Kas teadsid, et sinu arvutis võib olla krüptovaluuta kaevandus?

29. september 2017 - 12:10 Autor: AM

Krüptovaluuta kaevandamine oma arvutis pole teab mis tulutoov, kui just arvuti külge pole ühendatud kasti kümnete võimsate videokaartidega. Kui aga kaevandamine toimub sadades, võib-olla isegi tuhandetes võõrastes arvutites, siis võib rikkus juba kiiresti kasvada. Ja just seda teevad ka pahavaralevitajad.

Varjatud *mining*'uks ehk krüptoraha kaevandamiseks (krüptovaluuta genereerimiseks) mõeldud pahavara kogub kurjategijate hulgas aina enam populaarsust. Viimase kuuga avastas Kaspersky Lab sellist viisi kasumi saamiseks loodud mitu suurt robotite võrku – igaüks neist koosneb tuhandetest nakatatud arvutitest. Lisaks märgivad turvaeksperdid *miner*'ite (kaevandajad, programmid krüptovaluutade genereerimiseks) installimise katsete arvu kasvu organisatsioonide serveritesse. Analüütikute arvutuste järgi toob kaevandamisvõrk selle omanikele tulu mõnikord kuni 30 tuhat dollarit kuus. Ning kõige levinumateks valuutadeks varjatud kaevandamisel on Monero (XMR) ja Zcash.

Kõige sagedamini satuvad krüptovaluutade kaevandajad arvutitesse läbi reklaamitarkvara paigaldajate, mida levitatakse sotsiaalse sahkerdamise (*social engineering*) abil. Sealjuures kasutaja laeb neid paigaldajad alla iseseisvalt, näiteks tasuta tarkvarana või võtmetena litsentseeritud toodete aktiveerimiseks failide üles- ja allalaadimise saitidelt. Eksperdid fikseerisid ka läbi tarkvara nõrkade kohtade kaevandajate levitamise juhtumeid. Nii osutus EternalBlue nõrga koha kasutamisel kahjutooja ohvriks server, mis on kurjategijatele eriti soodne selle suurema tootlikkuse tõttu (jaksab rohkem kaevandada).

Kaevandamine iseenesest pole ebaseaduslik, pealegi – kasutaja on täiesti võimeline installima sellist tarkvara ja kasutama seda krüptovaluuta kaevandamiseks. Need asjaolud teevad arvutis või serveris kasutaja loata varjatud kaevandamise tuvastamise keerulisemaks. Pealegi nende programmidega kaasnevad sageli lisateenused, mis tagavad kinnistumise süsteemis, automaatkäivitamise arvuti sisselülitamisel ja varjatud kaevuritöö. Iseäranis jälgivad sellised kaasnevad teenused rakenduste käivitamist süsteemis ja peatavad kaevandaja tegevuse, kui töötab mõni aktiivsusmonitooringu programm. Samuti kontrollivad need programmid püsivalt kaevandaja olemasolu kõvakettal ja taastavad selle iga kord peale kustutamist.

„Kurjategijad kasutavad, nagu alati, iga võimalust ebaseaduslikul teel kasumi saamiseks ning teenimisviisid arenevad pidevalt. Krüptovaluutade turu areng avas uued võimalused küberkurjategijatele, kuid et kasutada neid võimalusi täiel määral, vajavad nad võõra seadme võimsusi. Ning see omakorda soodustas nende juhtumite tormilist kasvu, mil kaevandajaid installitakse kasutaja teadmata. Osaliselt saab seda varjatud kaevandamise buumi seletada sellega, et krüptovaluutade turu sündimise etapil oli palju lihtsam kaevandada ja selle pealt raha teenida kui praegu," seletab Evgeny Lopatin, Kaspersky Lab'i analüütik.

Üksikasjalikumalt varjatud kaevandamisest saab lugeda siit.

- Uudised

- Tarkvara
- Turvalisus