



Media Release

New complex and widespread worm located

Zurich - September 19, 2001 - F-Secure Corporation (HEX:FSC) is alerting computer users worldwide about a new, rapidly spreading e-mail worm. Known as "Nimda" this worm combines functionalities of a mass mailer and a web worm. The worm spreads through both e-mail attachments and by attacking vulnerable web servers in the net.

End-users can get infected by either opening an e-mail attachment called README.EXE or by surfing on an infected web site, which might offer the user to download README.EXE. After the end-user has executed the file, the worm will continue to spread in two different ways. First it will send itself out via e-mails directed to addresses found from users e-mail inbox. Secondly it will start to scan random internet addresses trying to locate vulnerable IIS web servers.

The worm uses several known security holes to spread. One of them enables the e-mail attachment to execute automatically when the e-mail attachment is read on some systems.

"Somebody has really put effort into this one", comments Mikko Hypponen, manager of Anti-Virus Research at F-Secure Corporation. "This worm is spreading fast mainly because it's combining many of the earlier attacks into one."

The worm is still under investigation. For example, it seems to open local network shares and try to propagate its code further via existing LAN shares. In addition, Nimda does generate massive amounts of internet traffic.

Nimda is the first worm to modify existing web sites to start offering infected files for download. Also it is the first worm to use normal end user machines to scan for vulnerable web sites. This technique enables Nimda to easily reach intranet web sites located behind firewalls - something worms such as Code Red couldn't directly do.

The worm contains this string: "Copyright 2001 R.P.China".

Latest security patches from Microsoft for Outlook and IIS web server will close the vulnerabilities the worm is using.

F-Secure Anti-Virus is capable of detecting and stopping the Nimda virus.

The detection of this virus was added on September 18.

Technical details as well as a screenshot of the worm are posted at:

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



About F-Secure Corporation

F-Secure Corporation is a leading provider of centrally managed security for today's mobile, wireless enterprise. The company offers a full range of award-winning, integrated anti-virus, file encryption, distributed firewall and VPN solutions for workstations, servers, gateways and mobile devices.

F-Secure products are uniquely suited for delivery of Security as a Service(tm) which provides invisible, reliable, always-on, and up-to-date security for the most widely distributed user base. Whether provided by corporate IT or delivered by service providers, F-Secure solutions extend policy-based security and instant alerts to all devices where information is created, stored or accessed. Founded in 1988, F-Secure Corporation is listed on the Helsinki Stock Exchange [HEX: FSC]. The company is headquartered in Espoo, Finland with North American headquarters in San Jose, California, as well as offices worldwide.

For more information, please contact:

F-Secure Corporation GmbH
Travis Witteveen
Maximilianstr. 35a
80539 München

Tel.: +49 (0)89 24218-425
Fax: +49 (0)89 24218-200
travis.witteveen@f-secure.com
www.f-secure.com

consul&ad
resulting by consulting
Rafael Cruz
P.O.Box
CH-8640 Rapperswil

Tel.: +41 (0)55 211 04 40
Tel.: +41 (0)55 211 04 41
rafael.cruz@consulad.ch
www.consulad.ch