Toimitusketjuista sähköpostin kautta mobiiliin: Yksikään ympäristö ei ole immuuni kyberhyökkäyksille

Check Pointin "Cyber Attack Trends: 2019 Mid-Year Report" -raportti paljastaa pankkihaittaohjelmien kehittyneen varsin yleiseksi mobiiliuhaksi. Hyökkäykset ovat lisääntyneet jopa 50% vuodesta 2018.

SAN CARLOS, CA — 26. heinäkuuta 2019 – Tietoturvayhtiö Check Point® Software Technologies julkaisi tänään puolivuotiskatsauksensa kyberhyökkäysten trendeistä. "Cyber Attack Trends: 2019 Mid-Year Report" paljastaa, ettei yksikään toimintaympäristö ole immuuni hyökkäyksille. Hyökkääjät kehittävät jatkuvasti uusia työkaluja ja tekniikoita ja ottavat tähtäimeensä yritysten pilvi-infrastruktuureihin tallennetut tiedot, yksityishenkilöiden mobiililaitteet, luotetut kolmannen osapuolen tavarantoimittajat ja jopa suositut sähköpostialustat:

- Mobiilipankkitoiminnot: Hyökkäysten määrän kasvettua yli 50% vuodesta 2018, pankkihaittaohjelmista on tullut varsin yleinen mobiiluhka. Nykyään pankkihaittaohjelmat pystyvät kalastelemaan uhrin tililtä maksutietoja sekä viemään varoja, ja ohjelmien uusimpia versiota voi massalevittää jokainen, jolla on varaa siitä maksaa.

- Hyökkäykset ohjelmistojen toimitusketjuihin: Hyökkääjät valitsevat kohteitaan uusilta alueilta, kuten keskittymällä toimitusketjuihin. Ohjelmistojen toimitusketjuihin kohdistuvissa hyökkäyksissä tekijä tavallisesti istuttaa haitallisen koodin lailliseen ohjelmistoon. Tällöin yhtä ohjelmiston tärkeistä osista muunnellaan ja saastutetaan.

- Sähköpostipalvelut: Sähköpostihuijarit ovat alkaneet käyttää uudenlaisia tekniikoita ohittaakseen tietoturvajärjestelmät ja roskapostisuodattimet. Niitä ovat esimerkiksi koodatut sähköpostiviestit, kuvana viestiin upotetut viestisisällöt sekä monimutkaiset taustakoodit, joissa tavallisia tekstikirjaimia sekoitetaan HTML-merkkeihin. Muita huijareiden käyttämiä tapoja tietoturvan ja suodattimien ulottumattomissa pysymiseen ovat erilaiset käyttäjän manipulointitekniikat sekä viestisisältöjen personalisointi ja variointi.

- Pilvipalvelut: Pilviympäristöjen kasvava suosio on johtanut siihen, että niihin varastoidut valtavat tietoresurssit ja arkaluontoinen data joutuvat yhä useammin kyberhyökkäysten kohteeksi. Pilvipalvelujen vajavaiset tietoturvakäytännöt kuten kokoonpanon haavoittuvuus ja pilviresurssien huono hallinta ovat myös vuonna 2019 merkittävin uhka pilviekosysteemille. Tämä asettaa pilvivarannot alttiiksi monille erilaisille hyökkäyksille.

"Mikään ympäristö ei ole immuuni kyberhyökkäyksille, oli kyse sitten pilvestä, mobiilista tai sähköpostista. Lisäksi uhat kuten kohdennetut kiristyshaittaohjelmat, DNS-hyökkäykset ja kryptolouhijat ovat huomioon otettavia edelleen vuonna 2019, ja tietoturva-asiantuntijoiden on oltava perillä uusimmista uhista ja hyökkäysmetodeista, jotta yritysten suojaus voidaan pitää parhaalla mahdollisella tasolla", sanoo **Maya Horowitz**, Check Pointin Threat Intelligence & Research Director.

Top 3 -bottiverkot, vuoden 2019 alkupuoli

1. **Emotet (29%) –** Kehittynyt, itsemonistuva ja modulaarinen troijalainen. Tullut laajalti tutuksi pankkitroijalaisena, mutta viime vuodesta lähtien sitä on käytetty myös bottiverkkona laajoissa roskapostikampanjoissa sekä muiden haittaohjelmien jakamisessa. Hyödyntää useita eri keinoja pysyäkseen elinvoimaisena ja kiertotekniikoita ollakseen huomaamaton. Pystyy leviämään haitallisia liitetiedostoja tai linkkejä sisältävien kalastelusähköpostien kautta.
2. **Dorkbot (18%) –** Pankkitroijalainen, joka urkkii uhrin tietoja ja jota käytetään usein myös palvelunestohyökkäysten toteuttamiseen.
3. **Trickbot (11%) –** Troijalainen, joka tunnistettiin lokakuussa 2016. Siitä lähtien kohdistunut pankkipalveluihin lähinnä Australiassa ja Iso-Britanniassa, mutta viime aikoina havaittu myös Intiassa, Singaporessa ja Malesiassa.

Top 3 -kryptolouhijat, vuoden 2019 alkupuoli

1. **Coinhive (23%)** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla. Ilmaantui vasta syyskuussa 2017, mutta on saastuttanut maailmanlaajuisesti 12% yrityksistä.
2. **Cryptoloot (22%)** – Coinhiven kilpailija kryptolouhinnassa.
3. **XMRig (20%)** – Avoimen lähdekoodin laitteille tarkoitettu Monero-louhija, joka tunnistettiin ensi kertaa vuonna 2017.

Top 3 -mobiilihaittaohjelmat, vuoden 2019 alkupuoli

1. **Triada (30%)** – Android-laitteiden takaovi, joka myöntää superkäyttäjäoikeudet haittaohjelmien lataamiseen.
2. **Lotoor (11%)** – Hyväksikäyttää Android-laitteiden haavoittuvuuksia saadakseen pääkäyttäjän oikeudet.
3. **Hidad (7%)** – Ohjelma paketoi Android-sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Se voi levitä laitteen käyttöjärjestelmään ja kerätä hyökkääjälle arkaluontoisia tietoja laitteen käyttäjästä.

Top 3 -pankkihaittaohjelmat, vuoden 2019 alkupuoli

1. **Ramnit (28%)** – Mato, joka leviää etenkin ulkoisten kovalevyjen ja julkisten FTP-palvelinten kautta.
2. **Trickbot (21%)** – Troijalainen, joka tunnistettiin lokakuussa 2016. Siitä lähtien kohdistunut pankkipalveluihin lähinnä Australiassa ja Iso-Britanniassa, mutta viime aikoina havaittu myös Intiassa, Singaporessa ja Malesiassa.
3. **Ursnif (10%)** – Windows-alustoille hyökkäävä troijalainen. Leviää tavallisesti exploit kitien – Anglerin ja Rigin – kautta. Sillä on kyky varastaa Verifone Point-of-Sale-maksuohjelmaan (POS) liittyviä tietoja. Ottaa yhteyttä etäpalvelimeen ladatakseen kerättyjä tietoja ja vastaanottaakseen ohjeita. Lisäksi lataa tiedostoja saastuttamaansa järjestelmään ja asentaa ne.

Check Pointin kyberhyökkäyksiin pureutuva puolivuotisraportti tarjoaa yksityiskohtaisen katsauksen kyberuhkien maailmaan. Raportti perustuu Check Point ThreatCloudin™ keräämiin tietoihin tammikuun ja kesäkuun 2019 välisenä aikana. Se nostaa esiin hakkereiden eniten suosimat tavat hyökätä yrityksiä vastaan.

Raportin täysversio on saatavissa täällä.

Seuraa Check Pointia:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blogi: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Lisätiedot ja haastattelupyynnöt:
Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com
Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065

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.

