**Varo silmäniskua! Liikkeellä on uusi, nopeasti yleistyvä kiristyshaittaohjelma**

*Pahamaineinen Phorpiex-bottiverkko levittää roskapostiviestien avulla uutta kiristyshaittaohjelmaa nimeltä Avaddon. Phorpiex oli kesäkuussa Suomen kolmanneksi yleisin tietoturvauhka.*

**ESPOO – 10. heinäkuuta 2019 –** Maailman johtavan tietoturvayhtiön Check Pointin tutkimustoiminnasta vastaava Check Point Research kertoo uusimmassa haittaohjelmakatsauksessaan, että pahamaineinen Phorpiex-bottiverkko levitti kesäkuussa suurella volyymillä uutta Avaddon-kiristyshaittaohjelmaa. Ensimmäiset havainnot Avaddonista tehtiin kesäkuun alussa, ja kampanjan ansiosta Phorpiex nousi Check Pointin eniten havaittujen haittaohjelmien listalla sijalle kaksi. Myös Suomessa Phorpiex ylsi yleisimpien haittaohjelmien joukkoon.

Phorpiex tunnetaan parhaiten levittämistään pornokiristysviesteistä, joita moni suomalainenkin on saanut sähköpostiinsa. Niissähän väitettiin, että vastaanottaja on katsonut laitteellaan pornoa, ja uhri uhattiin paljastaa läheisilleen. Bottiverkko on kuitenkin tehnyt myös monenlaista muusta kiusaa. Check Point laski viime vuonna, että Phorpiex-tartunnan saaneita tietokoneita oli yli miljoona, ja haittaohjelman avulla saadut tulot kohosivat noin 500 000 dollariin.

Uusi Avaddon on kiristysohjelma, jota myydään kyberrikollispiireissä avaimet käteen -palveluna (RaaS, Ransomware as a Service). Avaddon-viestien otsikko ja silmäniskua esittävä emoji houkuttelevat avaamaan zip-pakatun liitteen. Kiristyshaittaohjelma aktivoituu liitteen kuvaketta klikattaessa. Ohjelma salaa tietokoneen sisällön ja pyytää lunnaita palkkioksi sisällön avaamisesta.

”Phorpiex tunnetaan myös nimeltä Trik. Sen syntilista on pitkä, sillä se on jaellut ainakin GandCrab-, Pony- ja Pushdo-haittaohjelmia, orjuuttanut isäntäkoneita kryptovaluutan louhintaan ja levittänyt pornokiristysviestejä. Nyt sille on jälleen löydetty uutta käyttöä haittaohjelmakampanjassa. Yritysten ja organisaatioiden tulisi opastaa henkilöstään tunnistamaan yleisimmät haittaohjelmia sisältävät roskapostilajit. Silmäniskuemojin sisältävät viestit on nyt syytä liittää epäilyttävien joukkoon. Tärkeää on myös suojata tietoverkko tartunnoilta ajan tasalla olevalla, monikerroksisella tietoturvaratkaisulla”, kommentoi Check Pointin tietoturvatutkijaryhmän johtaja **Maya Horowitz**.

**Suomen yleisimmät haittaohjelmat kesäkuussa 2020:**

1. **Formbook**. Windows-järjestelmän haittaohjelma, joka kerää uhrien tietoja monin eri tavoin. Esiintyvyys 1,17 %

2. **Lotoor**. Hakkerointityökalu, joka hyödyntää Android-käyttöjärjestelmän haavoittuvuuksia juurioikeuksien saamiseksi vaarantuneista mobiililaitteista. Esiintyvyys 1,17 %.

3. **Phorpiex**. Windows-laitteiden mato, joka luikertelee palomuurin ohi tekeytymällä hyväksytyksi sovellukseksi. Esiintyvyys 1,17 %.

4. **Shiz**. Takaoviohjelma, joka piiloutuu Windows-prosesseihin ja pitää yhteyttä useisiin ohjauspalvelimiin. Esiintyvyys 1,17 %.

5. **XMRig**. Monero-kryptovaluutan louhija. Esiintyvyys 1,17 %.

6. **Pavelo**, esiintyvyys 0,78 %.

7. **Remcos**. Vuonna 2016 havaittu haittaohjelma, joka leviää sähköpostiviestin liitteenä olevien Microsoft Office-tiedostojen avulla. Esiintyvyys 0,78 %.

8. **Adylkuzz**. Troijalainen. Esiintyvyys 0,78 %.

9. **Emotet.** Itsestään leviävä ja modulaarinen pankkitroijalainen, jota käytetään pääasiassa muiden haittaohjelmien levittämiseen. Väistelee virustutkia ja poistoyrityksiä. Esiintyvyys 0,78 %.

10. **Joker.** Etenkin laskutushuijauksissa käytetty mobiilihaittaohjelma. Esiintyvyys 0,78 %.

**Maailman yleisimmät haittaohjelmaperheet ja haavoittuvuudet top 3, kesäkuu 2020**

Tietokoneiden haittaohjelmat:

**1. Agent Tesla.** Etäohjattava troijalainen, joka seuraa uhrin näppäimistöä, tutkii leikepöydät, poimii salasanoja ja lähettää ruutukaappauksia. Nousussa.

**2. Phorpiex**. Bottiverkko, joka levittää muita haittaohjelmia roskapostikampanjojen avulla. Tunnettu pornokiristysviestien lähettäjänä. Nousussa.

**3. XMRig**. Moneron louhintaa vuodesta 2017. Ennallaan.

Mobiilihaittaohjelmat:

**1. Necro.** Android-laitteiden haittaohjelma, joka levittää muita haittaohjelmia, mutta pystyy myös näyttämään mainoksia ja anastamaan rahaa väärennettyjen tilausten avulla.

**2. Hiddad.** Android-haitake, joka pakkaa sovelluksia uudestaan ja myy ne kolmannen osapuolen verkkokaupassa. Näyttää mainoksia ja varastaa tietoja.

**3. Lotoor.** Hakkerityökalu, joka hankkii pääkäyttäjän oikeudethyödyntämällä Android-järjestelmän haavoittuvuuksia.

Käytetyimmät haavoittuvuudet:

1. **OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)** Esiintyvyys 45 % globaalisti. Esiintyvyys viittaa havaittuihin hyödyntämisyrityksiin yrityksissä ja organisaatioissa.

2. **MVPower DVR Remote Code Execution.** Esiintyvyys 44 %.

3. **Web Server Exposed Git Repository Information Disclosure.** Esiintyvyys38 %.

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, joista se tunnistaa yli 250 miljoonaa haittaohjelmatapahtumaa päivittäin.

Täydellinen Top 10 -haittaohjelmalista löytyy [Check Pointin blogista](https://blog.checkpoint.com/).

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteessa [www.checkpoint.com](http://www.checkpoint.com).

**Lisätiedot ja haastattelupyynnöt:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com.
Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065.

**Seuraa Check Point Researchia:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**Check Point Research**

Check Point Research ([research.checkpoint.com](https://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](http://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.