lähes 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 henkilötietoja ja salasanoja.

Useimmin väärennetyt brändit, Q4 2021

1. DHL (mukana 23 prosentissa kaikista tietojenkalasteluyrityksistä globaalisti)
2. Microsoft (20 %)
3. WhatsApp (11 %)
4. Google (10 %)
5. LinkedIn (8 %)
6. Amazon (4 %)
7. FedEx (3 %)
8. Roblox (3 %)
9. Paypal (2 %)
10. Apple (2 %)

Lue lisää ja katso esimerkkejä DHL:n, PayPalin ja Fedexin nimissä lähetetyistä tietojenkalasteluviesteistä Check Pointin blogista.

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. ThreatCloud-tietokanta tarkastaa päivittäin yli 3 miljardia verkkosivustoa ja 600 miljoonaa tiedostoa ja tunnistaa yli 250 miljoonaa haittatapahtumaa päivittäin.

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.

Seuraa Check Point Researchia:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

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.

