Report on ESET NOD 32 Antivirus

CYBER SECURITY &
PRIVACY FOUNDATION

Software: NOD 32 Antivirus for Windows

Description of the Software as per the website:

AWARD-WINNING AND FAST ANTIVIRUS THAT'S EASY ON YOU

Enjoy your time online—protected with ESET NOD32 Antivirus.

Antivirus

Antispyware

Anti-Phishing

Gamer Mode

Exploit Blocker

Social Media Scanner

Autoscan of Removable Media

Advanced Memory Scanner

Portable Device Control

Cybersecurity Training

Lab Setup:

Oracle Virtualbox v4.3.6 r91406

Operating System:

Machine 1: Windows 7 32-Bit.

Machine 2: Windows XP 32-Bit. (Server)

Processor:

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

RAM:

512MB

Test Criteria:

This test is specifically done for Indian Environment as it is unique as 50% of the machine are pre infected machines. Though there are awards like Virus Bulletin 100, VB 100 concentrates on a product detecting 100% of all the viruses "In The Wild" (ITW). Many of the samples which are present in India do not make to ITW List. All the products of VB 100% award are checked for only detecting the virus, most of the products fail in Indian Environment because the machine is pre infected or the anti-virus is not able to clean them. We decided to test the products with the test criteria which is unique to the Indian Environment.

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 whose variant is been used for this test to see the level of detection of the variants.

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.

Report (Installation and configuration)

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 Details:

Test 1: Detection of Known Virus

File Name:

20130516_0328_Delivery_Information_ID-004588020234-Z31.exe

File Size: 35328 bytes

MD5: f57ce6b2b560e8f45abb43fa72a7883b

Detection Ratio: 42/54 (Virus Total) @ 2014-06-21 12:13:38 UTC

Result Found with NOD32:

Successfully detected the .exe file as a virus and quarantined it.

- ☑ Real-time
- ☑ Offline

We also tested these known samples and all of them were detected both Real-time and Offline.

RAT

FinFisher RAT

SHA 256:2ec6814e4bad0cb03db6e241aabdc5e59661fb580bd870bdb50a39f1748b1d14

xtreme_rat

SHA 256:f8024cab61c1a52d66c527601450974e5d894fe4243488786b8cc17e1f20dbdb

CyberGate

SHA 256:bfe22533c3fd67c7f3eb8c9243b866873065041de25c02bcca0e0059b44a2351

HTTP BOTNET

athena_http

SHA 256:3b9b0f564e8d7494d0389d9c11f62a7b621a337ebf3d520c033b1426ffbb8fa6

andromeda (2.6)

SHA 256:d8a632847964ab96592e473e335c9216a19e56705bda4d5686f51a7a55799293

VertexNet

SHA 256:954d2d1f35681c05f172f69e1005bf721468cd89a4962d2085195132534f2a92

IceIX Zbot (Variant of Zeus Bot)

SHA 256:be1fcba66173a9c38e6b087e241d99fa042e083492225b46087229aa8ea24707

betabot neurevt

SHA 256:057d73b1b7088f8ef4da7b2a962df13033548172c8462f6b47ba02411e49123b

BITCOIN MINER

Bitcoin Miner

SHA 256:12dfde650154ea2c7657701c2e6c3a8904d4aa9b958737037df2c8ecd8a94724

POS MALWARE

dexter pos

SHA 256:cae3cdaaa1ec224843e1c3efb78505b2e0781d70502bedff5715dc0e9b561785

Test 2: Detection of Known Keylogger

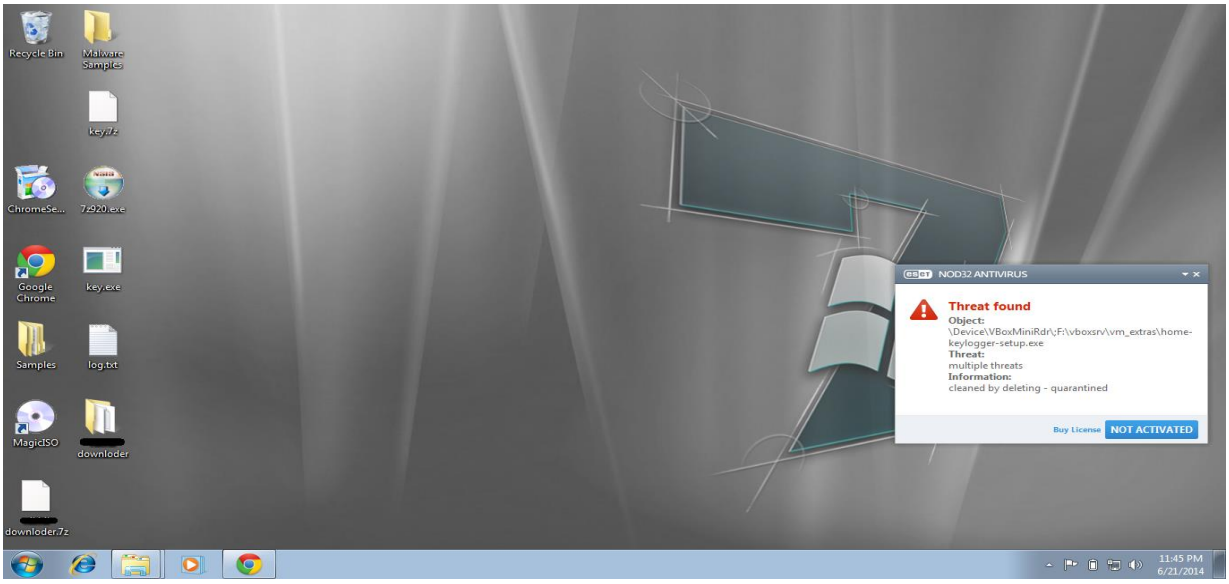
File Name: Home Keylogger.

File Size: 235 KB

MD5: d9e8ad04ba2c2075a3fd4544102cb9ac

Detection Ratio: 40 / 54 (Virus Total) @ 2014-06-16 00:32:58 UTC

Result Found with NOD32:



Detected the file to be a potential trojan and quarantined it automatically even without running the exe file.

- ☑ Real-time
- ☑ Offline

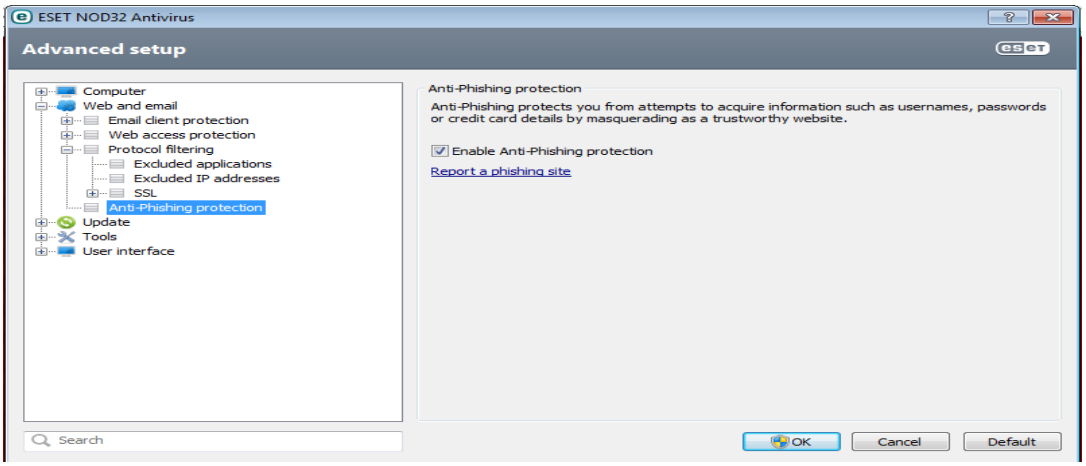
Test 3: Detection of Known Phishing Page:

Website URL:
http://www.videogameaudio.com/patches/Sichern/Sie/Ihre/Online-Banking-Konto/sparkasse.de/

Response Content SHA 256:
89398ceeff3ad80da551e1ec31ea44945d43c4f4a9ccd2619fec04466076fe03

Detection Ratio: 10 / 52 (Virus Total) @ 2014-06-22 03:19:16 UTC

Result Found with NOD32:



Did not detect the page to be a Phishing Page.

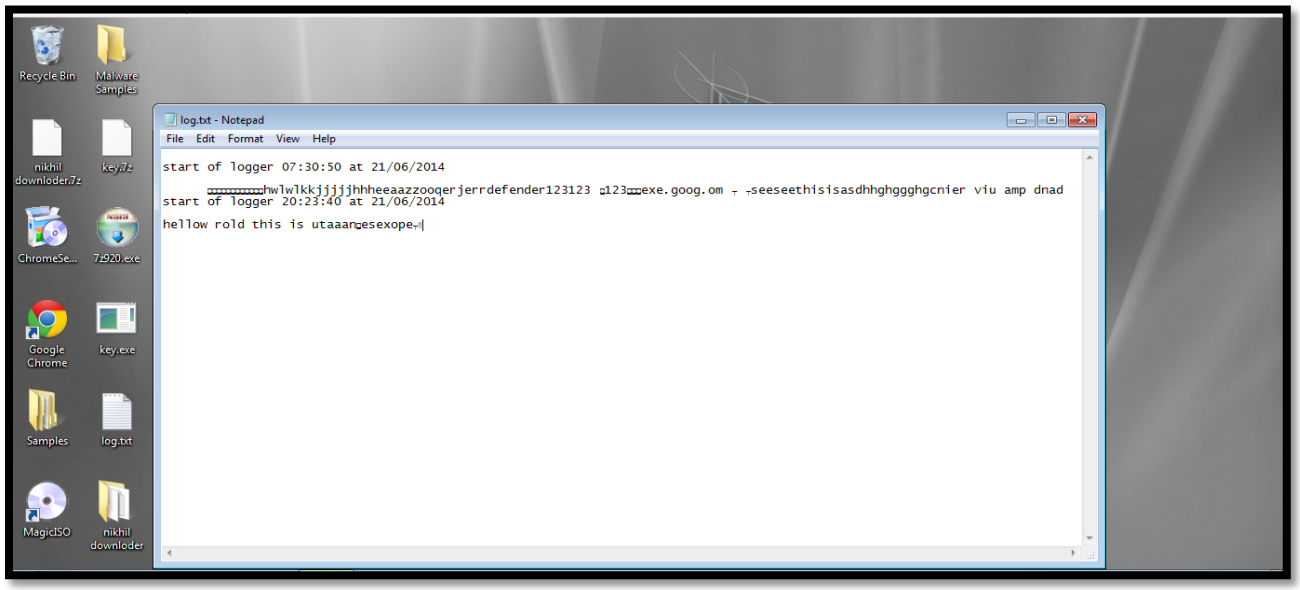
Test 4: Detection of an unknown Keylogger

File Name: key.exe

File Size: 858KB

Result Found with NOD32:

Was unsuccessful in detecting the keylogger on running the executable. Keylogger was able to run normally and capture keystrokes.



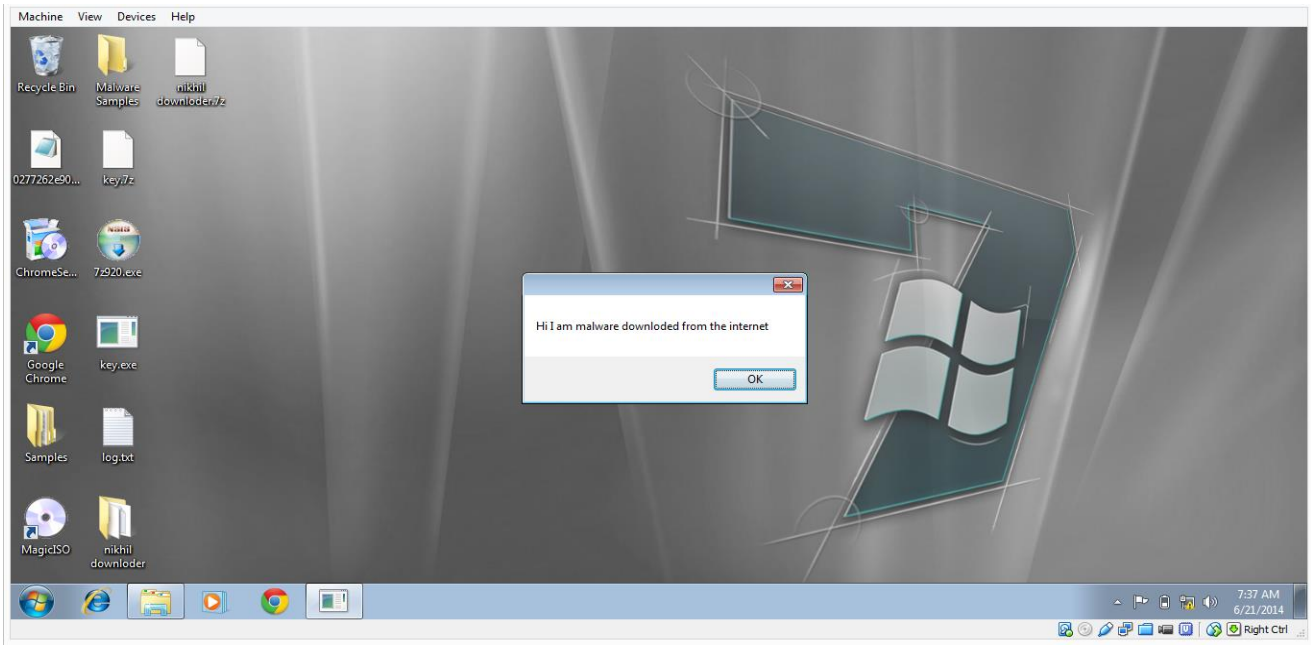
☒ Real-time
☒ Offline

Test 5: Detection of an unknown Malicious Downloader

File Name: downloader.exe

File Size: 846KB

Result Found with NOD 32:



Did not detect the downloader as Malicious. Even after the downloader connected to the remote server and was able to download the encrypted form of a test executable and decrypt it and run it.

☒ 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"