Check Point jakoi kyberhyökkäysten Oscarit Helsingissä

*Tietoturvayhtiö Check Pointin Software Technologiesin tutkijaryhmän vetäjä* ***Maya Horowitz*** *jakoi kyberhyökkäysten Oscarit Helsingissä järjestetyssä CPX Finland -tapahtumassa.*

**Espoo, 25. lokakuuta 2018.** Jos kyberkonnille jaettaisiin Oscareita, ketkä nousisivat korokkeelle pitämään kiitospuheita? Maya Horowitz jakoi Kalastajatorpalla pidetyssä tilaisuudessa omavaltaisesti tuomaroidut palkinnot kuudessa sarjassa:

1. **Vuoden hakkeri: Rikkaaksi hinnalla millä hyvänsä (G3tRich)**

Vuoden hakkeri -sarjassa voiton vei sofistikoitujen ja suurta taitoa vaativien APT-hyökkäysten nenän edestä nigerialainen nuori mies, joka sai aikaan erittäin laajalle levinneen kalastelukampanjan yksinkertaisen troijalaisen avulla. Hakkerin kampanja alkoi keväällä 2017, ja sen uhreiksi joutui useita isoja energia-, kuljetus-, rakennus- ja pankkialan yrityksiä pääasiassa Välimeren maissa, kuten Turkissa, Egyptissä, Italiassa ja Kreikassa.

Check Pointin tietojen mukaan kampanjaan liittyviä sähköpostiviestejä levisi ainakin 4 000 organisaatioon ja 6 000 osoitteeseen. Kalastelu onnistui 14 kertaa, ja mies kääri taskuihinsa tuhansien dollarien tulot. Tutkijat pääsivät kuitenkin hakkerin jäljille ja löysivät hänen julkiset Facebook-sivunsa, joissa hän kertoi motokseen ”Get rich or die when trying” eli vapaasti käännettynä Rikastu tai kuole sitä yrittäessäsi. Check Point luovutti tietonsa henkilöstä Nigerian poliisille.

Lisätietoja tapauksesta:

<https://blog.checkpoint.com/2017/08/15/get-rich-die-trying-case-study-real-identity-behind-wave-cyberattacks-energy-mining-infrastructure-companies/>

1. **Paras haittaohjelma sivuroolissa: Mirai**

Kybermaailman sivuosan esittäjiä ovat toimiviksi todetut haittaohjelmat, joita käytetään hyökkäyksissä kerta toisensa kenties vain hieman muunneltuina. Tässä sarjassa voiton vei maailman ensimmäinen IoT-bottiverkko Mirai, jota ehdittiin käyttää useita kertoja vuonna 2017, ennen kuin Check Pointin tutkijat jäljittivät sen tekijän.

Esimerkiksi Huawein reitittimiä piinannut bottiverkko oli Mirain muunnelma, samoin Netflixin ja Amazonin lamaannuttanut palvelunestohyökkäys Dyn DNS -palvelinta vastaan. Kävi ilmi, että ohjelman kehittäjä on ollut mukana perustamassa tietoturva-alan yritystä, jonka tuote suojaa palvelunestohyökkäyksiltä. Hänet on sittemmin vangittu Yhdysvalloissa.

Lisätietoja Miraista ja muista bottiverkoista:

<https://www.checkpoint.com/definition/botnet/>

1. **Paras lyhyt hyökkäys: WannaCry**

Lyhytelokuvan pituus mitataan minuuteissa, lyhyt kyberhyökkäys kestää alle viikon. Tässä sarjassa voittajasta ei ollut epäselvyyttä: se on toukokuussa 2017 liikkeelle laskettu WannaCry. Kiristyshaittaohjelma saatiin pysäytettyä nopeasti, koska sen koodista löytyi kaksikin pysäytyskytkintä, mutta se nousi kuolleista jo kuukauden kuluttua NotPetyana. WannaCry on tiettävästi pohjoiskorealaista tekoa.

Lisätietoa WannaCrystä ja sen pitkäaikaisvaikutuksista:

<https://blog.checkpoint.com/2018/05/15/one-year-later-wannacry-dawn-new-generation-cyber-attacks/>

**4. Paras visuaalinen ilme: WannaCry**

WannaCryn punareunainen kiristysviesti näkyi laajalti sekä laitteissa että mediassa ja tuli erittäin tunnetuksi. Samaa, erottuvaa graafista ilmettä on saatu ihastella niin mikroaaltouunien, älykellojen kuin pesukoneidenkin näytöissä.

**5. Paras vieraskielinen kampanja: Fireball**

Sarjan voittaja, kiinalainen Fireball, voi näyttää päälle päin harmittomalta. Se valjastaa uhrin selaimen tehokkaaksi mainosten välittäjäksi tahkoten siten tuloja kehittäjilleen. Lisäksi se sisältää kuitenkin mahdollisuuden ladata uhrin koneelle mitä tahansa muuta haittakoodia, joka on mahdollista käynnistää etäältä. Fireball levisi todella laajalle, jopa yli 250 miljoonaan koneeseen. Haittaohjelman kehitti yritys nimeltä Rafotech, jonka 9 vastuuhenkilöä on sittemmin vangittu.

Lisätietoja Fireballista:

<https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/>

**6. Levinnein haittaohjelma: kryptolouhijat**

Levinneimpien haittaohjelmien sarjassa olivat ehdokkaina pankkitroijalaiset, kiristyshaittaohjelmat ja kryptolouhijat. Oscarin saivat kryptolouhijat. Parhaassa tapauksessa ne ovat suhteellisen vaarattomia yksittäisillä tietokoneilla, mutta yritysten palvelimille ja pilveen päästessään ne voivat tehdä paljon vahinkoa. Ne käyttävät palvelinten resursseja, heikentävät henkilöstön tuottavuutta, vaikeuttavat asiakaspalvelua ja rapauttavat yrityksen mainetta. Esimerkiksi Check Pointin suomalaisten asiakkaiden verkoissa kryptolouhijat olivat viime vuonna yleisimmin tavattu haittaohjelmatyyppi.

Lisätietoa kryptolouhijoista:

<https://blog.checkpoint.com/2018/09/19/cryptomining-cyber-threat-alliance-report/>

**Lisätiedot ja haastattelupyynnöt:**

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

**Seuraa Check Pointia:**

Twitter: <http://www.twitter.com/checkpointsw>

Facebook: <https://www.facebook.com/checkpointsoftware>

Blog: <http://blog.checkpoint.com>

YouTube: <http://www.youtube.com/user/CPGlobal>

LinkedIn: <https://www.linkedin.com/company/check-point-software-technologies>

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden kohdistettujen hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri käsittää uuden 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen kaikkia verkko-, pilvi- ja mobiilitoimintoja kaikilta tunnetuilta hyökkäyksiltä, ja sitä hallitaan alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän kautta. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.