Krüptoviiruse Petya/NotPetya vastu on väidetavalt leitud lihtne ennetav vaktsiin

8 aastat tagasi - 28.06.2017 Autor: AM

Maailma tabanud uus krüptoviirus Petya/NotPetya, mis on eelmise hiti WanaCry modifitseeritud järeltulija, tabas ka Eestis mitmeid ettevõtteid, krüpteerides andmed ja nõudes nende lahtikrüpteerimise eest lunaraha. Levib aga info, et viirust on võimalik oma arvutitest eemal hoida, lisades sinna ühe (tühja) faili.

Kas see ettevaatusabinõu ka töötab, selle kohta veel täiesti kindlad andmed puuduvad, kuid mitmetes turvafoorumites ja ka turvatarkvara tootjate blogides on seda lahendust käsitletud.

Cybereasoni küberturvateadlane Amit Serper avastas, et viirus Petya (NotPetya/SortaPetya/Petna) otsib käivitudes Windowsi kataloogist üht faili ja kui see eksisteerib, siis ei asu kõiki andmeid krüpteerima. Seega aitab ise sellenimelise faili Windowsi kataloogi tekitamine suurema kahju ära hoida, küll aga ei kaitse Petya/NotPetya nakatumise eest.

Seda lahendust on kinnitanud ka PT Security, TrustedSec ja Emsisoft.

Kui luua fail nimega perfc oma arvutis ja määrata selle õigusteks *Read Only* (ainult lugemiseks), siis Petya/NotPetya edasi ei tegutse.

Sellepärast ongi see pigem lahja vaktsiin kui antiviirus. Pole välistatud, et viiruse loojad selle omaduse kiirelt uuematest versioonidest kõrvaldavad.

> Fail nimega **perfc** tuleb luua kataloogis **C:\Windows** ja õigusteks määrata **read only**.

Riigi Infosüsteemi Ameti andmetel on Eestis asuvatest ettevõtetest saanud pahavaraga pihta kaks Saint-Gobaini kontserni kuuluvat ettevõtet. Üks nendest on Ehituse ABC.

„Täna kella 10.00 seisuga ükski elutähtsat teenust osutav ettevõte või riigiasutus küberrünnaku ohvriks langemisest ei ole teada andnud. RIA intsidentide käsitlemise osakond (CERT-EE) tegeleb hetkel aktiivselt võimalike intsidentide kaardistamise ja analüüsiga," ütles CERT-EE juht Klaid Mägi.

CERT-EE palub ettevõtetel, kelle IT-süsteemid on pahavaraga nakatunud, anda sellest teada CERT-EE valvenumbrile 663 0299 või meiliaadressile cert@cert.ee.

Leviv krüptoviirus kasutab ära Windowsi turvaauku, mida kutsutakse Eternal Blue´ks ja mille paikas Microsoft sel kevadel Windowsi turvauuendusega. Sama turvaohtu kasutas ära ka WanaCry krüptoviirus, millest kirjutasime. Usutakse, et uuel krüptoviirusel on ka muid ründevektoreid ettevõtete võrgus levimiseks. CERT-EE soovitab lunavaraga nakatumise ärahoidmiseks paigaldada Windowsi operatsioonisüsteemi viimased turvauuendused ning sulgeda SMB versiooni 1 kasutamine organisatsiooni arvutites.

Praegu kiiresti leviv krüptoviirus on tabanud nii suuri kauplustekette, logistikafirmasid kui riigiasutusi üle maailma.

> Супермаркет в Харькове pic.twitter.com/H80FFbzSOj
>
> — Mikhail Golub (@golub) June 27, 2017

> #Nieuws: Rotterdamse containerterminal ligt plat door hack. O.a. 's werelds grootste rederij Maersk Line getroffen door grote cyberaanval. pic.twitter.com/liW1Tumrju
>
> — Paul Henriquez (@OpiniePaultje) June 27, 2017

> Saint-gobain uk pic.twitter.com/PtHD031ccY
>
> — The Animal (@AnimalDubz) June 27, 2017

> A tipster sends along this photo taken outside DLA Piper's D.C. office around 10am. #Petya pic.twitter.com/HWS4UFlvQR
>
> — Eric Geller (@ericgeller) June 27, 2017

> Vice Prime Minister of Ukraine, Павло Розенко (Pavlo Rozenko) on Facebook. This is what Petya looks like when it's encrypting your drive. pic.twitter.com/RgPtfuWK7p
>
> — Mikko Hypponen (@mikko) June 27, 2017

- Uudised

- Tarkvara
- Turvalisus

Pilt