Listakärjessä pankkirosvo Qbot, lohkoketjua hyödyntävä Glubteba teki paluun – Yleisimmät haittaohjelmat Suomessa ja maailmalla

Check Point Research kertoo joulukuun haittaohjelmakatsauksessaan, että Qbot ohitti Emotetin maailman yleisimpänä haittaohjelmana, mutta säilytti sijansa Suomen listaykkösenä. Check Point muistuttaa, että haittaohjelmat naamioituvat usein laillisiksi, sovelluskaupoissa julkaistuiksi ohjelmistoiksi.

ESPOO – 18. tammikuuta 2023 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research (CPR) on julkaissut joulukuun 2022 haittaohjelmakatsauksensa.

CPR kertoo, että kehittynyt troijalainen Qbot, joka varastaa pankkitunnuksia ja näppäinpainalluksia, ohitti Emotetin maailman yleisimpänä haittaohjelmana vaikuttaen joulukuussa seitsemään prosenttiin organisaatioista maailmanlaajuisesti. Paluun yleisimpien haittaohjelmien globaalille listalle tekivät lohkoketjua hyödyntävä troijalainen bottiverkko Glupteba sekä Android-haittaohjelma Hiddad.

Vaikka Google onnistui aiheuttamaan suurta häiriötä Glupteban toiminnalle joulukuussa 2021, se näyttää taas jatkavan toimintaansa. Modulaarisena haittaohjelmaversiona Glupteba voi aiheuttaa monenlaista haittaa tartunnan saaneella koneella. Bottiverkkoa käytetään usein muiden haittaohjelmien jakeluun ja lataamiseen, joten Glupteba-tartunta voi johtaa niin tietovarkauksiin ja kiristysohjelmatartuntaan kuin kryptolouhintaan uhrin koneella.

Hiddad nousi joulukuussa myös mobiilihaittaohjelmien kolmen kärkeen ensimmäistä kertaa vuonna 2022. Android-laitteisiin kohdistuva, mainoksia levittävä haittaohjelma paketoi lailliset sovellukset uudelleen ja julkaisee ne sovelluskaupassa.

”Uusimman tutkimuksemme toistuva teema on se, että haittaohjelmat usein naamioituvat laillisiksi ohjelmistoiksi pyrkimyksenään avata hakkereille takaovi laitteisiin epäilyksiä herättämättä. Siksi on tärkeää olla valppaana ohjelmistoja ja sovelluksia ladatessa tai linkkejä klikatessa riippumatta siitä, kuinka aidoilta ne näyttävät,” muistuttaa **Maya Horowitz**, VP Research Check Point Softwarelta.

Toimialoista joulukuussa hyökättiin Euroopan- ja maailmanlaajuisesti eniten koulutus-/tutkimusalaan, Pohjoismaissa valtionhallintoon/puolustusvoimiin.

Suomen yleisimmät haittaohjelmat joulukuussa 2022:

1. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 3,76 %.
2. **Remcos** – Etäkäyttötroijalainen eli RAT, joka havaittiin ensimmäisen kerran vuonna 2016. Se leviää roskapostien liitteinä olevien Microsoft Office -dokumenttien mukana ja se on suunniteltu ohittamaan Microsoft Windowsin käyttäjätilien valvonta (UAC) sekä käynnistämään haittaohjelmia. Esiintyvyys 3,23 %.

3. **Qbot** (eli Qakbot) – Ensimmäisen kerran vuonna 2008 havaittu pankkitroijalainen, joka varastaa uhrin pankkitunnuksia ja tallentaa näppäinpainalluksia. Qbotia levitetään yleensä roskapostiviestien välityksellä. Esiintyvyys 2,69 %.
4. **XMRig** – Monero-kryptovaluutan louhija. Uhkatoimijat väärinkäyttävät usein tätä avoimen lähdekoodin ohjelmistoa ja integroivat sen haittaohjelmiin louhiakseen laittomasti uhrien laitteilla. Esiintyvyys 2,69 %.
5. **Nanocore** – Etäkäyttöön tarkoitettu troijalainen, joka on suunnattu Windows-käyttöjärjestelmän käyttäjille. Esiintyvyys 2,15 %.
6. **GhOst** – Backdoor.Win32.Ghost on Windows-alustaan kohdistuva takaovi. Haittaohjelma on suunniteltu antamaan vilpilliselle käyttäjälle tartunnan saaneen tietokoneen etähallinta. Esiintyvyys 1,61 %.
7. **Amadey** – Troijalainen botti, joka havaittiin ensimmäisen kerran lokakuussa 2018. Tietovaras, joka kykenee myös jakelemaan muita haittaohjelmia. Esiintyvyys 1,61 %.
8. **Formbook** – Windows-järjestelmien haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 1,61 %.

9–11. **Scrinject**, **Cuba**, **Hiddad** – Kaikkien esiintyvyys 1,08 %.

Maailman yleisimmät haittaohjelmat joulukuussa 2022:

1. **Qbot** (AKA **Qakbot**) – Ensimmäisen kerran vuonna 2008 havaittu pankkitroijalainen, joka varastaa uhrin pankkitunnuksia ja tallentaa näppäinpainalluksia. Qbotia levitetään yleensä roskapostiviestien välityksellä. Esiintyvyys 7 %.
2. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 4 %.
3. **XMRig** – Monero-kryptovaluutan louhija. Uhkatoimijat väärinkäyttävät usein tätä avoimen lähdekoodin ohjelmistoa ja integroivat sen haittaohjelmiin louhiakseen laittomasti uhrien laitteilla. Esiintyvyys 3 %.

Mobiilihaittaohjelmien globaalilla listalla ensimmäisenä oli pankki- ja etäkäyttötroijalainen **Anubis**, joka on suunnattu Android-puhelimiin. Kiristysohjelmaominaisuuksillakin varustettu Anubis kykenee tallentamaan myös ääntä ja näppäinpainalluksia. Sitä on havaittu sadoissa Google Storen sovelluksissa. Toisella sijalla oli **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia. Kolmantena oli **AlienBot**, joka on palveluna myytävä Android-haittaohjelma (malware-as-a-service). Se sallii hyökkääjän ujuttaa pankkisovelluksiin haitallista koodia, jolloin hyökkääjä saa pääsyn uhrin tileille ja lopulta koko laitteen hallinnan.

Check Pointin tutkijat listasivat myös joulukuun käytetyimmät **haavoittuvuudet**. Yleisin haavoittuvuus oli **”Web Server Exposed Git Repository Information Disclosure”**, jota on yritetty hyödyntää 46 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli nimeltään **”Web Servers Malicious URL Directory Traversal”** (CVE-2010-4598, CVE-2011-2474, CVE-2014-0130, CVE-2014-0780, CVE-2015-0666, CVE-2015-4068, CVE-2015-7254, CVE-2016-4523, CVE-2016-8530, CVE-2017-11512, CVE-2018-3948, CVE-2018-3949, CVE-2019-18952, CVE-2020-5410, CVE-2020-8260), ja sen esiintyvyys oli 44 prosenttia. Kolmannella sijalla oli **”Command Injection Over http”** (CVE-2021-43936, CVE-2022-24086), jonka esiintyvyys oli 43 prosenttia.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin™ tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä Check Pointin tietoturvalaitteilta kautta maailman ja näyttää ne reaaliaikaisesti kartalla. ThreatCloud-tietokanta tarkastaa yli 3 miljardia verkkosivustoa ja 600 miljoonaa tiedostoa sekä tunnistaa yli 250 miljoonaa haittaohjelmatoimintaa päivittäin.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista: December 2022's Most Wanted Malware: Glupteba Entering Top Ten and Qbot in First Place

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa https://www.checkpoint.com/.

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

