Ettevaatust, sinu kohvimasin võib olla häkitud!

10 aastat tagasi - 25.11.2015 Autor: AM

Turvatarkvara tootja Kaspersky Lab laiendab oma tegevusala ja vaatab nüüd ka kodumasinate poole, sest neidki võivad ohustada turvaaugud. Nutikatel kodumasinatel on arvutitele ja nutitelefonidele sarnaselt turvaprobleemid. Kodumasinate turvaauke proovivad kurikaelad ära kasutada. Kaspersky Labi eksperdid veendusid selles eksperimendi käigus, milles uuriti müügilolevaid olmevidinaid.

Kodukasutajad lülitavad võrku mitte ainult arvuteid, tahvelid ja nutitelefone, aga ka mitmesuguseid olmeseadmeid, nagu televiisor, DVD/Blu-ray-mängija ja mängukonsoolid.

Eksperimendi jaoks valiti välja Google Chromecasti video voogedastuse USB-meedialpleier ja kolm nutitelefoni teel juhitavat seadet: beebimonitor, kohviaparaat ja kodu turvasüsteem. Nende üksikasjalik uurimine näitas, et tootjad teevad seadmete küberturbe tagamiseks suuri jõupingutusi, kuid ometi on igal nutitelefoniga juhitaval ühendatud seadmel peaaegu kindlasti vähemalt üks turvaprobleem, mis võib ründava poole jaoks läbimurdekohaks saada.

Näiteks avastati meediapleieril turvaauk, mis lubab kolmandatel isikutel seadmega ühenduda ja võõraste seadmete ekraani sisu näha. Seejuures võib suunatud antenni kasutamisel sellisesse seadmesse häkkida palju kaugemalt kui koduse WiFi-võrguga kaetud ala piires.

Beebimonitoris leitud turvaaugud lubavad häkkeritel IP-kaamera ja selle püsivara täielikult oma võimu alla saada. Sellise kohviaparaadi turvaauk, mille olekut saab spetsiaalse rakenduse abil jälgida, laseb kurikaeltel kätte saada koduse WiFi-võrgu salasõna. Paradoksaalsel viisil ei aita sel juhul võrku kaitsta ka salasõna sage muutmine, sest uuesti installimisel satub salasõna iga kord uuesti ohtu.

Kõige paremini on kaitstud kodu turvasüsteem. Aga ka siin on omad riskid, selgus testist: magnetitega töötavatest turvaanduritest saab häireta mööda hiilida, sest süsteemi on võimalik tavalise magneti abil petta.

Praegu on võrguvidinate turg veel üsna noor ja avastatud turvaaugud ei kujuta endast kasutajatele tõsist ohtu, nentisid testijad. Siiski ei ole see aeg enam kaugel, kui häkkerid hakkavad ründama ka ühendatud olmeseadmeid ja siis muutuvad need probleemid juba väga oluliseks.

Mida teha koduseadmete turvalisusega?

Kaspersky Lab soovitab nutiseadmete soeatmisel kontrollida, kas veebis on infot nende seadmete turvaaukude kohta ja võimaluse korral eelistada päris uutele, alles turule toodud seadmetele neid, mille tarkvara on juba korduvalt uuendatud.

„Kasutajad kipuvad arvama, et kui nad on oma arvutisse, nutitelefonisse ja tahvelarvutisse turvalahenduse installinud, on nad täielikult kaitstud. Tänapäeval ühendatakse aga kodus võrku veel muidki vidinaid ja olmeseadmeid. Turvaaukude olemasolu neis ei tähenda, et nende kasutamisest peaks loobuma, küll aga on mõistlik kaaluda nendega seotud riske ja mõelda, kuhu neid seadmeid paigaldada ja kuidas neid niimoodi võrku ühendada, et kurikaelad neisse häkkida ei saaks,” soovitab Kaspersky Labi ekspert Victor Alyushin.

Uuringu täpsema aruande leiab siit: https://securelist.ru/analysis/obzor/27244/uchimsya-zhit-v-internete-veshhej/.

FOTO: (CC) Tigerlily713 / PIXABAY

- Uudised

- Droonid
- Turvalisus