

Lehdistötiedote

F-Secure Oyj
PL 24
FIN-02231 HELSINKI
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



JULKAISTAVISSA 18.9.2001

Uusi monimutkainen Nimda-mato leviää nopeasti internetissä

F-Secure Oyj varoittaa uudesta nopeasti leviävästä verkkomadosta. Nimda leviää sekä sähköpostissa että www-palvelimien turva-aukkojen kautta. Nimda on ensimmäinen mato, joka yhdistää nämä toiminnot.

Mato tunketuu koneeseen joko siten, että käyttäjä avaa saastuneen README.EXE-nimisen sähköpostiliitteen tai siten, että käyttäjä surffaa internetissä ja lataa sieltä README.EXE-nimisen tiedoston. Tämän jälkeen mato leviää kahdella tavalla. Ensimmäinen lähettää sähköpostiviestejä koneesta löytämiinsä osoitteisiin ja sen jälkeen hakee internetistä www-palvelimia, joissa on turva-aukkoja. Nimda käyttää myös tekniikoita, joiden ansiosta madon liitetiedosto saattaa käynnistyä automaattisesti jo sähköpostia avattaessa.

"Tämän madon kehittämiseen on panostettu", sanoo Mikko Hyppönen, F-Secure Oyj:n virustorjuntayksikön päällikkö. "Nimda leviää nopeasti, koska siinä yhdistyy monta eri toimintoa".

Matoa tutkitaan edelleen, koska se näyttää esimerkiksi jakavan paikallisia kiintolevyjä vapaaseen käyttöön koko internetille, ja leviää lähiverkkojen sisällä levyjakojen kautta. Sen lisäksi Nimda aiheuttaa valtavasti verkkoliikennettä.

Nimda on ensimmäinen mato, joka muuttaa www-palvelimien toimintaa niin, että ne alkavat levittää virusta omille käyttäjilleen. Lisäksi se käyttää loppukäyttäjien koneita etsimään satunnaisista osoitteista mahdollisia tartutettavia www-palvelimia. Tämä tekniikka mahdollistaa Nimdan pääsyn palomuurien takana sijaitseviin intranetsivustoihin, joihin esimerkiksi Code Red -madot eivät yleensä päässeet.

Nimda sisältää tekstin: "Copyright 2001 R.P.China".

Nimda toimii ainostaan Microsoft Windows -järjestelmien alla. Microsoftin viimeisimmät turvapäivitykset sulkevat madon käyttämät turva-aukot Outlook-sähköpostissa ja IIS web-palvelimessa.

F-Secure Anti-Virus -tuote löytää, pysäyttää ja poistaa Nimda-madon. Madon tunnistus lisättiin 18.9.2001.

Teknisiä tietoja madosta: <http://www.f-secure.com/v-descs/nimda.shtml>.

F-Secure Oyj

F-Secure Oyj on suomalainen yritys, joka toimittaa hajautettuja, keskitetysti hallittavia tietoturvaratkaisuja. F-Securen tuotevalikoima sisältää palkittuja, keskitetysti hallittuja virustentorjunta-, tiedosto- ja verkkosalaus- sekä hajautettuja palomuurituotteita yritysten kaikille keskeisille laitealustoille työasemista, verkkolaitteisiin ja palvelimista langattomiin taskutietokoneisiin.

F-Securen tuotteet sopivat tietoturvan toimittamiseen myös palveluna (Security as a Service, SaaS). Palvelu tarjoaa luotettavan, aina toimivan ja ajanmukaisen tietoturvan hajautetulle käyttäjäkunnalle. F-Securen tuotteet ja ratkaisut voidaan toimittaa asiakkaiden omien IT-osastojen tai palveluntarjoajien kautta. Ratkaisujen avulla turvakäytäntöpohjainen tietoturva ja tarvittavat hälytykset saadaan kaikkiin laitteisiin, joilla tietoa luodaan ja tallennetaan tai joilta tietoa haetaan. Vuonna 1988 perustettu F-Secure Oyj on noteerattu Helsingin pörssissä. Yhtiön pääkonttori on Helsingissä. Yhtiöllä on lisäksi toimistoja eri puolilla maailmaa.

Lisätietoja:

Mikko Hyppönen, Tutkimuspäällikkö
F-Secure Oyj
Puh. 09 2520 5513
Fax 09 2520 5001
E-mail: Mikko.Hypponen@F-Secure.com

<http://www.F-Secure.com>