Uus häkk: küberkurjategijad õppisid ära sularahaautomaatidest raha varastamise pahavara abita

7 aastat tagasi - 19.12.2018 Autor: AM

2018. aasta jooksul tühjendasid kurjategijad sularahaautomaate Ida-Euroopa riikides, omades oma arsenalis vaid sülearvuteid ja paari legaalset programmi.

Üheks neist osutus sularahaautomaadis asuva raha väljastava seadme KDIAG töö testimiseks mõeldud utiliidi modifitseeritud versioon. Varem kasutasid selle programmi sama versiooni küberkurjategijad grupeeringust Carbanak.

KoffeyMaker'i kasutatav varastamise põhimõte sarnaneb Cutlet Maker'i omaga, ent seekord ei vajanud kurjategijad ühtegi kahjutoovat programmi, sest kõik vajalikud tööriistad ja juhendid oli võimalik alla laadida spetsialiseeritud saitidelt. Rünnaku läbiviimiseks oli vaja muukida sularahaautomaati ja ühendada oma sülearvuti USB kaudu raha väljastava seadmega. Seejärel jätab kurjategija oma seadme sularahaautomaadi korpusesse, sulgedes selle ja läks minema. Edasi toimus sülearvuti juhtimine eemalt.

Sularahaautomaati „petta" aitasid eelnevalt installitud draiverid, tänu millele tajus sularaha väljastav seade kõrvalist sülearvutit sularahaautomaadi arvutina. Edasi käivitas kurjategija KDIAG'i muudetud versiooni, mis võimaldas vajalikul hetkel väljastada sularaha väljastavas seadmes olevat raha. Pärast seda tarvitses vaid kindlal hetkel tulla ja raha endale võtta. Mõne aja pärast tulidki kurjategijad tagasi seadme ja raha järele.

„Nendes vargustes ei kasutatud kahjutoovat tarkvara ning sularaha väljastava seadmega ühendatavad sülearvutid võtsid kurjategijad kaasa, mistõttu on äärmiselt keeruline tuvastada, kes on intsidentide taga ning kas kõne all on uus grupeering või eraldi juhtumid," räägib Sergei Golovanov, Kaspersky Lab'i juhtiv viirusetõrje ekspert. „Need intsidendid kinnitavad veelkord, et kurjategijad ei pea omama sügavaid teadmisi ITs, veel enam – aina sagedamini valivad nad oma eesmärkide saavutamiseks legaalseid tööriistu, mis võimaldavad neil märkamatuks jääda," lisab ta.

Selliste varguste vastutoimeks on vaja kindlalt kaitsta sularaha väljastava seadme ja sularahaautomaadi ühenduse osa – mitte keegi kõrvaline ei tohi saada nendele

ligipääsu. Kui tehnilised võimalused lubavad, siis tuleb häälestada šifreerimine sularaha väljastava seadme ja arvuti vahel – see abinõu aitab vältida sularahaautomaadi juhtimise keskuse vahetamist.

KoffeyMaker varguste lainest üksikasjalikumalt lugege siin.

- Uudised

- Turvalisus

Pilt