Check Point selvitti, miten hakkerit olisivat voineet murtautua miljoonille laitteille mediasoitinten ja tekstitysten avulla

*Check Pointin tietoturvatutkijat löysivät menetelmän, jonka avulla hakkerit voivat luoda haittakoodia sisältäviä tekstityksiä ja ottaa hallintaansa satojen miljoonien suosittujen mediasoitinten käyttäjien tietokoneet, puhelimet ja älykkäät televisiot.*

**ESPOO — tiistai 23. toukokuuta 2017**. Tietoturvayhtiö Check Point Software Technologies julkisti tänään tutkijoidensa löytämän uuden hyökkäystavan, joka olisi voinut uhata satoja miljoonia mediasoitinten käyttäjiä. Haavoittuvuus löytyi neljästä suosituimmasta avoimen lähdekoodin suoratoistopalvelusta, jotka ovat VLC, Kodi (XBMC), Popcorn Time ja Stremio. Niistä suomalaisille tutuin on VLC.

Hyökkääjä olisi päässyt käsiksi palvelun käyttäjän laitteeseen laatimalla haittakoodia sisältäviä tekstityksiä, jotka käyttäjä olisi sitten ladannut laitteelleen.

”Tekstityksille on yli 25 eri formaattia, jotka eroavat toisistaan ominaisuuksien suhteen. Koska ekosysteemi on pirstaleinen ja sen tietoturva rajoittunutta, haavoittuvuuksia on mahdollista löytää ja hyödyntää. Kohde on hyökkääjien näkökulmasta erittäin houkutteleva”, sanoi **Omri Herscovici**, joka johtaa Check Pointin haavoittuvuuksia tutkivaa työryhmää.

”Paljastimme tavan luoda haittakoodia sisältäviä tekstityksiä ja jaella ne automaattisesti miljoonille laitteille tietoturvaohjelmistojen ohi. Näin hyökkääjä saa laitteen ja sen sisältävän datan täyteen hallintaansa”, Herscovici jatkoi.

Elokuvien ja tv-ohjelmien tekstittäjät lataavat kääntämänsä tekstit yleensä verkossa sijaitseviin arkistoihin, kuten OpenSubtitles.org. Siellä ne indeksoidaan ja luokitellaan. Check Pointin tutkijat osoittivat, että manipuloimalla arkiston luokittelujärjestelmää mediasoitin saadaan lataamaan käyttäjälle automaattisesti tekstitys, joka sisältää haittakoodin.

Haavoittuvuudet on raportoitu alan käytäntöjä noudattaen, ja kaikki neljä yhtiötä ovat korjanneet ne. [Stremio](https://megahexandword.com/rnw_H8hGnAaWDkyg) ja [VLC](http://get.videolan.org/vlc/2.2.5.1/win32/vlc-2.2.5.1-win32.exe)) ovat julkistaneet uudet ohjelmistoversiot, joissa paikka on mukana. Herscovici kehottaa mediasoitinten käyttäjiä minimoimaan hyökkäysriskin päivittämällä suoratoistosoittimensa uusimpaan ohjelmistoversioon.

VLC:n uusimmalla, viime kesäkuussa julkaistulla versiolla on [yli 170 miljoonaa latausta](https://www.videolan.org/vlc/stats/downloads.html). Kodi (XBMC) [on yltänyt](https://www.tvaddons.ag/kodi-stats-march2017/) yli 10 miljoonaan eri käyttäjään päivässä ja lähes 40 miljoonaan käyttäjään kuukaudessa. Popcorn Timen käyttäjämäärästä ei ole saatavissa tietoa, mutta sen arvellaan nousevan kymmeniin miljooniin. Check Pointilla on syytä uskoa, että samanlaisia haavoittuvuuksia on muissakin suoratoistavissa mediasoittimissa.

Lisätietoja Check Pointin blogista: <http://blog.checkpoint.com/2017/05/23/hacked-in-translation/>

Video hyökkäyksen suoritustavasta: <https://youtu.be/vYT_EGty_6A>

**Lisätiedot ja haastattelupyynnöt:**

OSG Viestintä, Maija Rauha, [maija.rauha@osg.fi](mailto: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 ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yritysverkot kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.