**Check Point ja Zoom korjasivat yhdessä etäkokouspalvelun tietoturvaongelman**

***Tietoturvayhtiö Check Point ja etäkokouksista tuttu Zoom havaitsivat palvelun muokattavissa URL-osoitteissa vian, joka olisi mahdollistanut kokouskutsujen linkkien manipuloinnin ja käyttämisen tietojen kalasteluun.***

**ESPOO – 16. heinäkuuta 2019 –** Maailman johtavan tietoturvayhtiön Check Pointin tutkimustoiminnasta vastaava Check Point Research auttoi äskettäin poistamaan Zoom-etäkokoustyökalun muokattaviin osoitteisiin liittyvän tietoturvaongelman.

Yritykset käyttävät räätälöityjä Zoom-osoitteita ([Vanity URL](https://support.zoom.us/hc/en-us/articles/215062646-Guidelines-for-Vanity-URL-Requests)), kun ne haluavat oman nimensä mukaan kokoustensa verkko-osoitteeseen. Etäkokoushuoneen osoite voi olla esimerkiksi muotoa https://yrityksesi.zoom.us. Haavoittuvuus olisi mahdollistanut hakkerille oikean näköisten, mutta väärennettyjen Zoom-kokouskutsujen lähettämisen yrityksen nimissä. Kutsua olisi voinut käyttää esimerkiksi haittaohjelmien levittämiseen ja sitä kautta tietojen anastamiseen. Aikaisemmin tänä vuonna Check Point työsti Zoomin kanssa paikan [haavoittuvuuteen](https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/), jonka kautta hakkeri pystyi osallistumaan kokouksiin ilman asianmukaista kutsua.

Zoomin käyttäjämäärät ovat moninkertaistuneet Covid-19-tilanteen takia. Joulukuussa palvelua käytti 10 miljoonaa kokoustajaa päivittäin maailmanlaajuisesti, kun huhtikuussa Zoom-kokouksiin osallistui yli 300 miljoonaan käyttäjää. Kyberrikolliset ovat havainneet videokokouspalveluiden suosion ja pyrkivät käyttämään niitä omiin tarkoituksiinsa. Check Pointilla on huomattu selvä nousu muun muassa Zoomia muistuttavien verkko-osoitteiden rekisteröintien ja väärennettyjen Zoom-asennusohjelmien määrässä.

Nyt korjattu tietoturva-aukko löytyi samalla, kun tutkijat paikkasivat edellistä ongelmakohtaa. Hakkerin olisi ollut mahdollista käyttää Zoom-kutsuja omiin tarkoituksiinsa kahdella tavalla:

* Suoran linkin avulla. Kokousta koolle kutsuttaessa kutsun verkko-osoitetta (URLia) on mahdollista muokata niin, että se sisältää minkä tahansa rekisteröidyn aliverkkotunnuksen (sub-domainin). Myös hakkeri olisi voinut tehdä tämän, eikä kutsun vastaanottajan olisi ollut ilman erityistä tietoturvakoulutusta mahdollista erottaa, onko osoite aito.
* Yrityksen räätälöidyn Zoom-liittymän kautta. Joillakin yrityksillä ja organisaatioilla on oma Zoom-käyttöliittymä kokouksiaan varten. Hakkeri olisi voinut väärentää tämän käyttöliittymän ja johdattaa käyttäjän rekisteröitymään valelomakkeelle aidon Zoom-käyttöliittymän sijasta. Tätäkin olisi ollut vaikea havaita.

Hakkeri olisi sitten voinut tekeytyä kohdeorganisaation työntekijäksi ja esimerkiksi hankkia järjestämänsä ”kokouksen” osanottajilta salassa pidettäviä tietoja.

”Zoom on niin laajasti yritysten, virastojen ja kuluttajien käytössä, että on tärkeää estää pahantekijöitä hyödyntämästä sitä rikollisiin tarkoituksiin. Olemme työskennelleet yhdessä Zoomin tietoturvatiimin kanssa tarjotaksemme Zoomin käyttäjille turvallisemman ja luotettavamman palvelun, jota he voivat huoletta hyödyntää. Tämä oli Check Pointin ja Zoomin yhteishanke, josta kaikki Zoomin käyttäjät hyötyvät”, sanoi **Adi Ika**n, Check Pointin Network Research & Protection Group Manager.

Tarkemmat tiedot haavoittuvuudesta löytyvät Check Point Researchin blogista: <https://blog.checkpoint.com/2020/07/16/fixing-the-zoom-vanity-clause-check-point-and-zoom-collaborate-to-fix-vanity-url-issue/>

Video havainnollistaa, miten haavoittuvuutta olisi voinut käyttää: <https://youtu.be/YIrgDkVYLKU>

**Lisätiedot ja haastattelupyynnöt:**

Sampo Vehkaoja, maajohtaja, Check Point Finland, [sampov@checkpoint.com](mailto:sampov@checkpoint.com)

Maija Rauha, viestintäkonsultti, OSG Viestintä, [maija.rauha@osg.fi](mailto: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_)

Podcast: <https://research.checkpoint.com/category/cpradio/>

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

**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.