Arvuteid ründab massiliselt väljapressimispahavara WanaCry

9 aastat tagasi - 13.05.2017 Autor: AM

Reedel algasid üle maailma massilised "WanaCry" nimelise pahavara rünnakud, mida peetakse maailma üheks suurimaks viiruserünnakuks. Kahju on see kõige rohkem tekitanud Suurbritannia meditsiiniasutustele, kus sellepärast on ära jäetud operatsioone ja raskendatud on patsientide vastuvõtt, kuid ka mujal maailmas levib vastik viirus ja nõuab peale andmete krüpteerimist nakatunud arvutites lunaraha.

Viirusetõrjetootja Avast andmetel nakatas väljapressimistarkvara (ametliku nimega) WanaCrypt0r 2.0 reedel üle 57 000 arvuti (laupäeva hommikuks juba üle 110 000). Täna on viiruse levik veidi aeglustunud, kuna leiti võimalus selle tööd takistada.

Viirust on nimetatud ka nimedega WanaCrypt0r ja WCry. Ohvriks langesid Hispaania telekomiettevõte Telefonica, mitmed haiglad ja logistikaettevõte Fedex. Riikidest sihib viirus kõige enam Venemaad, Ukrainat ja Taiwani, aga on leitud juba 99-st riigist üle maailma.

Riigi Infosüsteemi Ameti sõnul pole Eestis veel seda väljapressimistarkvara märgatud:

Viirus on juba jõudnud Lätti ja muuhulgas on selle kasutajaliidesel valik lülitamiseks läti keelele, et lunarahanõudest saaksid aru ka need lätlased, kes inglise keelt ei mõista (eesti keelt ei pakuta).

Aprillis esimest korda nähtud pahavara kasutab ära hiljuti lekkinud NSA häkkimistööriista koodist leitud üht Windowsi turvaauku ründavat vahendit, mille kaudu levimine on eriti massiline. Väljapressimise taga olevat häkkerirühmitus Shadow Brokers, kes näppas koodi oletatavalt NSA-ga seotud Equation Group´i tagant ja avalikustas. Turvaaugule ETERNALBLUE või MS17-010, mida ära kasutatakse, lasi Microsoft välja Windowsi uuenduse juba märtsis, aga nakatuvad need arvutid, millel uuendust pole tehtud.

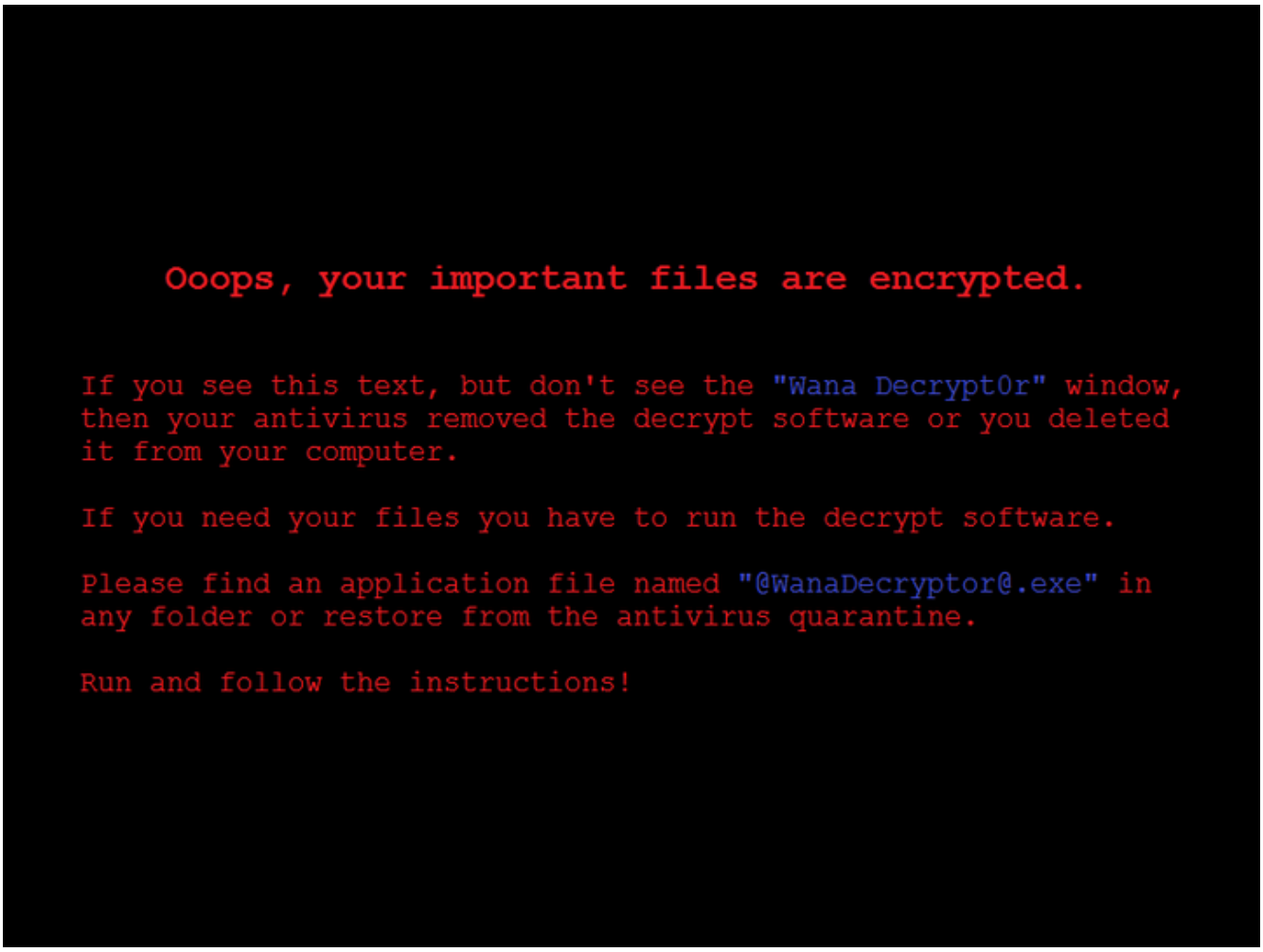
Shadow Brokers on mõnedel andmetel Vene valitsusele lähedalseisev rühmitus, mõned Vene tehnoloogiauudised aga väidavad, et kuna Wanacry ründas ka Vene

riigiasutusi, siis tegemist on pigem lääne häkkeritega, kes NSA koodi ära kasutasid.

Nagu allolevalt pildilt näha, nõutakse Telefonicalt 300 dollarit bitcoinites, et oma väärtuslikud andmed tagasi saada:

> As you can see from the screengrab in Engadget Spain's report on the Telefonica attack https://t.co/tGJFqTOzxW pic.twitter.com/OPMLpV3FqY
>
> — Graeme Neill (@gnei11) May 12, 2017

Nakatumine toimub kas mõne kahtlase faili klõpsamisel või Windowsis lappimata jäänud turvaaugu kaudu, seejärel krüpteeritakse kõik arvutis olevad ja ligipääsetavatel võrguketastel asuvad failid, mis saavad faililaiendi *.WNCRY*. Wana Cry muudab ka töölaua taustapilti, kuhu ilmub selline kiri:



Kõige esmane kaitse pahavara vastu on uuendada oma Windows kohe (*Kõik sätted - Värskendamine ja turvalisus*). Ka ametlikult mittetoetatavate operatsioonisüsteemide - Windows XP, Windows Vista ja Windows 7 jaoks on turvatäiendus Microsoftilt saadaval sellel lingil.

EKRAANIPILDID: AVAST

- Uudised

- Tarkvara
- Turvalisus

Pilt