Eset's Heuristically Identifies W32/Zafi.D, W32/Mydoom.AJ and Offers Free Cleaners

Submitted by: Chemistry TM
Friday, 17 December 2004

NOD32 Antivirus Software Customers Protected Without Updating Signatures

17th December 2004 – Eset, a global security software solutions company providing next generation virus protection, today announced that the company's advanced heuristics detected a variant of the Zafi virus family, named W32/Zafi.D. Eset is providing a free cleaner for infected enterprises and consumers not protected by its NOD32 antivirus software.

The W32/Zafi.D worm is spreading rapidly via email, and can also spread across networked machines; the worm was first detected early this morning by Eset's Virus-Radar at http://www.virus-radar.com which uses NOD32's advanced heuristics technology.

One reason for the early success of W32/Zafi.D may be that it includes a short Christmas greeting, in one of fifteen different languages, and purports to contain a greeting card. The language is selected on the basis of the recipients' top level domain, for example .de addresses will receive the message in German, and other languages include English, French, Spanish and Italian. The combination of the time of release in the holiday season, and the targeted message in the recipients own language, is likely to greatly increase the success of this worm. Earlier in the year, W32/Zafi.B became one of the most successful viruses of all time.

A free cleaner is available for download on Eset's web site at
http://www.nod32.it/cgi-bin/mapdl.pl?tool=ZafiD
This will remove the virus from any infected PC.

Later this morning, a minor variant of the MyDoom virus was also detected on the Virus-Radar, MyDoom.AJ, which also spreads via email. Some companies are calling this worm W32/Atak.g

Eset's NOD 32 detected the new variant and backdoor utilizing the company's unique advanced heuristics technology, which identifies the newest malware the instant it starts spreading "in the wild," providing immediate protection without the need for signatures and updates. Eset's advanced heuristics is based on complementary algorithms that analyze file structure and simulate file execution through virtual PC technology to determine potentially suspicious activity with only minimal system resources. As a result, NOD32 consistently identifies more "in the wild" viruses without generating false positives, than any other anti-virus vendor.

# # #

Notes to Editors
About Eset

Eset is a privately held software development and research company with offices in San Diego, London, Prague and Bratislava. Founded in 1992, Eset has focused on developing innovative antivirus software solutions. NOD32 has evolved from that development process to be consistently rated as one of the best anti virus products, holding more Virus Bulletin 100% Awards than any other product available. For more information, visit www.nod32.com.

For more information, please contact:
Paul Brook
Aspect Systems
Tel: 0800 138 0802
URL: www.nod32uk.com

Melissa Geddes
Worth PR
Tel: 020 8439 8200
URL: www.worthcommunications.com