Entistä vaarallisempi Valak nousi haittaohjelmien Top 10 -listalle

Tietoturvayhtiö Check Pointin tutkijat havaitsivat syyskuussa jyrkän nousun Valak-haittaohjelman esiintyvyydessä. Top 10 -listan kärkisijaa piti kolmatta kertaa peräkkäin Emotet-troijalainen.

ESPOO – 9. lokakuuta 2020 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research kertoo haittaohjelmakatsauksessaan, että päivitetty versio Valak-haittaohjelmasta on ensimmäistä kertaa yltänyt maailman yleisimpien joukkoon. Valak nousi syyskuussa haittaohjelmien kansainvälisen Top 10 -listan sijalle 9. Suomen levinneimpien haittaohjelmien joukossa se ei vielä ollut.

Ensimmäiset havainnot Valakista tehtiin viime vuoden lopulla. Hienostunut haittaohjelma luokiteltiin aluksi lataajaksi, jonka tehtävä on ujuttaa varsinaisia haittaohjelmia uhrin laitteelle. Viime kuukausien aikana on kuitenkin havaittu uudenlaisia Valak-variantteja, joiden toiminnallisuus on selvästi entistä kehittyneempää. Uudet Valak-versiot pystyvät myös varastamaan tietoja ja välittämään niitä edelleen, ja sen hyökkäykset kohdistuvat niin yksittäisiin uhreihin kuin yrityksiinkin. Vaarassa ovat Microsoft Exchange -sähköpostiohjelman sisältämät tiedot sekä käyttäjien tunnistetiedot ja verkkotunnusvarmenteet. Syyskuussa Valakia levitettiin laajalla kampanjalla haitallisen .doc-liitetiedoston sisältävien roskapostiviestien avulla.

”Kyberrikolliset pyrkivät usein maksimoimaan kehityspanostustensa tuoton päivittämällä vanhoja, toimiviksi osoittautuneita haittaohjelmia ja lisäämällä niihin ominaisuuksia. Elokuussa listoille noussut Qbot on samanlainen tapaus kuin Valak. Molemmat on nyt muokattu tunnistetietojen ja muun datan kerääjiksi. Yritysten kannattaa hyödyntää tietoturvaratkaisuja, jotka pysäyttävät epäilyttävät sisällöt ennen kuin ne ehtivät uhrien laitteille. Sähköpostien liitteisiin on jokaisen hyvä suhtautua epäluuloisesti, vaikka viesti näyttäisikin tulevan tutulta lähettäjältä”, ohjeistaa Check Pointin Suomen ja Baltian maajohtaja **Sampo Vehkaoja**.

Suomen yleisimmät haittaohjelmat olivat syyskuussa sähköpostiviestien välityksellä leviävä pankkitroijalainen Qbot sekä Emotet-troijalainen, joiden esiintyvyys oli yhtä suuri. Kansainvälisellä listalla Emotet oli ykkönen, ja Qbot nousi elokuun sijalta 10 sijalle 6. Suomen listalla se ei ollut elokuussa vielä ollenkaan.

Suomen yleisimmät haittaohjelmat syyskuussa 2020:

1. **Qbot**. Toiselta nimeltään Quackbot, pankkitroijalainen, joka seuraa näppäintoimintoja ja pyrkii nappaamaan uhrin tunnistetiedot. Käyttää kehittyneitä tekniikoita ohittaakseen virustutkat ja muut tietoturvaohjelmistot. Esiintyvyys Suomessa 5,04 %.
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 5,04 %.
3. **RigEK.** Haittaohjelmien lataaja Flash-, Java-, Silverlight- ja Internet Explorer -sovelluksissa. Esiintyvyys 4,20 %.
4. **XMRig**. Monero-kryptovaluutan louhija. Esiintyvyys 3,78 %.
5. **TrickBot**. Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma. Esiintyvyys 2,94 %.
6. **Mofksys**. Esiintyvyys 2,10 %.

7. **Formbook** – Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 1,68 %.
8. **FritzFrog**. Omaperäinen ja pitkälle kehitetty palvelinten haittaohjelma. Esiintyvyys 1,68 %.
9. **Neshta**. Troijalainen, joka havaittiin ensi kerran vuonna 2010. Piilottaa itsensä muiden ohjelmistojen koodin joukkoon ja pyrkii asentamaan selainlaajennuksia tai työkalurivejä omin päin. Esiintyvyys 1,26 %.
10. Remcos, Maze, Facexworm, SectorSec, DameWare, Eicar ja Floxif, kaikkien esiintyvyys 0,84 %.

Maailman yleisimmät haittaohjelmat ja haavoittuvuudet syyskuussa 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. **Trickbot**. Pääasiassa pankkihuijauksiin tähtäävä haittaohjelma, joka saa jatkuvasti uusia päivityksiä. Esiintyvyys 4 %.
3. **Dridex**. Windows-laitteiden troijalainen, jota levitetään pääasiassa sähköpostiviestien avulla. Haittaohjelma ottaa yhteyttä komentokeskukseen ja antaa tietoja kohdelaitteiston ominaisuuksista. Esiintyvyys 3 %.

Mobiilihaittaohjelmien globaalilla listalla ykkösenä oli syyskuussa **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 **Xafecopy**, troijalainen, joka naamioituu hyötysovellukseksi. Kun sovellus avataan, haittaohjelma kytkeytyy automaattisesti laskuttaville verkkosivuille, joiden laskut menevät suoraan puhelinlaskuun. Kolmannella sijalla oli Android-haittaohjelma **Hiddad**, joka paketoi sovelluksia uudelleen ja julkaisee ne sovelluskaupassa. Pääasiassa se levittää mainoksia.

Check Pointin tutkijat listasivat myös syyskuun käytetyimmät **haavoittuvuudet**. Yleisintä haavoittuvuutta nimeltään **MVPower DVR Remote Code Execution** on yritetty hyödyntää 46 prosentissa yritysverkoista maailmanlaajuisesti. Seuraavaksi yleisin oli **Dasan GPON Router Authentication Bypass (CVE-2018-10561**), jonka esiintyvyys oli 42 %. **OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)** kohosi kolmanneksi, esiintyvyys 36 %.

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 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:
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. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

