Check Point listasi haittaohjelmien trendit

Tietoturvayhtiö Check Pointin trendiraportti paljastaa kolme hyökkäystrendiä, joita kannattaa varoa.

Espoo, 22. helmikuuta 2017 – Check Point on julkaissut trendiraporttinsa H2 2016 Global Threat Intelligence Trends. Raportti paljastaa, että kiristysohjelmien määrä tuplaantui viime vuoden toisella vuosipuoliskolla. Niiden osuus kaikista yritysmaailman haittaohjelmahavainnoista nousi 5,5 prosentista 10,5 prosenttiin.

Check Pointin Threat Intelligence Group Managerin **Maya Horowitzin** arvion mukaan suuntaus johtuu siitä, että kiristyshaittaohjelmat ovat tehokkaita ja tuottavat kyberrikollisille tuloja. Ne toimivat, koska huonosti valmistautuneita yrityksiä ja organisaatioita on paljon. Niiden suojaukset eivät ole paikoillaan eikä henkilöstöä ole koulutettu tunnistamaan epäilyttäviä sähköpostiviestejä.

”Datasta voi päätellä myös, että pieni haittaohjelmaperheiden joukko vastaa hyökkäysten valtaosasta, ja samalla tuhannet haittaohjelmaperheet jäävät harvinaisiksi. Useimmat kyberturvallisuuden uhat leviävät globaalisti, mutta Aasian ja Tyynen meren alueella on useita omia haittaohjelmia, joita ei nähdä muualla”, Horowirz jatkaa.

Raportista ilmenevät tärkeimmät taktiikat, joita kyberrikolliset käyttävät hyökätessään yrityksiä kohti. Sen tiedot perustuvat Check pointin ThreatCloudin™ keräämään dataan.

Tärkeimmät meneillään olevat haittaohjelmatrendit:

1 Kiristysohjelmamarkkinat keskittyvät. Viime vuonna havaittiin tuhansia uusia kiristyshaittaohjelmavariantteja. Syksyn edetessä uhkamaisema kuitenkin muuttui selvästi, kun markkinat keskittyivät ja muutama tärkeä kiristysohjelmaperhe alkoi dominoida.
2 DDoS-hyökkäykset IoT-laitteiden kautta jatkuvat. Elokuussa 2016 havaittiin laatuaan ensimmäinen esineiden internetin (IoT) bottiverkko Mirai, joka otti orjikseen muun muassa videonauhureita (DVR) ja valvontakameroita (CCTV). Mirai käytti laitteita useissa palvelunesto- eli DDoS-hyökkäyksissä. Heikosti suojattuja IoT-laitteita on lähes joka kodissa, joten odotettavissa on niitä hyödyntäviä, massiivisia palvelunestohyökkäyksiä jatkossakin.
3 Roskapostikampanjoissa käytetään uudentyyppisiä liitetiedostoja. Roskapostikampanjoissa käytettiin viime syksynä yleisimmin liitetiedostoja, jotka perustuivat Windows Scriptin (WScript) käyttöön Etenkin Javascriptillä (JS) ja VBScribtillä (VBS) kirjoitettuja, haitallisia linkkejä sisältäviä viestejä liikkui paljon, mutta myös JSE, WSF ja VBE olivat hakkerien käytössä.

TOP 5 HAITTAOHJELMAT
Viime vuoden toisen vuosipuoliskon aikana:

1 Conficker (14,5 %) - Mato, joka mahdollistaa etäohjatun toiminnan ja haittaohjelmien latauksen. Tartunnan saanut kone ottaa säännöllisesti yhteyttä komentoserveriin, jonka orjana se toimii.
2 Sality (6,1 %) - Virus, joka mahdollistaa etäohjatun toiminnan ja lataa tartunnan saaneelle laitteelle lisää haittaohjelmia. Sen päätavoite on pysyä piilossa järjestelmässä ja tarjota väylä etäohjaukseen.
3 Cutwail (4,6 %) - Bottiverkko, joka pääasiassa lähettää roskapostia ja osallistuu DDoS-hyökkäyksiin. Laitteelle ladattuna se ottaa yhteyden komentopalvelimeen, jolta se saa ohjeet sähköpostien lähettämiseen. Suoritettuaan tehtävän haittaohjelma raportoi komentopalvelimelle tarkat tilastot postituksesta.

4 JBossjmx (4,5 %) - Mato kohdistuu järjestelmiin, joissa on haavoittuvuuden sisältävä versio JBoss Application Serveristä. Ohjelma luo haitallisen JSP-sivun, joka suorittaa mielivaltaisia komentoja. Lisäksi se luo uuden takaoven, joka hyväksyy etäkomentoja IRC-palvelimelta.
5 Locky (4,3 %) - Kiristyshaittaohjelma, joka alkoi levitä helmikuussa 2016. Sen levittäjänä on useimmiten sähköposti, jonka sisältämä latausohjelma on naamioitu Word- tai Zip-liitteeksi. Latausohjelma lataa ja asentaa laitteelle haittaohjelman, joka lukitsee käyttäjän tiedostot.

TOP 3 KIRISTYSHAITTAOHJELMAT

1 Locky (41 %) - Helmikuussa voittokulkunsa aloittanut kiristyshaittaohjelma yleistyi dramaattisesti vuoden toisella puoliskolla.
2 Cryptowall (27 %) - Cryptolockerin kopio, joka ohitti alkuperäisen yleisyydessä. Cryptowall on tunnettu tavastaan hyödyntää AES-salausta ja hoitaa komentoviestintä Tor-verkon kautta. Se leviää haittaohjelmien levittämiseen erikoistuneiden exploit kit -haittaohjelmien kautta, kalastelukampanjoiden avulla ja haittamainosten kautta.
3 Cerber (23 %) - Maailman suurin kiristyshaittaohjelmia palveluna välittävä järjestelmä. Cerberin kehittäjä myy menetelmää ja ottaa osansa ohjelman levittäjien kiristyksen avulla saamista voitoista.

TOP 3 MOBIILIHAITTAOHJELMAT

1 Hummingbad (60 %) - Check Pointin tietoturvatiimin löytämä Android-tuholainen, joka asentaa laitteelle sitkeän rootkit-haittaohjelman, lataa sen kautta vilpillisiä ohjelmia ja mahdollistaa esimerkiksi tunnistetietojen anastamisen, näppäimistön seurannan ja salatun sähköpostin säiliön ohituksen vain pienillä muutoksilla.
2 Triada (9 %) - Android-laitteiden takaovi, joka myöntää rikolliselle pääkäyttäjän oikeudet. Ne mahdollistavat haittaohjelmien lataamisen laitteelle ja auttavat sitä sulautumaan laitteen järjestelmään. Triadan on havaittu myös vakoilevan selaimen URL-osoitteita.
3 Ztorg (7%) - Troijalainen, joka käyttää pääkäyttäjän oikeuksia ohjelmien lataamiseen ja asentamiseen käyttäjän tietämättä.

TOP 3 PANKKIHAITTAOHJELMAT

1 Zeus (33 %) - Windows-laitteille suunnattu troijalainen, joka pyrkii varastamaan pankkitunnuksia seuraamalla näppäintoimintoja.
2 Tinba (21 %) - Pankkitroijalainen, joka anastaa uhrin pankkitunnukset tämän pyrkiessä kirjautumaan verkkopankkiinsa.
3 Ramnit (16 %) - Pankkitroijalainen, joka varastaa pankkitunnuksia, palvelinten salasanoja, evästeitä ja henkilötietoja.

Koko raportti löytyy täältä: http://blog.checkpoint.com/2017/02/21/ransomware-doubled-in-second-half-of-2016/

--
Check Pointin ThreatCloud™ on maailman laajin verkosto, joka kerää tietoja yrityksiin ja organisaatioihin kohdistuvista kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Check Pointin uhkakartta näyttää kyberhyökkäykset reaaliaikaisesti: ThreatCloud World Cyber Threat Map
Katso täältä, kun haluat tietää, mitä mikäkin haittaohjelma tekee: Check Point ThreatWiki
Tietoja Check Pointin uhkientorjuntaresursseista: Threat-prevention-resources
Check Pointin tietoturvatiimin blogi: Check Point Blog

Lisätiedot ja haastattelupyynnöt:

OSG Viestintä, Maija Rauha, maija.rauha@osg.fi, p. 0400 630 065

Seuraa Check Pointia:
Check Pointin blogi: http://blog.checkpoint.com/
Twitter: www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
YouTube: http://www.youtube.com/user/CPGlobal

Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) on maailman suurin yksinomaan kyberturvallisuustuotteisiin keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, joiden kyky havaita haittaohjelmat ja muut tunkeutujat sekä suojata asiakkaat kyberhyökkäyksiltä on ainutlaatuisen tehokas. Check Pointin täydellisen kattava tietoturva-arkkitehtuuri suojaa niin yritysverkot kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava sekä intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.

