Yleisimmät haittaohjelmat:
Uusi Qbot näyttää jatkavan aiempaa sähköpostikeskustelua

Tietoturvayhtiö Check Pointin tutkijat kertovat, että roskapostikampanjat levittävät nyt ahkerasti Qbot-haittaohjelman uutta, tuhoisampaa versiota. Sen tavoitteina ovat salasanojen ja luottokorttitietojen varastaminen, kiristysohjelmien asentaminen ja luvattomien tilitapahtumien tekeminen. Maailman yleisin haittaohjelma, Emotet, on ampaissut Suomen listakakkoseksi.

ESPOO – 10. syyskuuta 2020 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research kertoo haittaohjelmakatsauksessaan, että Qbot-troijalainen, joka tunnetaan myös nimellä Qakbot ja Pinkslipbot, on ensimmäistä kertaa yltänyt maailman kymmenen yleisimmän haittaohjelman joukkoon. Yleisin haittaohjelma on yhä Emotet-troijalainen, jota esiintyy 14 prosentissa yritysverkoista maailmanlaajuisesti.

Ensimmäistä kertaa vuonna 2008 havaittua Qbotia on kehitetty jatkuvasti. Haittaohjelma on erityisen monipuolinen edistyneiden kiristysohjelma- ja tietovarkaustekniikoidensa ansiosta. Niihin lukeutuu myös uusi sähköpostinkeräysmoduuli, jonka avulla Qbot voi kaapata aitoja sähköpostikeskusteluja tartunnan saaneiden käyttäjien Outlook-ohjelmasta. Näin Qbot tavoittelee uusia uhreja viesteillä, jotka näyttävät jatkavan aiempaa keskustelua. Qbot kykenee myös luvattomiin tilitapahtumiin.

Check Pointin tutkijat havaitsivat maalis-elokuussa useita kampanjoita, joissa Qbotin uutta versiota käytettiin myös Emotet-troijalaisen jakamana. Heinäkuussa 2020 tätä esiintyi viidessä prosentissa organisaatioista maailmanlaajuisesti.

”Kyberrikolliset etsivät aina tapoja päivittää haittaohjelmia, ja he ovat selvästi investoineet voimakkaasti Qbotin kehitykseen kyetäkseen laajoihin tietovarkauksiin yrityksiltä ja yksityishenkilöiltä. Olemme havainneet, että kampanjat jakavat Qbotia suoraan sekä Emotetin kaltaisten kolmansien osapuolten kautta. Yritysten tulisi harkita sellaisten haittaohjelmien torjuntaratkaisujen käyttöönottoa, jotka voivat estää tällaisen sisällön päätymisen loppukäyttäjille. Niiden tulisi myös opastaa työntekijöitä olemaan varovaisia sähköpostiviestejä avatessaan, vaikka ne näyttäisivät olevan luotettavasta lähteestä”, sanoo Check Pointin **Maya Horowitz**, Director, Threat Intelligence & Research, Products.

Suomessa yleisin haittaohjelma oli Windows-haittaohjelma Formbook. Maailman yleisin haittaohjelma Emotet on noussut Suomessa jo toiselle sijalle, ja sitä esiintyy noin viidessä prosentissa yritysverkoista.

Suomen yleisimmät haittaohjelmat elokuussa 2020:

1. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 5,78 %.
2. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään nykyään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 5,33 %.
3. **XMRig** – Monero-kryptovaluutan louhija. Esiintyvyys 4,4 %.
4. **TrickBot** – Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 3,56 %.

5. **RigEK** – Haittaohjelmien lataaja Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksissa. Esiintyvyys 2,22 %.
6. **AgentTesla** – Edistyksellinen etäkäyttötroijalainen, joka pystyy esimerkiksi uhrinsa näppäinten painalluksia seuraamalla ja kuvakaappauksia ottamalla pääsemään käsiksi WiFi-salasanoihin ja muihin kohdelaitteen tietoihin (esimerkiksi Outlook-sähköposti, Google Chrome ja Mozilla Firefox). Esiintyvyys 10,67 %.
7. **Remcos** – Jakaa haittaohjelmia roskaposteihin liitettyjen Microsoft Office -asiakirjojen kautta. Esiintyvyys 1,78 %.
8. **Vidar** – Windows-käyttöjärjestelmien haittaohjelma, joka varastaa salasanoja, luottokorttitietoja ja muuta arkaluontoista tietoa useista selaimista ja digitaalisista lompakoista. Esiintyvyys 1,33 %.
9. **Hiddad** – Android-haittaohjelma, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia, mutta pystyy myös nappaamaan puhelimen käyttäjätietoja. Esiintyvyys 1,33 %.
10. **Gandcrab** – Palveluna myytävä kiristyshaitake (ransomware-as-a-service), jonka kehittäjät ottavat kiristystuloista 30–40 prosenttia. Sen arvioidaan vaikuttaneen yli 1,5 miljoonaan Windows-käyttäjään ennen toiminnan pysähtymistä vuoden 2019 puolivälissä. Kaikille GandCrab-versioille on olemassa salauksen purkutyökalut. Esiintyvyys 1,33 %.

Maailman yleisimmät haittaohjelmat ja haavoittuvuudet elokuussa 2020:

1. **Emotet** – Kehittynyt, itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään nykyään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Pystyy leviämään myös sähköpostiliitteiden ja -linkkien kautta. Esiintyvyys 14 %.
2. **Agent Tesla** – Edistyksellinen etäkäyttötroijalainen, joka pystyy esimerkiksi uhrinsa näppäinten painalluksia seuraamalla ja kuvakaappauksia ottamalla pääsemään käsiksi WiFi-salasanoihin ja muihin kohdelaitteen (esimerkiksi Outlook-sähköposti, Google Chrome ja Mozilla Firefox) tietoihin. Esiintyvyys 3 %.
3. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 3 %.

Mobiilihaittaohjelmien globaalilla listalla ykkösenä oli elokuussa **xHelper**, jota käytetään muiden haitallisten sovellusten lataamiseen ja mainosten näyttämiseen. Sovellus pystyy piiloutumaan käyttäjältä ja virustorjuntaohjelmilta ja asentamaan itsensä uudelleen, jos käyttäjä poistaa sen. Toiseksi yleisin oli Android-haittaohjelma **Necro**, joka voi ladata muita haittaohjelmia. Se näyttää myös häiritseviä mainoksia ja varastaa rahaa. Kolmannella sijalla oli Android-haittaohjelma **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia.

Check Pointin tutkijat listasivat myös elokuun käytetyimmät **haavoittuvuudet**. Yleisintä haavoittuvuutta, **“Web Server Exposed Git Repository Information Disclosure”**, on yritetty hyödyntää 47 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisintä, **“MVPower DVR Remote Code Execution”**, esiintyy 43 prosentissa organisaatioista. Kolmannella sijalla on **”Dasan GPON Router Authentication Bypass (CVE-2018-10561)”**, esiintyvyys 37 prosenttia.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla.

ThreatCloud-tietokanta tarkastaa yli 2,5 miljardia verkkosivustoa ja 500 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:
Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com.
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. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

