

Myrskytroijalainen mellasti viime viikolla

16.4.2007 17:10 — Antti Kirves

Tietoturvayhtiö Postinin mukaan Myrskytroijalaisena tunnettu haittaohjelma nosti viime viikolla roskapostin määrän maailmalla 60-kertaiseksi normaalilanteeseen verrattuna. Määrä on yhtiön mukaan suurin vuoteen.

Myrskytroijalainen hyökkäsi viime viikolla kahdessa vaiheessa. Haittaohjelma aloitti tekaistuilla lemmenviesteillä. Liitteet, joissa haittaohjelma levisi, olivat nimeltään Love Card.exe, Love Postcard.exe, Greeting Card.exe tai Postcard.exe.

Hyökkäyksen toisessa vaiheessa troijalainen levitti viestiä, joka varoitti englanniksi haittaohjelman leviämisestä. Viestien otsikoita olivat esimerkiksi "Worm Alert!", "Worm Detected", "Spyware Detected" ja "Virus Activity Detected".

Viestin vastaanottaja yritettiin houkutella avaamaan zip-pakatussa liitteessä oleva haittaohjelma. Viestissä uskoteltiin, että vastaanottajan tietokone on saastunut ja että liitteessä olisi haittaohjelman poistava korjauspäivitys.

Postinin mukaan tarkoitus oli luoda hempeillä rakkausviesteillä ensin kuva leviävästä haittaohjelmasta. Toisen vaiheen varoituksilla hyökkääjät halusivat hyödyntää ensimmäisen luomaa epävarmuutta.

[F-Secure](#) tunnistaa Postinin Myrskytroijalaisena pitämän haittaohjelman Zhelatin-nimiseksi sähköpostimadoksi.

Myrskytroijalaisena tai Storm Worm-, Storm Trojan-, Small.DAM- ja Peacomm-nimillä tunnettu haittaohjelma levisi Windows-ympäristössä alun perin uutisotsikoiksi naamioituina sähköpostiviesteinä. Houkuttimena käytettiin Euroopassa tuolloin riehuneita myrskyjä.

Sittemmin otsikoita on tullut lisää. Houkuttimina on käytetty muun muassa väitteitä Kuuban johtajan **Fidel Castron**, Venäjän presidentin **Vladimir Putinin** ja Venezuelan presidentin **Hugo Chavezin** kuolemista. Yhden troijalaisversion mukaan Saddam Hussein puolestaan on sittenkin elossa.

Symantecin mukaan viikko sitten levinnyt haittaohjelma, joka käytti houkuttimenaan tekaistua Yhdysvaltain ja Iranin välistä sotaa, oli myös Myrskytroijalaisen variantteja. F-Secure luokittelee tämänkin haittaohjelman [Zhelatiniksi](#).

Virustorjuntaohjelmat tunnistavat kyseiset haittaohjelmat.

<http://www.digitoday.fi/tietoturva/2007/04/16/myrskytroijalainen-mellasti-viime-viikolla/20079196/66>