Keiden nimissä huijarit nyt viestittelevät? Check Pointin brändiväärennösraportti kertoo, että Microsoft-tilien haltijat ovat kyberkonnien suosikkikohde

Kyberturvayhtiö Check Point kertoo uusimmassa brändiväärennösraportissaan, että vuoden 2023 toisella neljänneksellä kyberhuijauksissa hyödynnettiin eniten maailman kolmen suurimman teknologiayrityksen brändejä.

ESPOO – 19. heinäkuuta 2023 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut vuoden 2023 toista kvartaalia koskevan Brand Phishing -raporttinsa. Raportista selviää, mitä tuotemerkkejä kyberrikolliset useimmin hyödynsivät kalastellessaan uhriensa henkilö- tai pankkitietoja huhti-, touko- ja kesäkuussa 2023.

Microsoft nousi tällä kvartaalilla ykköseksi alkuvuoden sijalta kolme. Kaikista tuotemerkkejä hyödyntävistä kalasteluyrityksistä peräti 29 prosenttia tehtiin tämän teknologiajätin nimissä. Osittain nousu johtunee kampanjasta, jossa hakkerit lähestyivät Microsoft-tilin haltijoita. Väärennetyssä sähköpostiviestissä väitettiin, että tilillä oli havaittu epätavallista toimintaa.

Google päätyi tällä kertaa listasijalle kaksi 19 prosentin osuudella kalasteluyrityksistä, ja kolmanneksi sijoittui Apple, jonka brändiä väärinkäytettiin viidessä prosentissa kalasteluviesteistä. Toimialan mukaan tarkasteltuna tällä kvartaalilla imitoitiin eniten teknologiayrityksiä, toiseksi eniten pankki- ja rahoitusalaa ja kolmanneksi eniten sosiaalisen median yrityksiä.

Check Point varoitti vuoden alussa nousevasta trendistä, jossa pankkialaa hyödynnetään entistä useammin tietojenkalastelussa. Tämä trendi on ollut voimissaan myös kolmen viime kuukauden aikana. Osoituksena tästä yhdysvaltalainen Wells Fargo nousi brändiväärennöslistan neloseksi sähköpostiviesteillä, joissa vastaanottajilta kysyttiin tilitietoja. Samantyyppisiä viestejä lähetettiin myös Walmartin ja LinkedInin nimissä.

”Vaikka yritykset vaihtuvat listauksessamme kvartaalista toiseen, kyberrikollisten menettelytavat pysyvät pääosin samoina. Tämä johtuu siitä, että menetelmä toimii aina vain. Tutun näköisten logojen tarkoitus on luoda vastaanottajille valheellista turvallisuuden tunnetta, ja se onnistuu niin usein, että sähköpostien massapostituksia kannattaa jatkaa”, sanoo Check Point Softwaren Data Group Manager **Omer Dembinsky**.

”Tästä syystä meidän kaikkien on syytä pysähtyä hetkeksi ennen linkkien klikkaamista. Näyttääkö jokin viestissä oudolta? Onko siinä kielivirheitä tai hoputetaanko siinä toimimaan nopeasti? Tällaiset ovat kalasteluviestien tunnusmerkkejä. Maineestaan huolta pitävien yritysten ja organisaatioiden tulisi ottaa käyttöön teknologiat, joiden avulla kalasteluviestit pystytään pysäyttämään ennen kuin ne ehtivät harhauttaa vastaanottajia”, hän jatkaa.

Check Point lisäsi uusimmassa Quantum Titan-versiossa R81.20 kalastelua estävään Zero Phishing -tietoturvateknologiaansa uuden ominaisuuden nimeltä Brand Spoofing Prevention eli tavaramerkkihuijauksen esto. Se on suunniteltu estämään brändinä esiintymisen ja havaitsemaan ja estämään tuotemerkkien käyttämisen houkuttimena. Se tunnistaa luonnollisten kielten rakenteita, joten sitä voi käyttää kaikilla kielillä ja kaikissa maissa. Kehittynyttä tekoälyä hyödyntävä ratkaisu toimii myös ennaltaehkäisevästi, koska se tunnistaa väärennetyt verkkosivustot jo varhaisessa vaiheessa ja estää pääsyn niihin.

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 puhelinsovelluksen avulla. Väärennetty verkkosivu sisältää usein lomakkeen, jonka tarkoitus on anastaa uhrin henkilö- tai maksutietoja tai salasanoja.

Useimmin väärennetyt brändit, Q2 2023

1. Microsoft (mukana 29 %:ssa kaikista tietojenkalasteluhyökkäyksistä maailmanlaajuisesti)
2. Google (19,5 %)
3. Apple (5,2 %)
4. Wells Fargo (4,2 %)
5. Amazon (4 %)
6. Walmart (3,9 %)
7. Roblox (3,8 %)
8. LinkedIn (3 %)
9. Home Depot (2,5 %)
10. Facebook (2,1%).

Lue lisää ja katso **esimerkkejä tietojenkalasteluviesteistä** Check Pointin blogista täältä.

Check Pointin blogissa julkaistut kuvat/ruutukaappaukset ovat saatavissa pyynnöstä.

Lisätiedot:

Viivi Tynjälä, Country Manager, Finland and Baltics, Check Point Software Technologies, viivit@checkpoint.com, p. 0400 411 530.

Haastattelu- ja kuvapyynnöt: Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. +358 400 630 065.

Seuraa Check Point Researchia:

Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

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 kolmesta 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.

