

Saddamin hirittäjäisillä puffataan haittaohjelmia

9.1.2007 08:14 — Antti Kirves

Irakin entisen hirmuhallitsijan teloituksesta tehtyä videota käytetään nyt erilaisten haittaohjelmien houkuttimena. Saddam Husseinin varjolla levitetään ainakin kolmea troijalaista.

Banload.BSW on troijalainen, jota levitetään sähköpostissa "video_sadan.exe" -nimisenä liitetiedostona. Se lataa saastuttamalleen koneelle toisen, Banker-nimisen troijalaisen ja ohjaa selaimen youtube.com-sivustolle, jossa se listaa teloitusvideohaun tuloksia.

Myös Delf.ACC ohjaa teloitusvideoiden äärelle ja lataa Bankerin saastuttamalleen koneelle. Delf.ACC leviää "sadan.exe"-nimisessä liitteessä.

"Saddam.morto.scr" -nimisessä sähköpostiviestin liitteessä levitettävä Banload.BSX-trojialainen ei tyydy yhteen Bankeriin, vaan se lataa koneelle kolme Banker-varianttia.

F-Securen mukaan päivitetty virustorjuntaohjelma tunnistaa kyseiset troijalaiset. Yhtiöllä ei ole tietoa siitä, miten laajalti niitä on levitetty.

Saddamia on ennenkin käytetty haittaohjelman houkuttimena. Pari vuotta sitten Bobax-niminen mato levisi Saddamin siivellä.

<http://www.digitoday.fi/tietoturva/2007/01/09/saddamin-hirttajaisilla-puffataan-haittaohjelmia/2007531/66>