Report on ESET NOD 32 Antivirus

CYBER SECURITY &
PRIVACY FOUNDATION

Software: NOD 32 Antivirus for Windows

Lab Setup:

Oracle Virtualbox v4.3.6 r91406

Operating System:

Machine 1: Windows 7 32-Bit.

Processor:

Intel(R) Core(TM)i5-4200U CPU @1.60GHz 2.30GHz

RAM:

512MB

Test Criteria:

ESET NOD32 has been constantly getting good ranks in the VB100 awards and is generally know as one of the best antivirus's in the market. We decided to run ESET NOD32 against a series of tests designed to stimulate a much more real scenario when it comes to malware and the Indian market.

We have set up the test in four levels.

Known Malware- Malware that is widely spread and is detect by a majority of antiviruses.

Known Malware (Variant) - Malware that is widely spread but has been crypted using a custom crypter (tried to make undetectable)

Unknown Malware- Malware samples that were developed exclusively for this test hence unknown to any antivirus vendor. The antivirus will only be able to stop such attacks using heuristics.

Pre Infected Machines-In this test the computers were infected with known malware before the anti-virus is installed. The reason for this test is that most of Indian computers are already infect with some sort of malware before an antivirus is installed and the this test hopes to test if the antivirus is able to remove all previous infections after it is installed.

Phishing Page: In this test, we open up a browser and browse to a URL that is considered to be a phishing page by most of the antiviruses, and whose entry is found in Phishtank database as well.

Installation:

General Installation with all the Terms and Agreement to be agreed.
(Found to be a light weight Antivirus)

Configuration:

General pre-built Configuration with NOD 32 Antivirus, and by enabling "Enabling Detection of Potentially Unwanted Applications" option.

Test Results (Known Malware):

Test 1: Detection of Known Virus

Successfully detected malware sample and quarantined it.

- ☑ Real-time
- ☑ Offline

Test 2: Detection of Known Keylogger

Successfully detected keylogger and quarantined it.

- ☑ Real-time
- ☑ Offline

Test 3: Detection of Known RAT (Remote Administration Tool)

Successfully detected RAT and quarantined it.

- ☑ Real-time
- ☑ Offline

Test Results (Known Malware -Variants):

Test 1: Detection of Known Virus-Variant

Successfully detected malware sample and quarantined it.

- ☑ Real-time
- ☑ Offline

Test 2: Detection of Known Keylogger-Variant

Successfully detected keylogger and quarantined it.

- ☑ Real-time
- ☑ Offline

Test 3: Detection of Known RAT (Remote Administration Tool) -Variant

Successfully detected RAT and quarantined it.

- ☑ Real-time
- ☑ Offline

Test Results (Unknown Malware-New Samples)

Test 1: Detection of Unknown Keylogger

Keylogger was able to run normally and capture keystrokes.

- ☒ Real-time
- ☒ Offline

Test 2: Detection of Unknown Downloader

Downloader was able to download the encrypted executable and decrypt it in temp and execute it without successfully.

- ☒ Real-time
- ☒ Offline

Pre-Infected Machines: The computer was infect by an assortment of malware before the anti-virus was installed .NOD32 was able to detect and remove 10/10 viruses that were installed in the system.

Conclusion:

Nod32 is a light weight product and does not reduce the system performance. After our testing, we observed that ESET NOD 32 is able to detect all the known malware samples and variants. It is also good at cleaning pre infected systems. The only place it was lacking is finding “Unknown” malware. It might be because ESET wanted to reduce the false positives made by the anti-virus and hence left the heuristics sensitivity low. Out of all the products tested by Cyber Security & Privacy Foundation, we found that ESET NOD 32 to be the Best Suited Antivirus for the Indian Environment.

The Overall Rating that we give ESET NOD-32 is:

“9/10”