ESET's NOD32 Detects Sober.P Worm

Submitted by: Chemistry TM
Tuesday, 3 May 2005

NOD32 uses ThreatSenseT technology to provide immediate protection from infection without having to wait for an updated signature

3rd May, 2005 – ESET, a global security software solutions company providing next-generation virus protection, today announced that the company's flagship product, NOD32 antivirus, detected a new variant of the Sober worm family-Win32/Sober.P. Over six thousand cases of detection have been reported so far, and infection continues to spread rapidly via e-mail. The worm was first detected early on May 2nd by ESET's Virus-Radar at http://www.virusradar.com, which uses NOD32's ThreatSense technology to detect malware in real-time by analyzing code behavior.

Sober.P uses its own SMTP engine to proliferate via email and create outgoing messages from a spoofed sender's address that may use the words "admin," "info," "postmaster," and "Web master." Subject lines for these infected emails include "your password," "registration confirmation," "your email was blocked," and "mailing error."

If the email attachment is executed, Sober.P collects email addresses from local files and then uses the addresses to send itself out to other computers and also attempts to delete many files on the system. Once a computer is infected the virus locks the files in the system's memory so that they cannot be easily detected or removed by antivirus products. For this reason, real-time detection even before the creation of a new signature update is crucial. Sober.P also seeks and destroys files in the registry that can potentially disable many anti-virus files and firewall programs.

ESET is providing a free cleaner for infected systems not protected by its NOD32 antivirus software. The cleaner can be downloaded at http://www.nod32.it/cgi-bin/mapdl.pl?tool=Sober. It is important to note that the Sober.P virus cannot easily be removed manually from a system. Once a computer has been infected, only a special cleaner like that offered by ESET should be used to remove the worm.

ESET's Virus Radar (www.virusradar.com)-a real-time malware tracking tool, identified the new Sober variant using NOD32. Virus Radar provides site visitors with easy access to in-depth analysis of the latest viruses and processes approximately four million email messages per day to provide information such as the exact date a virus was first detected and its current detection rate. Virus Radar is also capable of tracking the progression of a single virus over a given period-in some instances from the earliest heuristic detection of a new virus to the point where the virus disappears.

- ends -

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, please contact:

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