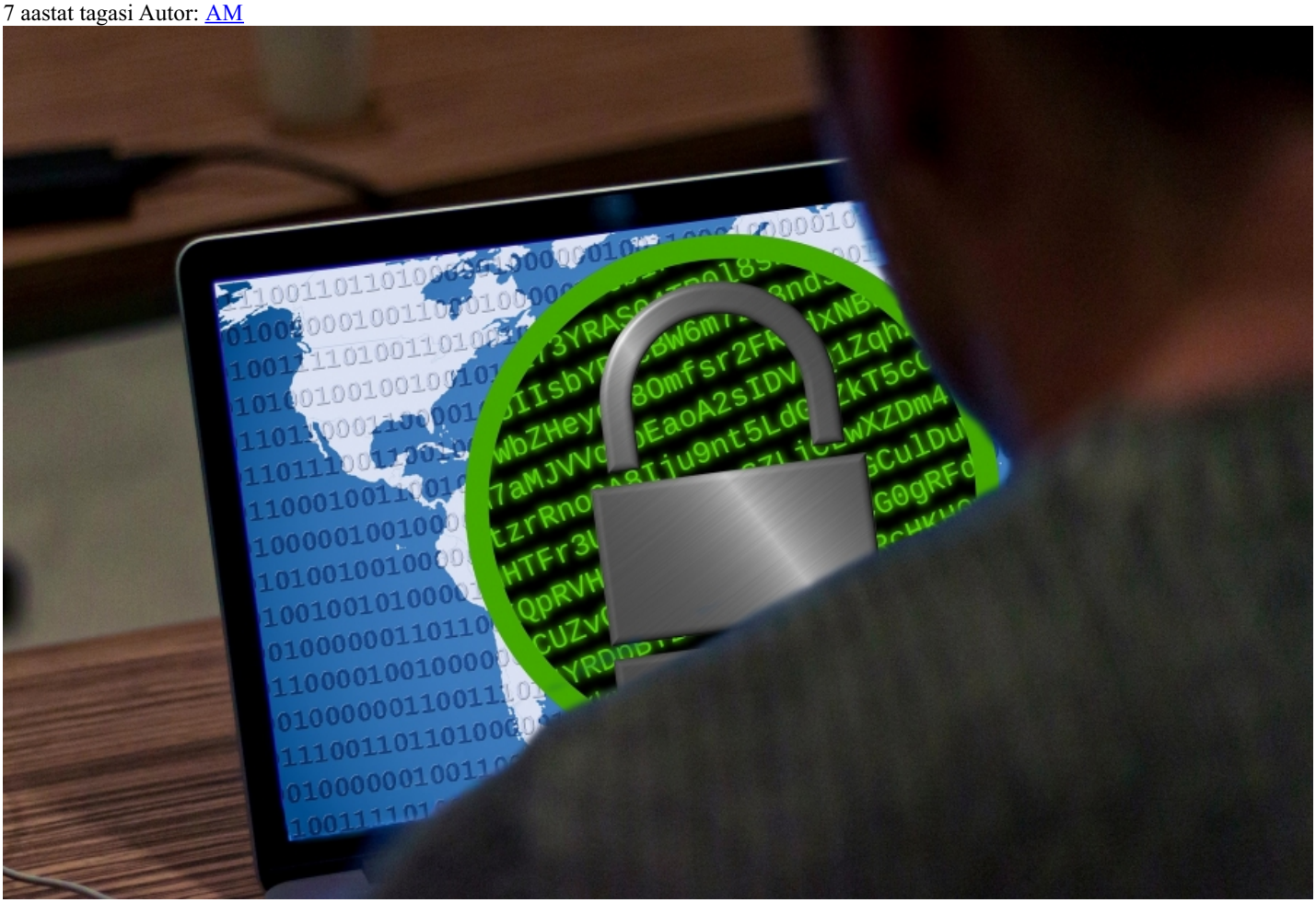
Väljapressimistarkvara ExPetr/Petya/NotPetya ei annagi andmeid tagasi, isegi kui lunaraha on makstud

7 aastat tagasi Autor: AM



Ehkki see pole veel sajaprotsendiliselt kinnitust leidnud, pakub Kaspersky Labi spetsialist Anton Ivanov pärast väljapressimistarkvara ExPetr (tuntud ka kui Petya/NotPetya) analüüsimist välja, et viimastel päevadel palju paha tekitanud pahalane ei suudagi krüpteeritud faile taastada, isegi kui ohver selle eest lunaraha maksab.

Kaspersky nimetab Petya/NotPetya lunaraha nõudvat pahavara nimega ExPetr, kuna see olevat siiski täiesti uus ründetarkvara, mitte kunagi tuntust kogunud Petya uus versioon. Ehkki ühe nakatumisvõimalusena kasutab ExPetr ära NSA-st lekkinud EternalBlue turvaauku Windowsis, on sellel ka muid levikuvahendeid ja krüpteerimine käib samuti teistmoodi.

Kaspersky spetsialisti sõnul maskeerib pahavara end väljapressimistarkvaraks, küsides ka lunaraha, kuid tegelikult on tegemist nö *Wiper*-tüüpi pahavaraga (*wipe* = puhtaks pühkima, jäädavalt kustutama). See tähendabki, et nakatunud arvutist pühitakse andmed jäädavalt ning neid kätte saada pole enam võimalik.

Pole teada, kas selline käitumine oli viiruseloojate eesmärk või oli tegemist lihtsalt kehvasti programmeeritud ja vigase koodiga.

Nakatunud arvuti ekraanile ilmub teade, milles palutakse saata oma Bitcoini rahakoti ID ja personaalne ExPetr´i kuvatav ID e-posti aadressile, mis on samuti antud, vastu saadetakse dekrüpteerimisvõti.

Personaalne ID genereeritakse aga viiruses funktsiooniga CryptGenRandom, mis sisuliselt tekitab juhusliku arvude jada. Seega pole saadetud võtmega võimalik suurt midagi teha.

Samale tulemusele jõudis sõltumatult ka Comae turvaekspert Matt Suiche.

Lisaks eksisteerib ka teine probleem: e-posti aadress, kuhu oma (juhuslikult genereeritud) võti tuli saata, on teenusepakkuja poolt juba kinni pandud:

> Victims keep sending money to Petya, but will not get their files back: No way to contact the attackers, as their email address was killed. pic.twitter.com/68vxThNIPM
>
> — Mikko Hypponen (@mikko) June 28, 2017

Saksa e-posti teenuse pakkuja Posteo otsustas väljapressijate e-postkasti sulgeda, et nad ei saaks raha välja pressida. Kaspersky Lab on avastanud 30. juuni seisuga 2000 ExPetri nakatumisjuhtu. Eile oli meedias uudis ka Eestis nakatunud ehituspoodide ketist, mis ohvriks langes. Enamus ohvreid aga olid pärit Upkarinast. Kaspersky soovitab nakatumise vältimiseks ettevõtte võrgus keelata KSN ja System

Watcher komponendid, Kaspersky HIPS komponendiga saab keelata faili perfc.dat käivitamine, samuti tuleks blokeerida PSExec utiliit paketis Sysinternals.

AM-is ilmus ka lugu lihtsast vaktsiinist pahavara vastu, kuid selle tõhusus kestab seni, kuni viiruse koodi pole vastavalt muudetud. Miski ei keela viiruse loojatel seda üht failinime muuta, et ExPetr ehk Petya/NotPetya saaks edasi levida.

- Uudised
- Turvalisus