Microsoft on yhä kyberrikollisten suosikkibrändi

Check Pointin tietoturvatutkijat kertovat uusimmassa brändiväärennösraportissaan, että Microsoft oli loka-joulukuussa 2020 kyberkonnien useimmin jäljittelemä tuotemerkki. Sitä seurasivat DHL ja LinkedIn.

Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut vuoden 2020 neljättä kvartaalia koskevan Brand Phishing -raporttinsa. Raportista selviää, mitä tuotemerkkejä kyberrikolliset useimmin hyödynsivät kalastellessaan uhrien henkilö- tai pankkitietoja.

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.

Loka-joulukuun useimmin kaapattu brändi oli edelleen Microsoft. Teknologiajättiin liittyi 43 % kaikista tietojenkalasteluyrityksistä maailmanlaajuisesti. Tähän saattaa olla syynä se, että hakkerit pyrkivät hyötymään koronapandemian toisen aallon myötä jatkuneesta etätyöntekijöiden suuresta määrästä. Vuoden kolmannella neljänneksellä yhtiö sijoittui myös ensimmäiseksi, tuolloin 19 prosentin osuudella.

Seuraavaksi yleisin brändi oli DHL, jonka nimi oli mukana 18 prosentissa tietojenkalasteluyrityksistä. Tähän myötävaikutti rikollisten hyödyntämä marras- ja joulukuun verkkokauppakausi.

Etätöiden ja verkkokauppakauden aikana kyberkonnat pyrkivät hyötymään lisääntyvästä mobiiliyhteyksien sekä verkkopalveluiden ja -kauppojen käytöstä. Toimialoista hyökkääjät suosivatkin teknologia-alaa sekä vähittäiskauppaa ja kuljetusta.

Väärennetyimmät brändit, Q4 2020

1. **Microsoft** (mukana 43 prosentissa kaikista brand phishing -yrityksistä globaalisti)
2. **DHL** (18 %)
3. **LinkedIn** (6 %)
4. **Amazon** (5 %)
5. **Rakuten** (4 %)
6. **IKEA** (3 %)
7. **Google** (2 %)
8. **Paypal** (2 %)
9. **Chase** (2 %)
10. **Yahoo** (1 %)**.**

”Vuoden 2020 viimeisellä neljänneksellä rikolliset yrittivät entistä useammin varastaa ihmisten henkilötietoja jäljittelemällä johtavia brändejä. He myös päivittivät tietojenkalastelutaktiikoitaan parantaakseen menestymisen mahdollisuuksiaan. Kehotamme käyttäjiä olemaan varovaisia luovuttaessaan henkilö- ja tunnistetietoja yrityssovelluksille. Kannattaa myös miettiä kaksikin kertaa ennen kuin avaa vaikkapa Microsoftin tai Googlen nimissä tulevien sähköpostien liitetiedostoja tai linkkejä,” sanoo Check Pointin **Maya Horowitz**, Director of Threat Intelligence & Research, Products.

Näin pysyt turvassa:

1. Käytä aitoja verkkosivustoja. Älä klikkaa sähköpostien mainoslinkkejä. Sen sijaan googlaa 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. ThreatCloud-tietokanta tarkastaa päivittäin yli 3 miljardia verkkosivustoa ja 600 miljoonaa tiedostoa ja tunnistaa yli 250 miljoonaa haittatapahtumaa päivittäin.

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.

