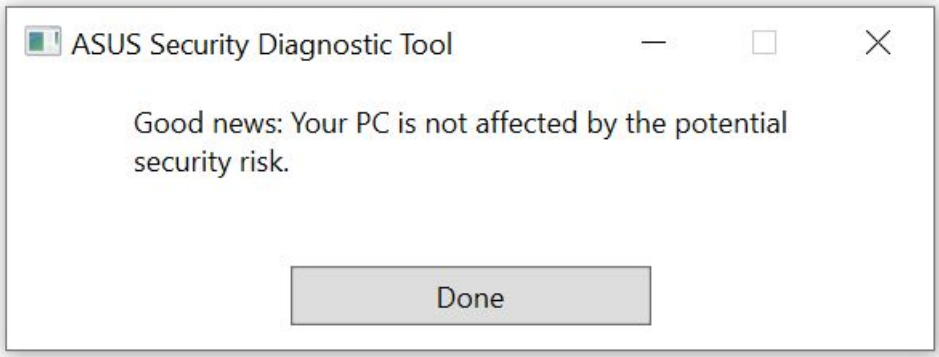
Asuse vastus uuenduste serverisse sokutatud pahavara uudistele

5 aastat tagasi Autor: AM



Kirjutasime teisipäeval, et Asuse tarkvarauuenduse serverisse sokutati pahavara, mis otsis kindlaid MAC aadresse, et neisse siis veel midagi täiendavat (nuhkimiseks) sokutada. Nüüd on Asus uuenduste tarkvara ära uuendanud ja pakub ka tööriista, et oma masinast pahalast avastada ja kõrvaldada.

Tegemist oli sihitud rünnakuga, mis Asuse esindajate sõnul polnud suunatud tavakasutaja, vaid kindlate organisatsioonide vastu. Seega kui tavakasutaja arvuti ka nakatus, ei tehtud seal tõenäoliselt midagi, sest vajati kindlat sihtmärki.

Kaspersky viirusetõrje tarkvara tootja mainib, et sihtmärke oli 600.

ASUS Live Update on tarkvara, millega Asuse arvutid kontrollivad, kas olemas on uusimad draiverid ja riistvara juhtprogrammid ning uuendab neid, kui vaja. Live Update tõmmatakse kõigepealt alla Asuse enda serverist.

Mingil põhjusel sai keegi serverisse ligipääsu ja sokutas pahavaraga koodi allalaadimiseks sinna, kust miljonid masinad seda automaatselt alla tõmbavad.

Praeguseks on tarkvarale välja tulnud uuendus - versioon 3.6.8 Live Update´i tarkvarast, mis kõrvaldas võimaluse manipuleerida allalaadimistega ja nüüd toimub uuendus täielikult krüpteeritud kanali abil.

Kui keegi tunneb end ohustatuna, saab kontrollida Asuse tööriistaga, kas tema masin on puhas või mitte. See on lihtne allalaaditav programm (paki lahti), mis tuleb käivitada. Allalaadimine toimub siit:
dlcdnets.asus.com/pub/ASUS/nb/Apps_for_Win10/ASUSDiagnosticTool/ASDT_v1.0.1.0.zip

Oma Live Update´i versiooni kohta saad vaadata siit:
https://www.asus.com/support/FAQ/1018727/

Kaspersky Lab'i globaalse ohtude uuringute ja analüüsi keskuse juht Costin Raiu märkis, et rünnak ASUS'ele erineb muudest taolistest: „See rünnak erineb eelmisest keerulisuse ja varjatuse kõrge taseme poolest. Sihtmärkide filtreerimine kirurgilise täpsusega MAC-aadresside järgi on üks põhjuseid, miks ei õnnestunud rünnakut niivõrd kaua tuvastada. Kui te pole sihtmärk, siis kahjutoov programm on praktiliselt märkamatu," rääkis ta portaalile Motherboard.

Kahjutoov programm hakkas levima 29. jaanuaril. Enamik nakatatud masinatest (umbes 18%) asusid Venemaal. Nakatumiste arvu poolest järgnesid Saksamaa ja Prantsusmaa. 5% nakatatud klientidest asusid USAs.

- Uudised
- Turvalisus