

Lehdistötiedote

F-Secure Oyj
PL 24
FIN-00181 HELSINKI
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
<http://www.F-Secure.com>



JULKAISTAVISSA 31.10.2001

F-Secure varoittaa uudesta Nimda.E -verkkomadosta

F-Secure Oyj varoittaa uudesta Nimda-verkkomadon versiosta joka tunnetaan nimellä Nimda.E. Nimda.E on luultavasti saman tekijän kirjoittama kuin alkuperäinen Nimda (Nimda.A).

Käytännössä Nimda.E –mato on uudelleen kirjoitettu versio Nimda.A:sta. Tästä syystä suurin osa virustentorjuntatuotteista jotka pystyivät tuhoamaan Nimda.A:n, eivät pysty poistamaan uutta Nimdaa ilman päivityksiä. Suurin osa tiedostonimistä, joita ensimmäinen Nimda käytti on nimetty uudelleen. Esimerkiksi alkuperäisen Nimdan käyttämä tiedosto README.EXE on nyt SAMPLE.EXE -niminen. Mato sisältää useita koodimuutoksia. Toiset näistä on luultavasti tehty korjaamaan ohjelmointivirheitä alkuperäisessä madossa, toiset ovat luoneet lisää vikoja.

Näyttää siltä, että Nimdan kirjoittaja halusi ensimmäisen version tulevan tunnetuksi "Concept"-nimellä. Kun tämä ei onnistunut, hän on lisännyt uuteen matoon piilotetun tekijänoikeustekstin: "Concept Virus(CV) V.6, Copyright(C)2001, (This's CV, No Nimda.)"

Muuten Nimda.E on toiminnaltaan samanlainen neljällä eri tavalla leviävällä verkkomato kuin Nimda.A. Mato leviää saastuttamalla tiedostoja, välittämällä sähköpostia koneesta löytämiinsä osoitteisiin, käyttämällä hyväkseen www-palvelimien turva-aukkoja ja lähiverkkojen levyjakoja.

Kun Nimda.A puhkesi syyskuussa 2001, se saastutti yli 2 miljoonaa konetta ympäri maailmaa. Sen on arvioitu olevan yksi viidestä laajimmin levinneestä viruksesta kautta aikojen. Nimda.A aiheutti suurimmat tuhot luomalla valtavan määrän verkkoliikennettä yritysten sisäisissä verkoissa.

“Nimda.E ei leviä yhtä laajalti kuin alkuperäinen Nimda.A, koska Nimda.A:n saastuttamat internet-palvelimet on suojattu ja Nimda on nyt tunnettu”, toteaa Mikko Hyppönen, Virustentorjuntayksikön päällikkö F-Securesta.”

Nimda.A levisi tehokkaimmin www-palvelinten välityksellä käyttäen hyväkseen Microsoftin IIS-palvelinten turva-aukkoja. www-palvelin saattaa olla alttiina Nimda.E:lle vaikka viimeisimmät virustentorjuntaversiot ovat käytössä. Nimda.E käyttää takaportteja, joita muun muassa Code Red –mato asensi päästäkseen internet-palvelimille. Jos näitä takaportteja ei ole erikseen poistettu, palvelin saattaa saastua uudelleen.

Mato leviää useiden tunnetujen turva-aukkojen välityksellä. Yhden turva-aukon avulla sähköpostiliite aktivoituu automaattisesti, kun sähköpostiliite luetaan.

Tietokoneen käyttäjiä neuvotaan olemaan avaamatta SAMPLE.EXE –nimisiä sähköpostiliitteitä, käyttämään viimeisimpiä turvapäivityksiä ja virustentorjuntaohjelmia.

F-Secure Anti-Virus löytää ja pysäyttää Nimda.E -madon. Madon tunnistus lisättiin 31.10.2001.

F-Secure on saanut ilmoituksia Nimda.E -madosta Yhdysvalloista, Kiinasta, Ruotsista, Norjasta, Suomesta, Ranskasta ja Saksasta.

Teknisiä tietoja madosta: http://www.f-secure.com/v-descs/nimda_e.shtml

Lisätietoja:

Mikael Albrecht, Tuotepäällikkö
F-Secure Oyj
PL 24
FIN-00181 Helsinki
Puh. (09) 2520 5640
Fax (09) 2520 0700
Gsm +358 40 550 9349
Sähköposti: Mikael.Albrecht@F-Secure.com

[Http://www.F-Secure.com](http://www.F-Secure.com)