Asuse tarkvarauuenduste serverisse sokutati pahavara, nakatati miljon masinat

7 aastat tagasi - 26.03.2019 Autor: AM

Nii, nagu 2017. aastal sokutati tarkvara CCleaneri tarkvarauuenduste serverisse pealtnäha usaldusväärselt signeeritud pahavara, nii tegid häkkerid samamoodi Asuse tarkvarauuenduste serveris, istutades sinna Asuse signeeringuga uuenduse, mis sisaldas väikest troojalast.

See troojalane ei tahtnud siiski kõigi enam kui miljoni masina järgi nuhkida, vaid tarkvarasse olid sisse kirjutatud kindlad MAC-aadressid, mis huvi pakkusid. Neid oli üle maailma, peamiselt USA-st, Venemaalt, Saksamaalt, Prantsusmaalt ja Itaaliast.

Pahalane nimega Operation Shadowhammer on viirusetõrjujate poolt nimetatud "spioonitarkvaraks", kuna sisaldab mõnesid selle elemente: levib võimalikult laialdaselt, kuid võtab põhjalikumalt ette teatud kindlad sihtmärgid, mida siis täiendavalt nakatatakse. Kust täpselt spioonitarkvara pärit on, pole veel teada.

Kaspersky pani üles lehekülje, kust saab uurida, kas ka sinu arvuti MAC-aadress võiks olla selle pahalase sihtmärgiks. Selle leiab Windowsi käsureaga *ipconfig /all* ja tulemuste realt *Physical Address* ongi MAC aadress. Nimekirjas on siiamaani tuvastatud enam kui 600 aadressi.

Esimesena kirjutas Asuse lekkest Motherboard.

- Uudised
- Turvalisus

Pilt


7
8
9
/
4
5
6
*
1
2
3
−
enter
0
.
+