Yleisimmät haittaohjelmat ja haavoittuvuudet Suomessa ja maailmalla – Varo pääsiäisaiheisia viestejä

Check Point Research kertoo maaliskuun haittaohjelmakatsauksessaan, että maailman yleisin haitake oli yhä Emotet, jota esiintyy jo joka kymmenennessä yritysverkossa maailmanlaajuisesti. Suomen yleisimpänä kyberkiusana jatkoi kiristysohjelma Netwalker. Pohjoismaissa hyökkäysten kohteena olivat useimmin valtionhallinto ja puolustusvoimat. Check Point varoittaa myös pääsiäisteemaisista tietojenkalasteluviesteistä.

ESPOO – 12. huhtikuuta 2022 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research (CPR) on julkaissut maaliskuun 2022 haittaohjelmakatsauksensa. Tutkijat raportoivat, että Emotet jatkaa voittokulkuaan suosituimpana haittaohjelmana ja vaikuttaa jo 10 prosenttiin organisaatioista maailmanlaajuisesti. Määrä on kaksinkertainen helmikuuhun verrattuna.

Emotet on kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään pääasiassa muiden haittaohjelmien levittämiseen. Se väistelee virustutkia ja poistoyrityksiä ja pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Bottiverkkoa ovat levittäneet useat aggressiiviset sähköpostikampanjat, kuten erilaiset pääsiäisaiheiset tietojenkalasteluhuijaukset. Ympäri maailmaa lähetettyjen sähköpostien aiheena on ollut esimerkiksi "*buona pasqua*, hyvää pääsiäistä", ja sähköpostin liitteenä on ollut haitallinen XLS-tiedosto Emotetin toimittamiseksi.

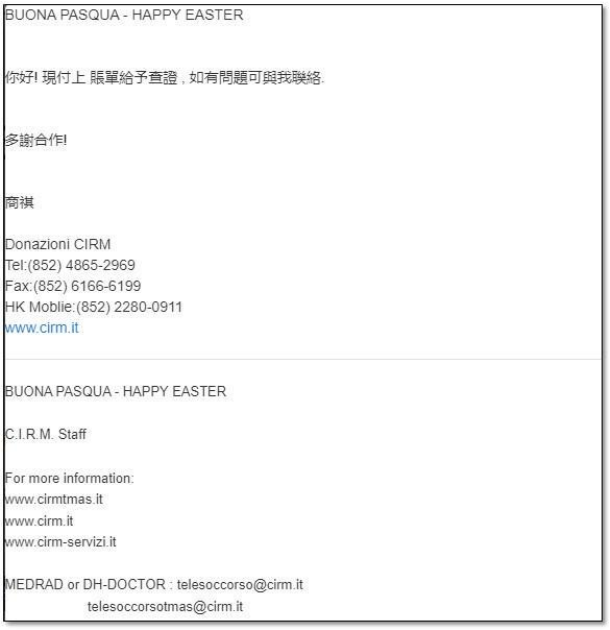
Maaliskuun toiseksi yleisin haittaohjelma oli Agent Tesla, edistyksellinen etäkäyttötroijalainen, joka pystyy esimerkiksi uhrinsa näppäinpainalluksia seuraamalla pääsemään käsiksi kohdelaitteen tietoihin. Agent Teslan nousu johtuu useista uusista, haitallisia xlsx-/pdf-tiedostoja levittävistä roskapostikampanjoista, joista osa on käyttänyt houkuttimena Ukrainan sotaa.

”Teknologia on edennyt viime vuosina siihen pisteeseen, että kyberrikolliset ovat entistä enemmän ihmisten luottavaisuuden varassa yrityksen verkkoon päästääkseen. Teemoittamalla tietojenkalastelusähköpostinsa juhla-aikojen, kuten pääsiäisen, mukaan, he voivat hyödyntää kuhinaa niiden ympärillä ja houkutella uhreja lataamaan haittaohjelmia sisältäviä liitteitä. Pääsiäisviikonloppuna odotamme lisää tällaisia huijauksia ja kehotamme ihmisiä olemaan tarkkana, vaikka sähköposti näyttäisikin olevan peräisin hyvämaineiselta lähettäjältä. Pääsiäinen ei ole ainoa yleinen vapaapäivä, ja verkkorikolliset käyttävät jatkossakin samaa taktiikkaa”, toteaa VP Research **Maya Horowitz** Check Point Softwarelta.

"Havaitsimme myös Apache Log4j:n nousevan jälleen eniten hyödynnetyksi haavoittuvuudeksi. Kaiken loppuvuoden kohun jälkeenkin se aiheuttaa haittaa vielä kuukausia havaitsemisensa jälkeen. Organisaatioiden on ryhdyttävä välittömiin toimiin hyökkäysten estämiseksi."

CPR:n mukaan maailmanlaajuisesti eniten hyökkäyksiä kohdistui maaliskuussa koulutus- ja tutkimusaloille, joita seurasivat valtionhallinto/puolustusvoimat ja ISP/MSP-palveluntarjoajat. Pohjoismaissa hyökkäyksiä kohdistui eniten hallintoon ja maanpuolustukseen, ja niitä seurasivat viestintä ja kuljetusala.

Esimerkkejä pääsiäisteemaisista tietojenkalasteluviesteistä



BUONA PASQUA - HAPPY EASTER

你好! 現付上 賬單給予查證，如有問題可與我聯絡.

多謝合作!

商祺

Donazioni CIRM
Tel:(852) 4865-2969
Fax:(852) 6166-6199
HK Moblie:(852) 2280-0911
www.cirm.it

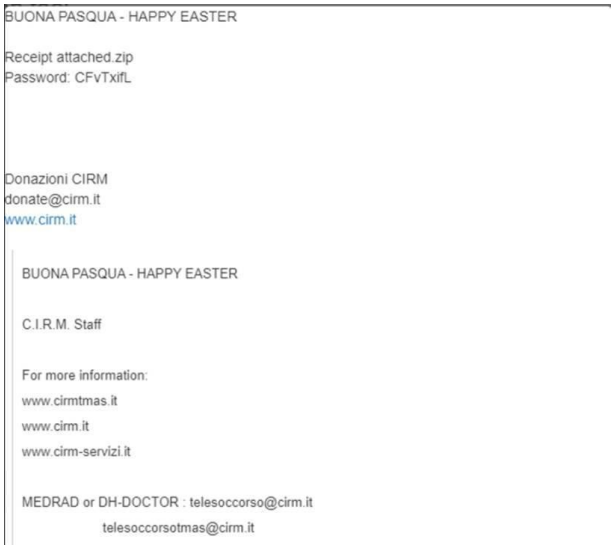
BUONA PASQUA - HAPPY EASTER

C.I.R.M. Staff

For more information:
www.cirmtmas.it
www.cirm.it
www.cirm-servizi.it

MEDRAD or DH-DOCTOR : telesoccorso@cirm.it
telesoccorsotmas@cirm.it

Kuva 1 Esimerkki japanilaisesta pääsiäisen tietojenkalastelusähköpostista



BUONA PASQUA - HAPPY EASTER

Receipt attached.zip
Password: CFvTxifL

Donazioni CIRM
donate@cirm.it
www.cirm.it

BUONA PASQUA - HAPPY EASTER

C.I.R.M. Staff

For more information:
www.cirmtmas.it
www.cirm.it
www.cirm-servizi.it

MEDRAD or DH-DOCTOR : telesoccorso@cirm.it
telesoccorsotmas@cirm.it

Kuva 2 Esimerkki pääsiäisen tietojenkalasteluviestistä, joka on lähetetty useisiin eri maihin

Suomen yleisimmät haittaohjelmat maaliskuussa 2022:

1. **Netwalker** (tunnetaan myös nimellä **Mailto**) – Päivitetty versio Kokoklock-kiristyshaittaohjelmasta, joka leviää enimmäkseen tietojenkalastelusähköpostien kautta. Esiintyvyys 7,36 %.
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 3,03 %.
3. **Glupteba** – Vuonna 2011 löydetty takaovi, joka on vähitellen kehittynyt bottiverkoksi. Esiintyvyys 2,16 %.
4. **Revenge RAT** – Windows-troijalainen, joka hyväksyy komentoja etäkäyttöpalvelimelta ja voi mm. kerätä järjestelmätietoja, suorittaa/päivittää tiedoston linkistä tai levyltä, ladata lisäosia sekä sulkea/käynnistää uudelleen haittaohjelman. Esiintyvyys 2,16 %.
5. **XMRig** – Monero-kryptovaluutan louhija. Uhkatoimijat usein väärinkäyttävät tätä avoimen lähdekoodin ohjelmistoa ja integroivat sen haittaohjelmiin suorittaakseen laitonta louhintaa uhrien laitteilla. Esiintyvyys 2,16 %.
6. **Banload** – Troijalainen, joka lataa ei-toivottuja tiedostoja etäpalvelimista uhrien koneeseen. Esiintyvyys 2,16 %.

Maailman yleisimmät haittaohjelmat maaliskuussa 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 10 %.
2. **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 %.
3. **XMRig** – Monero-kryptovaluutan louhija. Uhkatoimijat usein väärinkäyttävät tätä avoimen lähdekoodin ohjelmistoa ja integroivat sen haittaohjelmiin suorittaakseen laitonta louhintaa uhrien laitteilla. 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. Toisella sijalla 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. Kolmantena oli Android-haittaohjelma Flubot, joka esiintyy usein logistiikkayrityksenä ja jota levitetään tietojenkalastelutekstiviestien (*smishing*) välityksellä. Kun käyttäjä klikkaa viestissä olevaa linkkiä, FluBot asennetaan ja hakkeri saa pääsyn puhelimen arkaluonteisiin tietoihin.

Check Pointin tutkijat listasivat myös maaliskuun käytetyimmät **haavoittuvuudet**. Yleisin haavoittuvuus oli ”**Apache Log4j Remote Code Execution**” (CVE-2021-44228)”, jota on yritetty hyödyntää 33 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli nimeltään ”**Web Server Exposed Git Repository Information Disclosure**”, ja sen esiintyvyys oli 26 %. Kolmannella sijalla oli ”**HTTP Headers Remote Code Execution**” (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-13756), jonka esiintyvyys oli 26 %.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista: blog.checkpoint.com.

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.

