Colonial Pipeline´i naftatorustiku küberrünne on ilmselt üks suurim selline digiväljapressimine

5 aastat tagasi - 10.05.2021 Autor: AM

Kui tavaliselt nõuavad küberväljapressijad ettevõtetelt või eraisikutelt nende arvutis olnud andmete dekrüpteerimise eest lunaraha, siis seekord on olukord tõsisem. Küberkurjategijate rühmitus DarkSide sai USA idaranniku 8850 km pikkust naftatorustikku omavalt Colonial Pipeline´ilt näpata ligi 100 GB andmeid, mille dekrüpteerimise eest oodatakse lunaraha, kuid mis võimaldavad ka suure infrastruktuuri seisma panna. Hiiglaslik tehnoloogiarajatis suletigi ettevõtte enda poolt peale rünnet, kuna firma kahtlustab, et kättesaadud andmetega võivad pahalased võrku rünnata ja mõned osad sellest rivist välja lüüa.

Colonial Pipeline´i torustik transpordib naftatooteid Texasest USA idarannikule, sh New Yorgi piirkonda. Seda torustikku pidi liigub 45% kogu idarannikule transporditavast kütusest. Iga peatatud torustiku tööpäev ähvardab tuua suurema kütusepuuduse ning mõjutada isegi nafta maailmahindu, mille kohta arvatakse, et mõne päeva pärast võib see naftatorustiku seiskumise tõttu tõusta mitu protsenti.

Küberrünnaku korraldanud rühmitus DarkSide omab tumeveebi lehekülge, kus muuhulgas avaldatakse ka andmeid, mis on väljapressimisrünnakutega kätte saadud ja mille eest pole lunaraha makstud (nii-öelda "häbipost"). Rühmitus tutvustab end robinhoodilikult, lubades lunaraharünnakutega saadud raha heategevuseks annetada ning mitte rünnata haiglaid ja haridusasutusi.

Augustist tegutsema hakanud grupi päritolu pole teada, aga mõned vihjed selle tegevuse suuna kohta annab rünnakute iseloom - kunagi pole rünnatud endise Nõukogude Liidu ja idaploki riikide ettevõtteid, vaid ainult Lääne-Euroopa ja USA firmasid. DarkSide´il on oma klienditeenindus ja avalike suhete osakond, ohvritelt on kätte saadud miljoneid.

DarkSide´i tööriistu analüüsis USA tarkvaratudeng Chuong Dong, kes jõudis järeldusele, et kasutatakse suhteliselt tavalist väljapressimistarkvara lahendust. Kui pahavara on kasutaja arvuti üle võtnud, siis kontrollib see ühtlasi, kas tegemist on administraatoriõigustes kasutajaga ning kui on, siis püüab oma õigusi eskaleerida kõigisse teistesse süsteemidesse, kuhu võimalik. Kõigis ligipääsetud masinates info krüpteeritakse, kuid krüpteerimiskiirus on Dongi sõnul mitte just

muljetavaldavalt kiire. Siiski õnnestus pahavaral torujuhtmefirmas piisavalt kärmelt tegutseda, et olulised andmed kätte saada ja lukustada.

Associated Pressi ajakirjanikul pole õnnestunud DarkSide´iga Colonial Pipeline´i teemal ühendust võtta, kuigi grupil on olemas ka PR kontaktid ja tavaliselt vastatakse sealt päringutele väga kiirelt. See vihjab AP teatel sellele, et ohvriga kas peetakse läbirääkimisi või on saavutatud mingi kokkulepe. Ka USA presidendi administratsioon on lubanud sekkuda juhtumi lahendamisse, juhtumit uurib ka FBI ja mitmed küberturvalisuse asjatundjad oletavad selle põhjal, et küberrünnak sihtmärgile toimus pigem juhuslikult. Ilmselt DarkSide ei soovinud sellist tähelepanu ja USA luureasutuste sekkumist, nii suure portsu otsa võidi sattuda juhuslikult robotitega võrku läbi kammides.

- Uudised
- Turvalisus

Pilt