Haittaohjelmien top 10: Trickbot yhä ykkönen maailmalla – Flubot kalastelee suomalaisten tietoja tekstiviesteissä

Tietoturvayhtiö Check Pointin tutkijat kertovat, että Trickbot oli heinäkuussa maailman yleisin haittaohjelma jo kolmatta kuukautta peräkkäin. Toiseksi yleisin, Snake Keylogger, ylsi globaaliin kärkikymmenikköön ensimmäistä kertaa. Suomalaisia piinasi logistiikkayritykseksi naamioituva Flubot.

ESPOO – 12. elokuuta 2021 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research on julkaissut heinäkuun haittaohjelmakatsauksensa.

Tutkijat kertovat, että Trickbot säilytti paikkansa maailman yleisimpänä haittaohjelmana myös heinäkuussa. Snake Keylogger, joka havaittiin ensimmäisen kerran marraskuussa 2020, on noussut toiselle sijalle intensiivisen tietojenkalastelukampanjan jälkeen.

Snake Keylogger on modulaarinen .NET -keylogger eli näppäilytallennin sekä kirjautumistietojen varastaja. Sen ensisijainen tehtävä on tallentaa uhrin tietokoneen tai mobiililaitteen näppäinpainallukset ja välittää kerätyt tiedot ulkopuolisille. Snake on yleistynyt nopeasti viime viikkoina eri aiheisten tietojenkalastelusähköpostien kautta ympäri maailmaa kaikilla liiketoiminta-alueilla.

Snake-tartunnat uhkaavat käyttäjien yksityisyyttä ja verkkoturvallisuutta, koska haittaohjelma voi varastaa käytännössä kaikenlaisia arkaluonteisia tietoja. Tällä hetkellä Snake Keylogger on ostettavissa underground-hakkerointifoorumeilla 25–500 dollarin hintaan tarjottavan palvelun tasosta riippuen.

Keylogger-hyökkäykset voivat olla erityisen vaarallisia, sillä monilla on tapana käyttää samaa salasanaa ja käyttäjätunnusta useilla eri tileillä. Kun yksi kirjautumistunnus on murrettu, verkkorikollinen voi päästä käsiksi kaikkiin samaa tunnusta käyttäviin tileihin. Tämän estämiseksi jokaisella tilillä tulisi käyttää eri tunnusta. Salasanojen hallintaohjelman (password manager) avulla voidaan sekä hallita että luoda erilaisia luotettavia yhdistelmiä kullekin palvelulle.

”Jos mahdollista, käyttäjien tulisi vähentää riippuvuuttaan pelkistä salasanoista esimerkiksi ottamalla käyttöön monivaiheinen tunnistautuminen tai kertakirjautuminen”, sanoo Check Point Softwaren Suomen ja Baltian maajohtaja **Sampo Vehkaoja**.

”Salasanakäytäntöjen osalta paras neuvo on valita vahva, ainutlaatuinen salasana kullekin palvelulle. Vaikka pahantekijät sitten saisivatkin jonkun salasanasi haltuunsa, se ei anna heille heti pääsyä useisiin sivustoihin ja palveluihin. Snaken kaltaisia näppäilytallentimia levitetään usein tietojenkalastelusähköpostien välityksellä, joten on tärkeää osata varoa pieniä eroavaisuuksia, kuten kirjoitusvirheitä linkeissä ja sähköpostiosoitteissa. Ei myöskään koskaan kannata klikata epäilyttäviä linkkejä tai avata tuntemattomia liitteitä”, muistuttaa **Maya Horowitz**, Check Point Softwaren tutkimusjohtaja.

Suomen yleisin haittaohjelma heinäkuussa oli Flubot, jota esiintyi 1,8 prosentissa maan yritysverkoista. Trickbot oli Suomen kahdeksanneksi yleisin haittaohjelma.

Suomen yleisimmät haittaohjelmat heinäkuussa 2021:

1. **Flubot** – Android-haittaohjelma, jota levitetään tietojenkalastelutekstiviestien välityksellä ja joka esiintyy useimmiten logistiikkayrityksenä (kuten viime aikoina DHL). Kun käyttäjä klikkaa viestissä olevaa linkkiä, FluBot asennetaan ja hakkeri saa pääsyn puhelimen arkaluonteisiin tietoihin. Esiintyvyys 1,8 %.
2. **REvil** – Ensimmäistä kertaa vuonna 2019 havaittu, palveluna myyty kiristyshaittaohjelma (ransomware-as-a-service), joka salakirjoittaa uhrinsa tiedostot ja vaatii lunnaita niiden palauttamisesta. Esiintyvyys 0,9 %.
3. **Darkside** – RaaS eli palveluna ostettava kiristyshaittaohjelma tunnetaan hyökkäyksistään hieman harvinaisempiin kohteisiin, kuten öljy- ja kaasuyhtiöiden palvelimiin. Esiintyvyys 0,9 %.
4. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 0,9 %.
5. **Guloader** – Haittaohjelmien lataaja, jota on käytetty laajalti joulukuusta 2019 lähtien. Esiintyvyys 0,9 %.
6. **PsKill** – Esiintyvyys 0,9 %.
7. **Zloader** – Haittaohjelma, joka varastaa pankkitunnusten lisäksi uhrin verkkoselaimiin tallennettuja salasanoja ja evästeitä. Esiintyvyys 0,9 %.
8. **TrickBot** – Windows-alustaan kohdistettu, pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, jota levitetään lähinnä roskapostikampanjoiden tai muiden haittaohjelmaperheiden kautta. Esiintyvyys 0,9 %.
9. **Ursnif** – 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. Esiintyvyys 0,9 %.
10. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 0,9 %.

Maailman yleisimmät haittaohjelmat ja haavoittuvuudet heinäkuussa 2021:

1. **Trickbot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, joka saa jatkuvasti uusia päivityksiä. Esiintyvyys 4 %.
2. **Snake Keylogger** – Modulaarinen .NET -näppäilytallennin ja kirjautumistietojen varastaja, joka havaittiin ensimmäisen kerran marraskuussa 2020. Tallentaa uhrin näppäinpainallukset ja lähettää kerätyn datan ulkopuolisille. Esiintyvyys 3 %.
3. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 3 %.

Mobiilihaittaohjelmien globaalilla listalla ensimmäisenä oli **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta sekä asentamaan itsensä uudelleen, jos käyttäjä poistaa sen. Toisella sijalla oli **AlienBot**, joka on palveluna myytävä Android-haittaohjelma (malware-as-a-service). Se sallii hyökkääjän ujuttaa pankkisovelluksiin haitallista koodia, jolloin hyökkääjä saa pääsyn uhrien tileille ja lopulta koko laitteen hallinnan. Kolmannella sijalla oli Android-haittaohjelma **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia.

Check Pointin tutkijat listasivat myös heinäkuun käytetyimmät **haavoittuvuudet**. Yleisintä haavoittuvuutta nimeltään **”Web Server Exposed Git Repository Information Disclosure”** on yritetty hyödyntää 45 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 44 %. Kolmannella sijalla oli **”MVPower DVR Remote Code Execution”**, jonka esiintyvyys oli 42 %.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin™ tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä 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.
Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa www.checkpoint.com.

Lisätiedot:
Sampo Vehkaoja, Country Manager, Finland and Baltics, Check Point Software Technologies, sampov@checkpoint.com, p. 050 555 5500
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 (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) 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. Siihen sisältyvät Check Point Harmony etäkäyttäjille, Check Point CloudGuard pilven automaattiseen suojaukseen ja Check Point Quantum datakeskusten suojaukseen. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.