Emotet-troijalainen kiertää nyt Microsoftin estot OneNote-tiedostojen avulla – Nämä olivat maaliskuun yleisimmät haittaohjelmat Suomessa ja maailmalla

Check Point Researchin maaliskuun haittaohjelmakatsaus kertoo, että kyberrikolliset ovat kehittäneet keinon Microsoftin makrokiellon kiertämiseen: Emotet-troijalaista levittävissä roskaposteissa on nyt mukana haitallisia OneNote-linkkejä. Suomessa Emotet oli maaliskuun kolmanneksi yleisin haittaohjelma.

ESPOO – 12. huhtikuuta 2023 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research (CPR) on julkaissut maaliskuun 2023 haittaohjelmakatsauksensa. Sen tärkeimpiin havaintoihin kuuluu uusi Emotet-troijalaista levittävä haittaohjelmakampanja, jonka myötä Emotet nousi maailman toiseksi yleisemmäksi haittaohjelmaksi. Suomessa Emotet oli kolmanneksi käytetyin haittaohjelma maaliskuussa.

CPR:n tutkijat huomasivat jo aiemmin tätä vuonna, että kyberrikolliset ovat tutkineet uusia tapoja haitallisten tiedostojen levittämiseen sen jälkeen, kun Microsoft ilmoitti estävänsä sähköpostin kautta tai muualta internetistä tulleissa Office-tiedostoissa olevien makrojen avaamisen. Uusimmassa kampanjassa on käytössä uusi strategia: roskapostiviestit sisältävät haitallisen OneNote-tiedoston. Kun tiedosto avataan, näkyviin tulee väärennetty viesti, joka houkuttelee klikkaamaan asiakirjaa. Napsautus lataa Emotet-tartunnan. Haittaohjelma voi kerätä uhrin sähköpostiohjelmasta esimerkiksi kirjautumistietoja ja yhteystietoja. Nämä ovat rikolliselle arvokas apu kampanjan laajentamisessa ja myöhempien hyökkäysten valmistelussa.

”Microsoftin kaltaiset isot teknologiayritykset tekevät parhaansa estääkseen kyberrikollisten aikeet jo varhaisessa vaiheessa, mutta on käytännössä lähes mahdotonta pysäyttää jokaista hyökkäystä. Emotet on tunnetusti hienostunut troijalainen, eikä ole yllätys, että se on onnistunut luovimaan Microsoftin uusimpien suojausten ohi. Tärkeintä, mitä jokainen voi tehdä, on varmistaa, että sähköpostin suojaukset ovat asianmukaiset. Odottamatta saatuja tiedostoja ei pidä ladata koneelle, ja sähköpostien alkuperään ja sisältöön on syytä suhtautua terveen epäluuloisesti”, sanoo Check Point Softwaren tutkimusjohtaja **Maya Horowitz**.

Suomen yleisimmät haittaohjelmat maaliskuussa 2023:

1. **Qbot** (eli Qakbot) – Ensimmäisen kerran vuonna 2008 havaittu pankkitroijalainen, joka varastaa uhrin pankkitunnuksia ja tallentaa näppäinpainalluksia. Qbotia levitetään yleensä roskapostiviestien välityksellä. Esiintyvyys 6,90 %.
2. **XMRig** – Monero-kryptovaluutan louhija. Kyberkonnat väärinkäyttävät usein tätä avoimen lähdekoodin ohjelmistoa ja integroivat sen haittaohjelmiin louhiakseen laittomasti uhrien laitteilla. Esiintyvyys 4,02 %.
3. **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 3,45 %.

4. **Remcos** – Etähallintaohjelma (RAT), joka havaittiin ensimmäisen kerran vuonna 2016. Se leviää roskapostien liitteinä olevien Office -tiedostojen avulla ja se on suunniteltu välttämään Microsoftin virustutkat. Esiintyvyys 2,87 %.
5. **OffLoader** – Tunnetaan haitallisten ohjelmien lataajana ja suorittajana, joka pystyy nappaaman arkaluonteisia tietoja ja kuvakaappauksia. Leviää roskapostitusten ja väärennettyjen ohjelmistopäivitysten avulla. Esiintyvyys 2,30 %.

6–10. **Anubis**, **Formbook**, **GhOst, Shiz ja Zegost** – Kaikkien esiintyvyys 1,72 %.

Maailman yleisimmät haittaohjelmat maaliskuussa 2023:

1. **Qbot** (eli **Qakbot**) – Ensimmäisen kerran vuonna 2008 havaittu pankkitroijalainen, joka varastaa uhrin pankkitunnuksia ja tallentaa näppäinpainalluksia. Qbotia levitetään yleensä roskapostiviestien välityksellä. Esiintyvyys 10 %.
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. **Formbook** – Windows-järjestelmien haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 4 %.

Mobiilihaittaohjelmien globaalilla listalla ensimmäisenä oli etäkäyttötroijalainen (RAT) **AhMyth**, joka havaittiin ensimmäisen kerran vuonna 2017. Sitä levitetään sovelluskaupoista ja useilta sivustoilta löytyvissä Android-sovelluksissa. Toiseksi yleisin 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. Listakolmonen oli **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia.

Check Pointin tutkijat listasivat myös maaliskuun käytetyimmät **haavoittuvuudet**. Yleisin haavoittuvuus oli **Apache Log4j Remote Code Execution (CVE-2021-44228)**, jota on yritetty hyödyntää 44 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli nimeltään **HTTP Headers Remote Code Execution (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756)**, jonka esiintyvyys oli 43 prosenttia. Kolmannella sijalla oli **MVPower DVR Remote Code Execution**, jonka esiintyvyys oli 40 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: March 23's Most Wanted Malware

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.

Haastattelu- ja kuvapyynnöt:
Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065.

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.

