Check Pointin brändiväärennösraportti: Tietojenkalastelussa jäljitellyimmät brändit Walmart ja Microsoft, Mastercard top 10:ssä ensimmäistä kertaa

Kyberturvayhtiö Check Point kertoo brändiväärennösraportissaan, että vuoden 2023 kolmannella neljänneksellä kyberhuijauksissa hyödynnettiin eniten Walmartin ja Microsoftin mainetta. Kymmenen kärjessä olivat myös muun muassa Google, Apple, LinkedIn, Mastercard ja Netflix.

ESPOO – 24. lokakuuta 2023 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut vuoden 2023 kolmatta kvartaalia koskevan Brand Phishing -raporttinsa. Raportista selviää, mitä tuotemerkkejä kyberrikolliset useimmin hyödynsivät kalastellessaan uhriensa henkilö- tai pankkitietoja heinä-, elo- ja syyskuussa 2023.

Check Point kertoo, että vuoden 2023 kolmannella neljänneksellä tietojenkalasteluhyökkäyksissä eniten jäljitelty brändi oli vähittäiskaupan jättiläinen Walmart. Sen osuus kaikista tietojenkalasteluhyökkäyksistä oli 39 prosenttia, mikä oli iso harppaus edeltävän kvartaalin kuudennelta sijalta.

Teknologiajätti Microsoft sijoittui toiseksi 14 prosentin osuudella ja monikansallinen rahoituspalveluyritys Wells Fargo kolmanneksi 8 prosentin osuudella.

Mastercard, maailman toiseksi suurin maksupalveluja tarjoava yritys, nousi top 10 -listalle ensimmäistä kertaa ja sijoittui yhdeksänneksi. Amazonia hyödyntävien tietojenkalastelukampanjoiden määrä pysyi myös korkeana ajoittuen yhtiön ilmoitukseen syksyn 2023 Prime Day -myynnistä.

”Tietojenkalastelu on edelleen yksi tuotteliaimmista hyökkäystyypeistä, ja kyberrikolliset jäljittelevät useita vähittäiskaupan, teknologian ja pankkialan brändejä. Tekoälyn lisääntynyt käyttö on myös vaikeuttanut, joskaan ei tehnyt mahdottomaksi, luotettavien ja vilpillisten sähköpostien erottamista toisistaan”, sanoo Data Group Manager **Omer Dembinsky** Check Point Softwarelta.

”On tärkeää olla valppaana myös sellaisten viestien suhteen, jotka näyttävät tulevan hyvämaineisilta yrityksiltä. On hyvä aina tarkistaa lähettäjän sähköpostiosoite ja viestin oikeellisuus ja käydä tekemässä mahdolliset maksutapahtumat turvallisella sivustolla sen sijaan, että klikkaisi sähköpostiviestissä olevaa linkkiä. Jos organisaatiot huomaavat nimeään käyttävän tietojenkalastelukampanjan, niiden tulee tiedottaa asiasta ja varoittaa asiakkaita mahdollisista uhkista asianmukaisia kanavia käyttäen”, ohjeistaa Check Pointin Suomen ja Baltian maajohtaja **Viivi Tynjälä**.

Kalasteluhyökkäyksessä rikolliset yrittävät jäljitellä tunnetun yrityksen tai tuotemerkin verkkosivuja käyttämällä samantyyppistä domain-nimeä tai URL-osoitetta ja sukunäköistä ulkoasua. Väärennetylle verkkosivulle vievä linkki voidaan lähettää uhreille sähköpostitse tai tekstiviestinä. On myös mahdollista, että uhri pyritään ohjaamaan väärennetylle sivulle verkkoselailun aikana tai väärennetyn mobiilisovelluksen avulla. Väärennetty verkkosivu sisältää usein lomakkeen, jonka tarkoitus on anastaa uhrin henkilö- tai maksutietoja tai salasanoja.

Useimmin väärennetyt brändit, Q3 2023

1. Walmart (39 %)
2. Microsoft (14 %)
3. Wells Fargo (8 %)

4. Google (4 %)
5. Amazon (4 %)
6. Apple (2 %)
7. Home Depot (2 %)
8. LinkedIn (2 %)
9. Mastercard (1 %)
10. Netflix (1 %).

Lue lisää ja katso **esimerkkejä LinkedInin ja Amazonin nimissä lähetetyistä tietojenkalasteluviesteistä** Check Pointin blogista: Walmart Jumps to Top Spot as the Most Impersonated Brand for Phishing Scams in Q3 2023

Check Pointin blogissa julkaistut kuvat/ruutukaappaukset ovat saatavissa pyynnöstä.

Lisätiedot:

Jarno Ahlström, Lead Security Engineer, Cyber Security Evangelist, Check Point Software Technologies, jarnoa@checkpoint.com, p. 040 707 0706.
Viivi Tynjälä, Country Manager, Finland and Baltics, Check Point Software Technologies, viivit@checkpoint.com, p. 0400 411 530.

Haastattelu- ja kuvapyynnöt:

Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. +358 50 441 6068.

Seuraa Check Pointia:

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

Check Point Research

Check Point Research (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. (https://www.checkpoint.com/) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Check Point Infinityn ratkaisuportfolio suojaa yrityksiä ja julkisia organisaatioita 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Infinity koostuu neljästä peruspilarista: Check Point Harmony etäkäyttäjille; Check Point CloudGuard pilven automaattiseen suojaamiseen; ja Check Point Quantum tietoverkkojen ja datakeskusten suojaamiseen. Näitä kaikkia hallitaan alan kattavimmalla ja intuitiivisimmalla yhtenäisellä hallintajärjestelmällä; Check Point Horizonilla, joka on tietoturvapoikkeamien ennaltaehkäisyyn tähtäävä ohjelmisto- ja palvelukokonaisuus. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

