

## Salasanoja varastava troijalainen leviää

31.5.2006 07:44 — Marko Mannila

Salasanoja varastava Sinowal- troijalainen houkuttelee uhrejaan liitteellä, jonka virus sanoo olevan Windows-päivitys.

Trojan-PSW.Win32.Sinowal.u -troijalainen on Kaspersky-turvayhtiön mukaan uuden sukupolven virus. Kun uhri vierailee verkkosivulla eikä selainta ole asianmukaisesti päivitetty, haittaohjelma asentaa itsensä tietokoneelle ja etsii käyttäjätunnuksia ja salasanoja eurooppalaisiin pankkeihin.

Sinowal-trojialainen pystyy asentamaan html-koodin, joka tuo ruudulle pop-up-ikkunan, vaikka ssl-salaus olisi käytössä pankin verkkosivulla. Virus on ohjelmoitu reagoimaan tiettyjen pankkien sivuihin.

Trojialainen on edistynyt, sillä se lähettää tiedot heti krakkerin palvelimelle, eikä varastoi niitä uhrin tietokoneelle. Se pystyy myös asentamaan päivityksiä.

Viimeaikaisissa viesteissä on .de-sähköpostiosoite. Sinowal ei tartu istestään, vaan se yrittää harhauttaa uhrin asentamaan haittaohjelman. Saksankielinen viesti väittää, että uusi virus on liikkeellä, ja että uhrin tulisi ladata mukana tuleva tiedosto suojellakseen järjestelmäänsä.

- Sinowal-perhe on koodattu Venäjällä, sillä koodi sisältää venäjää, **Roel Schouwenberg** Kasperskyltä totesi IDG-uutispalvelulle.

[Kasperskyn Sinowal.u -tietosivu](#)

<http://www.digitoday.fi/tietoturva/2006/05/31/salasanoja-varastava-trojialainen-leviaa/20067888/66>