

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 meditsiinasutustele, 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 telekomiettevõtte Telefonica, mitmed haiglad ja logistikaettevõtte 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 häkkimistöörühma 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 tehnoloogiaudised 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:

Oops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

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

Wana Decrypt0r 2.0

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw