VIDEO: kui kohvimasin hakkab väljapressijaks

5 aastat tagasi - 27.09.2020 Autor: AM

Tahad teada, kuidas lõhnab ja kostab häkitud kohvimasinaga väljapressimine? Turvatarkvara tootja Avast blogis kirjutab Martin Hron ja näitab videos, kuidas see kõik käib, kui asjade Internet liiga ebaturvaline on.

Paljude koduseadmete ja asjade interneti vidinate püsivara uuendus käib üle õhu (OTA ehk *Over-the-Air*). Nii käis see ka testis osalenud kohvimasinal, mis saab uuendusi ja suhtleb väga lihtsa TCP protokolliga, millel puudub igasugune krüpteering. Andmed saadetakse kujul *käsk - andmed - terminaator (0x7E)*. Masin suhtleb võrgus üle TCP, pordi 2081 kaudu. Rohkem polegi eriti vaja teada, et hakata masinale käsklusi andma. Mida üks või teine käsklus teeb, selle leiab Githubist.

Kuid vajalik on ka kohvimasina püsivara uuendamine. Selleks tuleb hankida uuendusfail, see lahti võtta, lisada kahjulik kood ja üles laadida.

Siis peab natuke võrguliiklust kuulama või äppi uurima, mis andmeid sel hetkel masinaga vahetatakse. Martin Hron avastas peagi, et käsk 0x6D 0x7E viibki seadme tarkvara uuendamise režiimi. Kuid siis veel midagi ei juhtunud - selgus, et mobiiliäpp ise sisaldab uuendatavat tarkvara ning iga äpiuuendusega saabub ka tarkvarauuendus, kohvimasina tarkvara eraldi ei kontrollitagi. Seega pidi häkitud tarkvara mobiiliäpi sisse istutama. Aga ega seegi kuigi keeruline pole. Kõige keerulisem on *Firmware* enda lahtimuukimine assembleris. Selleks peab teadma, mis protsessorile kood on kirjutatud.

Kohvimasina tarkvara muutmiseks peab veel kodusesse WiFi võrku sisse häkkima. See on juba omaette teema, aga ebauturvalise ruuteriga tehtav. Siis pole vaja kohvimasinat väljapressijaks muutes isegi kohale minna. Veelgi lihtsam masinale ligipääsu mõttes on aga kasutajale pahavaraga mobiiliäpi sokutamine, mis juba ise kõik vajaliku kohvimasinaga ära teeb ilma võrku häkkimata. Siin on kõige keerulisem *Social Engineering*u kasutamine, et kuidagi meelitada kasutajat endale seda mobiiliäppi telefoni paigaldama.

Selle konkreetse kohvimasina puhul lisab kindlust häki õnnestumisele veel see, et masinale enam tootja tuge ei paku, seega ei muuda keegi kunagi nende masinate tarkvara turvalisemaks ja uuendusi ei saabu. Füüsiliselt võivad ju kodumasinad pidada vastu palju aastaid, kuid tootja huvi vanade masinate turva- ja

tarkvarauuenduste vastu kaob palju kiiremini ning kõik need vanad ebaturvalised koduseadmed jäävad võrgus ripakile esimeste huviliste rünnakute kätte.

Vaata lähemalt Smarter Coffee seadme väljapressimismasinaks muutmise kohta **siit**.

Vaata ka seda, kuidas kohvimasin hakkab trikitama, vett kuumale plaadile kõrvetama ja ubasid lõputult keerutama, siit videost:

- Uudised
- Videod

- Kodumasinad
- Turvalisus

Pilt


WANT YOUR
MACHINE BACK?
bit.ly/2wiH5aS