» Eset Gives Antivirus a New NOD

NOD32 version 2.5's heuristics find intrusions that signature detection misses

BY CURTIS FRANKLIN JR.

good

- Antivirus, -worm, -spyware and -adware in one package
- Easy scheduling and scripting setup
- Heuristics and signature matching used for rapid malware response

bad

- Not part of a unified policy-enforcement suite
- Local system status and setup on multiple screens rather than a single view

Eset Software's NOD32 has long been known for its reliance on heuristics, rather than signatures, for detecting viruses. With version 2.5, Eset claims to have improved both management and function with significant changes to the product's core code. I found this new version a solid anti-malware offering, protecting against viruses, worms, spyware and adware.

The lightweight footprint of NOD32 belies its reach—it goes onto both desktops and laptops without placing a burden on storage or system performance. The intuitive management interface, designed to be used by both individuals and large organizations, can be accessed from a local GUI or the Eset Remote Administrator. In addition, Eset has built in minimal signatures for additional virus recognition, and a more complete signature set for protection against spyware and adware. Although NOD32 can be an effective individual anti-malware product, the central management capabilities of Remote Administrator make it of greater interest to network administrators.

Network Protection

Eset sent a beta of NOD32 2.0 to my office/lab in Gainesville, Fla. Installation included simple network configuration and server assignment work for updates. The update function may seem odd for a program that bases its performance on heuristics, but the combination of behavioral and signature detection is intended to make NOD32 faster and more complete in its malware detection. After installation, NOD32 reminds you that it needs to check for current signatures, installs them and then sets up its five modules for operation.

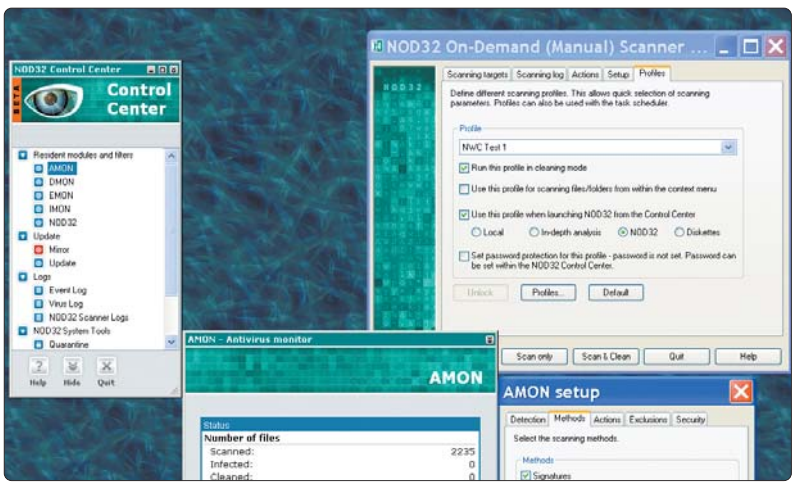
In my tests, I had NOD32 perform a complete scan on the hard disk of a workstation that until moments before NOD32's installation had been used for testing another antivirus package. On its first pass, the package flagged a file for containing "Probably unknown NewHeur_PE virus." After prompting me to leave, delete or rename the file, NOD32 asked if I would like to submit the file for analysis. This process is part of Eset's ThreatSense.Net, a system for gathering data on new malware and distributing information and data on protection and remediation. It turns out the file was infected, and its information was added to the ThreatSense database.

Profile Creation

A tree structure in the left-side pane provides access to details that show up in the right-side panel, where the profile-creation feature is found. You can set up profiles with different levels of protection based on time, user, location or other criteria, and fill the profile with information on scanning targets, actions taken on positive results, alert types and log entries generated during operation.

NOD32's spyware and adware real-time protection, new to 2.5, sends alerts when malware is detected or when any program that could take control of computer actions or data streams, such as a spambot, is found. I downloaded three files known to contain adware, and NOD32 successfully alerted on all three.

If your network uses programs such as Timbuktu for remote access and SpectorSoft for key-

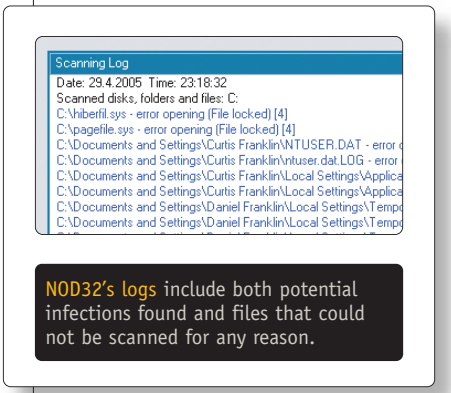


Execution parameters can be pushed back and forth between the administration console's automated protection policies and manual scans.

logging, you'll need to tell NOD32 to ignore that software, but the "ignore" list is easy to establish and keeps intrusions to a minimum.

Information Access

NOD32 offers configurable alerting, logging and reporting capabilities with both detected event and malware logs sent to administrators using SMTP or network messaging alerts. Additionally, logs can be configured to be stored on the local machine or forwarded to a central console. Remote administration consoles are similar to the individual computer-management screens, with a mirror function available to replicate report changes made by an administrator to the local user.



NOD32's logs include both potential infections found and files that could not be scanned for any reason.

Central management also includes automated updating of enterprise hosts from a central company server, as well as administrator-scheduled updates of signature rollouts and software updates. As with most enterprise antivirus software, local machine settings can be password-protected to prevent users from changing profiles without authorization.

Eset submitted NOD32 to Checkmark for certification evaluation, and Checkmark gave version 2.5 antivirus Level 1, Level 2, Trojan and Spyware Checkmarks. NOD32 is effective protection that's now easier to use and administer than previous versions, and a realistic anti-malware option for large and small organizations.

■ NOD32 2.5, starts at $39 for single-user license. Eset Software, (800) 343-3738. *www.eset.com*

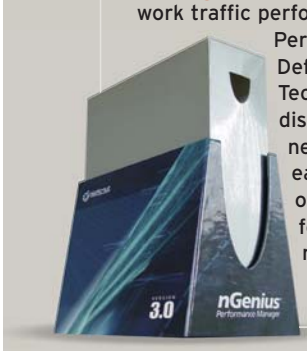
■ ID# *1612sp3*

Curtis Franklin Jr. is a senior technology editor for Network Computing. *He has been writing about the computer and network industries since 1985. Write to him at* cfranklin@nwc.com.

Quick Takes

Hitachi Global Storage Technologies Ultrastar 15K147 With the release of its Ultrastar 15K147, Hitachi Global Storage Technologies becomes the first to ship a 4GFC (4-Gbps Fibre Channel) hard drive, complete with SAS (Serial-Attached SCSI). Offering 36-GB, 73-GB or 147-GB capacity, the drive features 16-MB cache sizes to minimize command overhead and improve read/write response times. SAS supports data-transfer rates as high as 3 Gbps and up to 16,384 full-duplex, point-to-point connections for greater scalability. Fully backward-compatible with 1-Gbps and 2-Gbps hardware, the 4GFC interface allows for a data-transfer rate of up to 400 MBps half-duplex and 800 MBps full-duplex, per port. *Starts at $371 for 36 GB with SAS interface. Hitachi Global Storage Technologies, (800) 801-4618. www.hitachigst.com*

NetScout Systems nGenius Performance Manager 3.0 Promising more granular insight into network traffic performance, NetScout has unveiled nGenius Performance Manager 3.0, part of its High-Definition Performance Management Technology. The new version adds lets you display granular historical application and network performance metrics—as often as each minute, with corresponding one-second peak values. It offers enhancements for HTTP session reconstruction and replay, as well as playback of voice over IP calls, pattern matching and alarming, and direct connection to Ethernet segments. The nGenius Performance Manager keeps IT apprised of all applications, hosts and conversations on the network, including resource-draining P2P apps like Kazaa, Morpheus and Shareaza. *$50,000; upgrade to version 3.0 free. NetScout Systems, (800) 357-7666. www.netscout.com*



FullArmor IntelliPolicy for Clients 1.5 Designed to eliminate certain security vulnerabilities on Windows desktops, IntelliPolicy for Clients 1.5 lets you assign rights to applications such as Outlook and Word without giving users local administrative privileges. It also can change the local admin password on all enterprise machines at user-defined intervals, always keeping the new password encrypted. *Starts at $7 per managed machine. FullArmor, (800) 653-1783, (617) 457-8100. www.fullarmor.com*

Sandstorm Enterprises LANWatch 7.0 This software-based packet analyzer monitors traffic in real time, examining and verifying network protocols in both hexadecimal and formatted venues. Version 7.0 introduces DICOM (Digital Imaging and Communications in Medicine) support, including parsing for HIPAA compliance. *Starts at $695. Sandstorm Enterprises, (781) 333-3200. www.sandstorm.net*