**Tiedote julkaisuvapaa keskiviikkona 5.2. klo 13.00**

**Älyvalaistuksen pimeä puoli: Kotisi ja yrityksesi tietoverkot voidaan hakkeroida älylampun kautta – Näin se tapahtuu**

*Hakkerit voivat levittää kiristys- tai vakoiluohjelmia älylamppujen ja niiden ohjaimien kautta hyödyntämällä niin sanotun ZigBee-protokollan haavoittuvuuksia, varoittavat tietoturvayhtiö Check Pointin tutkijat. He suosittelevat Philips Hue -älyvalojen käyttäjiä varmistamaan, että laiteohjelmisto on ajan tasalla.*

**CPX Wien, Itävalta – 5. helmikuuta 2020 –** Tietoturvayhtiö Check Point Software Technologiesin tutkijat ovat löytäneet haavoittuvuuksia, joiden avulla hakkeri voi levittää kiristys- ja muita haittaohjelmia yritys- ja kotiverkkoihin ottamalla hallintaansa älylamppuja ohjaimineen.

Check Point Researchin tutkijat havaitsivat, että hakkeri voi hyökätä kotien, yritysten ja jopa älykaupunkien tietoverkkoihin IoT-laitteiden (kuten älylamppujen ja niiden ohjauslaitteiden) verkkoyhteyden kautta. Tutkijat keskittyivät markkinoiden johtavaan [Philips Hue](https://www2.meethue.com/en-us) -älyvalaistukseen. He löysivät siitä haavoittuvuuksia, jotka sallivat verkkoon soluttautumisen pienitehoista, langatonta [ZigBee](https://en.wikipedia.org/wiki/ZigBee)-protokollaa käyttäen. ZigBee on usein käytetty protokolla älylaitteiden ohjauksessa.

Vuonna 2017 julkaistussa ZigBee-ohjattujen älylamppujen [turvallisuusanalyysissä](https://eyalro.net/publication/rosw17.html) tutkijat pystyivät ottamaan hallintaansa Hue-hehkulampun verkossa, asentamaan siihen haitallisen laiteohjelmiston ja levittämään sitä muihin, vierekkäisiin lamppuverkkoihin. Check Point Researchin tutkijat päättivät viedä asian askeleen pidemmälle: he käyttivät Hue-lamppua alustana, ottivat ohjauslaitteen haltuunsa ja lopulta hyökkäsivät kohteen tietokoneverkkoon. Hue-lamppujen uusimmissa laitesukupolvissa haavoittuvuutta ei ole.

Näin hyökkäys tapahtuu:

1. Hakkeri huijaa käyttäjiä muuntamalla lampun väriä tai kirkkautta, ikään kuin siinä olisi joku vika. Polttimo näkyy ohjaussovelluksessa 'tavoittamattomana', joten käyttäjä yrittää resetoida sen.
2. Ainoa tapa nollata polttimo on poistaa se sovelluksesta ja ohjeistaa sitten ohjaussiltaa etsimään lamppu uudelleen.
3. Silta löytää vahingoittuneen polttimon, ja käyttäjä lisää sen takaisin verkkoon.
4. Hakkereiden ohjaama lamppu, jossa on päivitetty laiteohjelmisto, käyttää sitten ZigBee-protokollan haavoittuvuuksia lähettämällä siihen suuren määrän dataa. Tietojen avulla hakkeri voi myös asentaa haittaohjelmia siltaan, joka puolestaan on yhteydessä kohdeyritykseen tai kotiverkkoon.
5. Haittaohjelma yhdistyy takaisin hakkerille ja voi tunnettua hyökkäysmenetelmää (kuten [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue)) käyttäen tunkeutua kohteen IP-verkkoon ja levittää kiristys- tai vakoiluohjelmia.

"Monet tietävät jo, että IoT-laitteet voivat olla turvallisuusriski. Tämä tutkimus osoittaa, kuinka hakkerit voivat hyödyntää jopa kaikkein arkipäiväisempiä, näennäisesti "tyhmiä" laitteita, kuten valolamppuja, ja käyttää niitä verkkojen kaappaamiseen ja haittaohjelmien levittämiseen", sanoo Check Point Researchin kybertutkimuksen johtaja **Yaniv Balmas**.

”On erittäin tärkeää, että organisaatiot ja yksityishenkilöt suojautuvat näiltä hyökkäyksiltä päivittämällä laitteet viimeisimmillä korjauksilla ja pitämällä ne erillään muista verkossa olevista koneista haittaohjelmien leviämisen rajoittamiseksi. Nykyiset viidennen sukupolven hyökkäykset ovat niin monimutkaisia, ettei meillä ole varaa unohtaa minkään verkkoihimme liitetyn laitteen tietoturvaa", hän jatkaa.

Tel Avivin ylipistossa [Check Point Institute for Information Securityn (CPIIS)](http://cpiis.cs.tau.ac.il/) avulla tehdyn tutkimuksen tulokset kerrottiin Philipsille ja Signifylle (Philips Hue -brändin omistaja) marraskuussa 2019. Signify vahvisti haavoittuvuuden olemassaolon ja julkaisi korjatun laiteohjelmistoversion (1935144040). Check Point suosittelee käyttäjiä varmistamaan, että heidän tuotteensa on päivitetty automaattisesti tähän laiteohjelmistoversioon.

”Olemme sitoutuneet suojelemaan käyttäjien yksityisyyttä ja tekemään kaikkemme tuotteidemme turvallisuuden varmistamiseksi. Olemme kiitollisia Check Pointin vastuullisesta yhteistyöstä. Se on antanut meille mahdollisuuden kehittyä, ottaa käyttöön tarvittavat korjaukset ja välttää kuluttajille koituvat riskit”, sanoo Philips Huen teknologiajohtaja **George Yianni**.

Katso [demovideo hyökkäyksestä](https://youtu.be/4CWU0DA__bY). Tekniset tutkimustiedot julkaistaan myöhemmin, jotta käyttäjille voidaan antaa aikaa korjata haavoittuvat laitteet.

Check Point on ensimmäinen tietoturvatoimittaja, joka tarjoaa IoT-laitteiden ohjelmistoja suojaavia kokonaisratkaisuja. Sen uutta [teknologiaa](https://www.checkpoint.com/press/2019/check-point-software-acquires-cymplify-iot-startup/) hyödyntävät ratkaisut vähentävät laitetason hyökkäyksiä.

**Lisätiedot:**

Rami Rauanmaa, tietoturva-asiantuntija, Check Point Software Technologies, ramira@checkpoint.com
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068

**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.