Veel üks suurelt leviv pahavara paneb WanaCry väljapressimisviiruse ees ukse kinni

9 aastat tagasi - 19.05.2017 Autor: AM

Viirused läksid omavahel kaklema, milline paljastatud NSA turvaaukude kaudu kasutajate arvutitele ligi pääseb. Turvaettevõte Proofpoint kirjutab, et WanaCry´st veel suurem viirusepuhang, mis kasutab samuti ära NSA-st lekkinud mitut Windowsi turvaauku, paneb peale arvuti nakatamist SMB võrgu kinni (SMB - *Microsoft Server Message Block*) ja hakkab nakatunud masinas krüptoraha kaevandama. See tähendab, et viirus näppab arvuti ressurssi ja lunaraha ei küsi, kuid tarvitab riistvara enda peremehele lisaraha teenimiseks.

Kasutaja jaoks tähendab see, et arvuti ressurss on kogu aeg maksimaalselt hõivatud mitte kasuliku töö, vaid võõra heaks tehtava töö tegemisega ja teenib sellega raha hoopis kellelegi teisele. Arvatakse, et niimoodi krüptoraha kaevandades teenivad viiruse loojad hoopis rohkem, kui seni on WanaCry väljapresimistarkvaraga inimestelt raha välja pressitud.

Viirus, mis peale arvuti nakatumist ukse WanaCry ees kinni paneb, sulgedes SMB võrgu kasutamise väljastpoolt, kannab nime Adylkuzz ja on tüübilt krüptoraha kaevandav pahavara. Adylkuzz aitas ka nädalavahetusel WanaCry massipuhangut ohjeldada, sokutades end turvamata arvutitesse ja takistades teistel viirustel sama SMB turvaauku edasi kasutada, pannes selle enda selja taga lihtsalt kinni.

Rünnakut juhitakse suure hulga VPS-idega (virtuaalsed privaatserverid), mis skannivad võrgust porte 445 ja kui turvaauk on leitud, installivad Doublepulsari nimelise tagaukse. See omakorda asub tegutsema ja käivitab arvutis krüptoraha kaevandaja Adylkuzz´i.

Viirusetõrjetootja Symantec ei pea seda siiski nii ohtlikuks, kuna erinevalt WanaCry´st ei suuda Adylkuzz ise ühest arvutist teise edasi levida.

Mis on krüptoraha kaevandaja?

Krüptoraha kaevandaja on programm, mis teeb hulga keerulisi arvutusi, mille annab ette krüptoraha süsteem ja arvuti omanik teenib selle eest krüptoraha. Teenistus on väike ja arvutilt üsna mahukat arvutamist nõudev, kuid rikkaks saamise valem peitub massilisuses: kui ühe omaniku heaks teevad arvutusi sajad

või tuhanded nakatunud arvutid, siis võibki koguneda suurem summa, kui paarkümmend tuhat eurot teeninud WanaCry levitajatel. Adylkuzz ei kaevanda mitte kõigile tuntud Bitcoineid, vaid samasugust, kuid vähem teatud Monero krüptoraha (kurss 1 XMR = 23 EUR). Üks Monero konto, kuhu kaevandatav raha kogunes, oli teeninud mõni päev tagasi juba 22 000 dollarit, kuid neid aadresse on mitmeid.

Adylkuzzi levitaja on tegutsenud juba oluliselt rohkem päevi kui WanaCry ja kogunud ka raha rohkem. Selle viiruse vastu võitlemiseks aitavad samad abinõud, nagu Wanacry puhul: SMB teenus kohe sulgeda või kiirelt Windowsi turvauuendus teha. Microsoft tõi isegi Windows XP-le, mida ametlikult enam ei toetata, välja uuenduse, mis seda tüüpi viiruste levikut tõkestab.

- Uudised
- Turvalisus

Pilt

