Haittaohjelmien Top 10 toukokuussa:
Snake Keylogger luikertelee nyt uhrien laitteille PDF-tiedostojen mukana

Check Point Research kertoo toukokuun haittaohjelmakatsauksessaan, että käyttäjien näppäinpainalluksia taltioiva Snake Keylogger on palannut käytetyimpien haittaohjelmien listalle saavuttaen sijan 8. Listan ykkössijaa pitää edelleen teknisesti edistynyt troijalainen Emotet, jonka levinneisyys on jopa hieman kasvanut viime kuukaudesta.

ESPOO – 9. kesäkuuta 2022 -- Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research (CPR) on julkaissut toukokuun 2022 haittaohjelmakatsauksensa. Tutkijat raportoivat, että useat isot levityskampanjat nostivat kehittyneen, itsestään monistuvan ja modulaarisen Emotet-troijalaisen haittaohjelmalistan kärkeen. Sen esiintyvyys oli 8 % organisaatioista kautta maailman, kun se edellisessä kuussa oli 6 %.

Snake Keyloggerin päätoiminto on uhrin näppäintoimintojen tallentaminen ja kerättyjen tietojen lähettäminen toimeksiantajalle. Haitake on yleensä levinnyt sähköpostien liitteinä olevien, makroja sisältävien tekstitiedostojen kautta, mutta viime kuussa tutkijat havaitsivat sen luikertelevan uhrien laitteille PDF-tiedostojen mukana. Uusi toimintatapa voi johtua siitä, että Microsoft estää nykyään oletusarvoisesti makrot Office-ohjelmissa. Kyberrikollisten on ollut pakko kehittää uusia, luovia keinoja. Uusi levitystapa on todennäköisesti ollut tehokas, koska monet pitävät PDF-tiedostoja turvallisempina kuin Word-tiedostoja.

Emotet on monitaitoinen haittaohjelma, joka välttelee ketterästi tietoturvaohjelmistoja. Sinnikkyytensä ansiosta se jää helposti huomaamatta ja poistamatta laitteelta, mikä tekee siitä loistavan välineen kyberrikollisten työkalupakkiin. Emotet leviää yleisimmin haitallisia linkkejä tai liitteitä sisältävien sähköpostiviestien välityksellä. Se pystyy toimimaan väylänä myös muille haittaohjelmille, mikä tekee siitä vielä vaarallisemman.

”Uudet Snake Keylogger -kampanjat osoittavat, että kaikki, mitä teemme tietoverkossa, altistaa kyberhyökkäyksille. Tämä pätee myös PDF-tiedoston avaamiseen”, sanoo Check Pointin tutkimusjohtaja **Maya Horowitz**.

”Virukset ja haittakoodit voivat olla piilossa tiedoston multimediasisällössä ja linkeissä, ja ne ovat valmiina iskemään, kun käyttäjä avaa tiedoston. Sähköpostien PDF-liitteisiin pitää suhtautua samalla varovaisuudella kuin docx- tai xlsx-liitteisiin. Nyt on tärkeämpää kuin koskaan, että yrityksillä ja organisaatioilla on käytettävissään sähköpostit turvaava vankka tietoturvaratkaisu, joka ottaa viestit karanteeniin, tarkistaa liitetiedostot ja estää haitallisten sisältöjen pääsyn yritysverkkoon”, hän jatkaa.

CPR:n mukaan koulutus- ja tutkimusala oli toukokuussa edelleen eniten hyökkäysten kohteena oleva ala globaalisti. Pohjoismaissa kyberhyökkäyksiä tehtiin varsin tasaisesti eri aloille.

Suomen yleisimmät haittaohjelmat toukokuussa2022:

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 2,21 %.
2. **Remcos** – Jakaa haittaohjelmia roskaposteihin liitettyjen Microsoft Office -asiakirjojen kautta ja osaa väistellä Microsoftin tietoturvaa. Esiintyvyys 2,21 %.
3. **GhOst** – Windows-laitteiden takaovi, jonka kautta asiaton tunkeutuja pääsee etäkäyttämään uhrin tietokonetta. Esiintyvyys 2,21 %.
4. **Fujacks** – Mato, joka tarttuu laitteesta toiseen internetistä ladattujen sisältöjen, USB-tikkujen ja pikaviestien kautta. Esiintyvyys 1,33 %.
5. **Netwalker** (tunnetaan myös nimellä **Mailto**) – Päivitetty versio Kokoklock-kiristyshaittaohjelmasta, joka leviää enimmäkseen tietojenkalastelusähköpostien kautta. Esiintyvyys 1,33 %.

Maailman yleisimmät haittaohjelmat tammikuussa 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 8 %.
2. **Formbook** – Windows-järjestelmien haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 2 %.
3. **Agent Tesla** – Edistyksellinen etäkäyttötroijalainen, joka pystyy esimerkiksi uhrinsa näppäinpainalluksia seuraamalla ja kuvakaappauksia ottamalla pääsemään käsiksi WiFi-salasanoihin ja muihin kohdelaitteen tietoihin (esimerkiksi Outlook-sähköposti, Google Chrome ja Mozilla Firefox). Esiintyvyys 2 %.

Mobiilihaittaohjelmien globaalilla listalla ensimmäisenä 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. Toisena oli Android-haittaohjelma **FluBot**, joka esiintyy usein logistiikkayrityksenä ja jota levitetään tietojenkalastelutekstiviestien välityksellä. Kun käyttäjä klikkaa viestissä olevaa linkkiä, FluBot asennetaan ja hakkeri saa pääsyn puhelimen arkaluonteisiin tietoihin. Kolmanneksi ylsi **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta sekä asentamaan itsensä uudelleen, jos käyttäjä poistaa sen.

Hyödynnetyimpien haavoittuvuuksien listaykkösenä oli tällä kertaa **Web Servers Malicious URL Directory Traversal**, jota yritettiin käyttää 46 prosentissa maailman yrityksistä ja organisaatioista. Ykkössijan jakoi sen kanssa **Apache Log4j Remote Code Execution**" (CVE-2021-44228), esiintyvyys 46 prosenttia. Kolmanneksi hyödynnetyin haavoittuvuus oli **Web Server Exposed Git Repository Information Disclosure**, jonka globaali esiintyvyys oli 45 prosenttia.

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.

