

S-Files: Trust No One

7.5.2007 13:32 — Tuomas Karvonen

Symantec kertoo löytäneensä mielenkiintoisen troijalaisen nimeltä Kardphisher. Se ei ole kovin tekninen, vaan pikemminkin perinteinen social-engineering -hyökkäys, jolla käyttäjä yritetään juksata luovuttamaan luottokorttitietonsa. Erottavana tekijänä on kuitenkin toteutuksen yksityiskohtaisuus.

[Tietoturvyhtiön mukaan](#) troijalaisen laatija on paiskinut kovasti töitä tehdäkseen huijauksestaan mahdollisimman uskottavan. Kun tietokone käynnistetään ensi kertaa troijalaisen asentumisen jälkeen, näytölle ilmestyy ilmoitus Microsoftin piratismikontrollista, jossa väitetään, että joku toinen on aktivoinut käyttäjän Windows XP:n. Käyttäjää pyydetään siksi aktivoimaan Windowsinsa uudelleen.

Käyttäjä voi valita joko "kyllä" tai "ei". Jos hän valitsee jälkimmäisen, kone sulkeutuu. Myöntävästi vastaava saa ruudulleen kaavakkeen, joka vaatii muun muassa luottokorttitietoja Windows XP:n aktivoimiseksi.

Graafiseen ulkoasuun on selvästi kiinnitetty huomiota, ja kieltävä vastaus aiheuttaa siis loputtoman kierteen koneen sulkeutumisen ja käynnistämisen välillä.

Symantec katsookin troijalaisen olevan tärkeä opetus kaikille - tv-sarja X-Filesin slogania mukaillen yhtiö sanoo, että "Trust No One" eli älä luota kehenkään.

<http://www.digitoday.fi/tietoturva/2007/05/07/s-files-trust-no-one/200711057/66>