**Tietojenkalastelu on yhä kasvava uhka: Urkkijat naamioituvat useimmiten Facebookiksi – suosittuja myös Spotify, Netflix ja PayPal**

*Tietoturvayhtiö Check Pointin tutkijat selvittivät, että Facebook on tietojenkalastelijoiden eniten matkima brändi. Sähköpostiurkinnassa suosituin on Yahoo! ja verkkokalastelussa Spotify.*

**CPX Wien, Itävalta – 6. helmikuuta 2020 –** Tietoturvayhtiö Check Point Software Technologiesin tutkijat ovat julkaisseet tietojenkalasteluraportin, jonka mukaan tietojenkalasteluhyökkäyksissä eniten jäljitelty brändi on Facebook.

Raportissaan Check Point Research nostaa esiin brändit, joiden nimissä rikolliset yrittävät useimmiten urkkia yksityishenkilöiden henkilökohtaisia tietoja tai maksutietoja. Tarkasteltu ajanjakso oli vuoden 2019 viimeinen neljännes, johon sisältyvät verkkokauppojen vuoden vilkkaimmat kaudet.

Brändihuijauksissa rikolliset yrittävät jäljitellä tunnettujen brändien virallisia verkkosivustoja käyttämällä samankaltaista verkkotunnusta tai URL-osoitetta ja sivuston ulkoasua kuin alkuperäinen sivusto. Linkki väärennettyyn verkkosivustoon voidaan lähettää uhrille sähköpostitse tai tekstiviestinä tai uhri voidaan ohjata sivustolle nettiä selatessa tai saastuneen mobiilisovelluksen kautta. Väärennetty verkkosivusto sisältää usein lomakkeen, jonka tarkoituksena on varastaa hyökkäyksen kohteen käyttäjä- ja maksutietoja tai muita henkilökohtaisia tietoja.

**Top10 tietojenkalastelubrändit (Q4 2019)**

Brändit on luokiteltu niiden huijausyrityksissä yleisen ulkoasun perusteella:

1. **Facebook** (liittyi 18 %:iin kaikista brändihuijausyrityksistä maailmanlaajuisesti)
2. **Yahoo** (10 %)
3. **Netflix** (5 %)
4. **PayPal** (5 %)
5. **Microsoft** (3 %)
6. **Spotify** (3 %)
7. **Apple** (2 %)
8. **Google** (2 %)
9. **Chase** (2 %)
10. **Ray-Ban** (2 %).

**Top tietojenkalastelubrändit alustan mukaan**

Tietojenkalastelussa käytetyt brändit vaihtelivat huomattavasti hyökkäysvektoreittain: esimerkiksi mobiilihyökkäyksissä tietojenkalastelijat keskittyivät suuriin teknologia-alan ja sosiaalisen median brändeihin sekä pankkeihin, kun taas sähköpostihyökkäysten toiseksi suosituin brändi oli osana [ostostietojenkalastelukampanjaa ennen marraskuun 2019 Black Fridayta](https://blog.checkpoint.com/2019/11/26/november-shopping-do-it-the-smart-way/).

Sähköposti (27 % kaikista kalasteluhyökkäyksistä Q4/2019)

1. Yahoo
2. Rbs (Ray-Ban aurinkolasit)
3. Microsoft
4. DropBox.

Verkko (48 % kaikista kalasteluhyökkäyksistä Q4/2019)

1. Spotify
2. Microsoft
3. PayPal
4. Facebook.

Mobiili (25% kaikista kalasteluhyökkäyksistä Q4/2019)

1. Chase Mobile Banking
2. Facebook
3. Apple
4. PayPal.

”Tietoverkkorikolliset käyttävät erilaisia ​​hyökkäysvektoreita huijatakseen uhrinsa luopumaan henkilökohtaisista tiedoista ja kirjautumistiedoista tai siirtämään rahaa. Usein he tekevät sen roskapostien avulla. Olemme myös huomanneet, että hyökkääjät voivat hankkia käyttöoikeustiedot sähköpostitileille, tutkia uhriaan viikkojen ajan ja kohdentaa hyökkäyksiä kumppaneihin ja asiakkaisiin rahaa ​​varastaakseen”, kertoo Check Point Researchin Head of Cyber Research and Threat Intelligence **Maya Horowitz**.

”Kahden viime vuoden aikana tämän tyyppisiin hyökkäyksiin on liittynyt pilvipohjaisen sähköpostin lisääntynyt käyttö, jolloin rikollisten on helpompaa naamioida itsensä luotettavaksi osapuoleksi. Tietojenkalastelu on edelleen kasvava uhka vuonna 2020", Horowitz totaa.

Check Pointin brändihuijausraportti perustuu Check Pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Check Pointin uhkientorjuntaresurssit: <http://www.checkpoint.com/threat-prevention-resources/index.html>.

**Lisätiedot:**

Rami Rauanmaa, tietoturva-asiantuntija, 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:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**Check Point Research**

Check Point Research ([research.checkpoint.com](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. ([www.checkpoint.com](http://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.