Check Point tutki pohjoiskorealaisen virustorjuntaohjelman

*Check Pointin tietoturvatutkijat saivat käsiinsä harvinaisen pohjoiskorealaisen SiliVaccine-virustorjuntaohjelman. Ohjelman lähdekoodissa on osia, jotka ovat identtisiä japanilaisen Trend Micron virustorjuntaohjelman koodin kanssa.*

**Espoo, 2. toukokuuta 2018.** Tietoturvayhtiö Check Point Software Technologies on saanut toimittaja [Martyn Williams](https://www.northkoreatech.org/about/)in kautta haltuunsa harvinaisen, Pohjois-Koreassa käytössä olevan SiliVaccine-virustorjuntaohjelman.

Tutkiessaan ohjelmaa Check Pointin tutkijat havaitsivat, että se on osittain identtinen japanilaisen Trend Micron virustorjuntaohjelman 10 vuotta vanhan version kanssa. Suurin osa näistä vastaavuuksista on huolellisesti peitetty. Check Pointin tutkijat arvioivat, että tämä on ollut mahdollista vain, jos SiliVaccinen kehittäjillä on ollut suora pääsy Trend Micron ohjelman keskeisiin ohjelmakomponentteihin.

Virustorjuntaohjelman tarkoitus on tunnistaa haittaohjelmat ja estää niiden leviäminen. Check Pointin tutkijat huomasivat kuitenkin, että SiliVaccine päästää läpi yhden tietyn haittaohjelmatunnisteen, jonka Trend Micron ohjelma tunnistaa ja estää.

Williams sai samassa lähetyksessä myös SiliVaccinen paikkaamiseen tarkoitetun tiedoston, joka sisälsi JAKU-haittaohjelman. JAKUlla on noin 19 000 uhria, joiden joukossa tiedetään olevan eteläkorealaisia ja japanilaisia kansainvälisten järjestöjen työntekijöitä, tutkijoita ja valtion viranhaltijoita.

**Yhteyksiä Japaniin**

SiliVaccinen parissa vaikuttavat työskennelleen Pohjois-Koreassa yhtiöt nimeltä PGI (Pyonyang Gwangmyong Information Technology) ja STS Tech-Service. Viimeksi mainittu on tehnyt yhteistyötä muun muassa kahden japanilaisen yhtiön, Silver Starin ja Magnolian, kanssa. Niillä puolestaan on ollut aiempaa yhteistyötä KCC:n (Korea Computer Centre) kanssa, joka on Pohjois-Korean valtiollinen toimija.

Trend Micro kommentoi, ettei se ole koskaan tehnyt yhteistyötä Pohjois-Korean kanssa. Se ei ota kantaa Check Pointin käsiinsä saaman ohjelman autenttisuuteen, mutta toteaa, että siinä on hyödynnetty yli 10 vuotta vanhaa Trend Micron virustorjuntatuotteiden ydinohjelmaa (scan engine), jota on käytetty useissa Trend Micron ja kolmansien osapuolten tuotteissa.

Check Point on julkaissut tarkemmat tiedot havainnoistaan ja Trend Micron laajemman lausunnon blogissaan, jonka tiedot ovat vapaasti käytettävissä:

<https://research.checkpoint.com/silivaccine-a-look-inside-north-koreas-anti-virus/>

**Check Pointin kansainvälisten asiantuntijoiden 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>Blogi: [http://blog.checkpoint.com](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 maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yrityksen verkot, pilvipalvelut kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.