Näin se käy: Check Point selvitti, miten tv-tikku avaa ulkopuolisille oven kotiverkkoon

*Tietoturvayhtiö Check Point Software Technologies löysi tunnetusta tv-tikusta haavoittuvuuden, joka mahdollistaa pääsyn käyttäjän kotiverkkoon. Tapaus havainnollistaa esineiden internetin tietoturvariskejä sekä kodeissa että yrityksissä.*

**Espoo, torstai 7. tammikuuta 2015 –** Check Point Software Technologies julkisti eilen raportin, joka havainnollistaa IoT-riskejä tv-tikun kautta. EZCast tekee tavallisesta televisiosta älytelevision peilaamalla älypuhelimen tai tietokoneen kuvan tv-ruudulle. Check Pointin tutkijat löysivät väylän, jonka avulla ulkopuolisen on mahdollista saada tv-tikun kautta hallintaansa käyttäjän langaton lähiverkko ja sen myötä myös verkossa liikkuva tieto ja kaikki siihen yhteydessä olevat laitteet.

EZCastilla on arviolta viisi miljoonaa käyttäjää kautta maailman, ja se on markkinoilla myös Suomessa. Tv-tikulla on oma Wi-Fi-verkko, jonka avulla se välittää datan tietokoneelta tai puhelimelta televisiolle. Tv-tikku edustaa nopeasti yleistyvää esineiden internetiä (IoT) eli suuntausta, jossa kodinteknologia ja muut laitteet ovat yhteydessä internetiin. Check Pointin raportti tuo esiin seuraavat tietoturvariskit:

* Hyökkääjä pääsee sisään Wi-Fi-järjestelmän kautta ja pääsee helposti käsiksi sekä EZCastin omaan verkkoon että kodin muihin verkkoihin.
* Sisään päästyään hyökkääjä pystyy liikkuman langattomassa lähiverkossa kenenkään huomaamatta. Pahimmassa tapauksessa tarjolla voi olla niin terveystietoja kuin tiliotteitakin, mikä tekee identiteetin varastamisesta helppoa.
* Hyökkäys on mahdollista käynnistää etänä.

– Raporttimme tuo valaistusta asiaan, josta on hyvää vauhtia tulossa normaali – kyberrikolliset käyttävät luovasti hyväkseen raot, joita jää, kun yhä useammat laitteet ovat yhteydessä toisiinsa. IoT-trendi tulee jatkumaan, joten ihmisten on tärkeää miettiä muidenkin laitteiden kuin tietokoneiden ja älypuhelinten tietoturvaa, sanoi Check Pointin tietoturvatutkijoiden ryhmää vetävä **Oned Vanunu** raporttia julkistettaessa**.**

IoT koskee jo laajaa laitejoukkoa pienistä tv-tikun tapaisista kuluttajalaitteista autoihin ja monimutkaisiin teollisuuden järjestelmiin asti. Markkinoilla olevien laitteiden taso tietoturvan kannalta vaihtelee. Check Point kehottaa myös kuluttajia ottamaan selvää laitteiden tietoturvasta jo ostovaiheessa.

Lisätietoja Check Pointin blogista:

<http://blog.checkpoint.com/2016/01/07/youre-watching-tv-is-it-also-watching-you/>

Täydellinen raportti täältä:

<http://blog.checkpoint.com/wp-content/uploads/2015/12/EZCast_Report_Check_Point.pdf>.

**Lisätietoja myös:**

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

Seuraa Check Pointia:

Check Pointin blogi: <http://blog.checkpoint.com/>

Twitter: [www.twitter.com/checkpointsw](http://www.twitter.com/checkpointsw)

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

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

**Check Point Software Technologies Ltd.**
Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin yksinomaan tietoturvaan keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, jotka torjuvat asiakkaisiin kohdistuvat kyberhyökkäykset havaiten haittaohjelmat ja muut tunkeutujat ainutlaatuisen tehokkaasti. Check Pointin täydellinen tietoturva-arkkitehtuuri suojaa yritysverkot mobiililaitteisiin asti, ja sen ratkaisuja ohjataan kattavan ja intuitiivisen hallintajärjestelmän kautta. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.