

ISS etsii virustorjunnan aukkoja

17.2.2005 12:49 — Jaakko Kuivalainen

Asiantuntijat uskovat, että Symantecin ja F-Securen virustorjuntaohjelmista löytyneet haavoittuvuudet saanevat lähiaikoina seuraa muiden valmistajien ohjelmien tietoturva-aukoista.

- Molemmat tietoturva-aukot löysi tietoturvaohjelmia valmistava Internet Security Systems eli ISS. Näyttäisi siltä, että ISS testaa järjestelmällisesti ainakin virustorjuntaohjelmistojen turvallisuutta, sanoo Viestintäviraston tietoturvaryhmän CERT-FI:n tietoturva-asiantuntija **Johanna Kinnari**.

Uusia virustorjuntaohjelmien tietoturva-aukkoja ennusti myös SANS-instituutin Internet Storm Center -keskuksen päivystäjä **Matt Fearnow** kommentoidessaan Symantecin ja F-Securen varoituksia.

- Uskoisin, että ISS käy läpi erilaisia haavoittuvuuksia kaikkien virustorjuntayhtiöiden tuotteista. Kerromme lisää, kun tietoa on saatavilla, Fearnow kirjoitti ISC:n sivuilla viime viikolla. Haavoittuvuudet johtuvat ohjelmoinnin tai ohjelmoinnin suunnittelun virheistä.

Mediahuomio taattua

Johanna Kinnarin mukaan ainakaan julkisuudesta ei ole pulaa tietoturvaohjelmistojen aukkojen löytäjälle. Oikein rakennettu tietoturva ei kuitenkaan kaadu virustorjunnan haavoittuvuuksiin.

- Tietoturvaohjelmistot ovat ohjelmistoja siinä missä muutkin. Onhan niiden aukot vakava asia, koska tietoturvaohjelmistojen tarkoitus on juuri suojata järjestelmää. Tietojärjestelmien turvallisuudessa ei kuitenkaan voida nojata pelkästään tietoturvaohjelmistojen antamaan turvallisuuteen, Kinnari sanoo.

Virustorjunnan reikiä hakkeritapahtumassa

Haavoittuvuudet on merkitty ISS:n tiedotteissa yhtiön X-Force-ryhmässä työskentelevän haavoittuvuustutkijan **Alex Wheelerin** nimiin.

Wheeler esiintyy yhdessä kollegansa **Neil Mehtan** kanssa Blackhat Europe -hackeritapahtumassa ensi kuun lopussa. Haavoittuvuustutkijoiden esityksen aiheena ovat hyökkäykset virustorjuntaa vastaan - "Owning Antivirus".

Wheeler ja Mehta kyselevät provosoivasti esityksen kuvauksessa, auttaako virustorjunta murtautujia sen sijaan, että se suojaisi ihmisiä niiltä.

Esityksen kuvauksessa Wheelerin kerrotaan löytäneen haavoittuvuuksia useiden virustorjuntayhtiöiden tuotteista. Lähiaikoina päivitystyötä ovat joutuneet virustorjujista tekemään kuitenkin vain F-Secure ja Symantec.

ISS pistää vahingon kiertämään

Wheelerin työnantaja ISS on ajoittain kritisoinut tuotemerkkinoinnissaan perinteistä virustorjuntaa jälkijättöiseksi. Yhtiön omat tuotteet perustuvat tunkeutumisen havainnointiin ja tunnistamiseen, mikä osaltaan selittää yhtiön kiinnostusta virustorjunnan heikkouksiin.

Muiden tietoturvyhtiöiden koodin tarkistusta on saattanut innoittaa myös yhtiön omat kokemukset haavoittuvista tietoturvaohjelmistoista. Kilpaileva tietoturvyhtiö löysi viime maaliskuussa ISS:n tuotteista aukon, jonka hyödyntämismenetelmä päätyi muutamassa päivässä matokoodiin.

Witty-verkkomato levisi muutamassa tunnissa tuhansiin päivittämättömiin koneisiin. Witty oli nopean ilmestymisensä lisäksi harvinainen verkkomato myös siksi, että se sisälsi tehokkaan tuhorutiinin. Arvioiden mukaan mato saastutti ja tuhosi 10 000-40 000 tietokonetta.

<http://www.digitoday.fi/tietoturva/2005/02/17/iss-etsii-virustorjunnan-aukkoja/20058253/66>