# Trend Micro Comparison Test: Protection

A test commissioned by Trend Micro and performed by AV-Test GmbH
Date of the report: August 23rd, 2016, last update: September 7th, 2016

## Executive Summary

In July 2016, AV-Test performed a comparative review of Trend Micro Virusbuster Versions 8, 10 and 11 against Norton Security 2016 and Microsoft Windows Security Essentials 4.9 to determine their exploit and ransomware prevention.

The malware test corpus for the exploit test consisted of 11 samples and for the ransomware test 15 malware samples. To perform the single test runs, a clean Windows 7 Professional (SP1, 64-bit) image was used on several identical PCs. On this image, the security software was installed and then the system is infected with the exploit or ransomware sample. Any detection by the security software was noted. Additionally the resulting state of the system was compared with the original state before the test in order to determine whether the attack was successfully blocked or not.

All three Trend Micro products and Norton Security delivered perfect results for the two protection tests. Only Windows Security Essentials 4.9 missed a few test cases.

## Overview

With the increasing number of threats that is being released and spreading through the Internet these days, the danger of getting infected is increasing as well. A few years back there were new viruses released every few days. This has grown to several thousand new threats per hour.

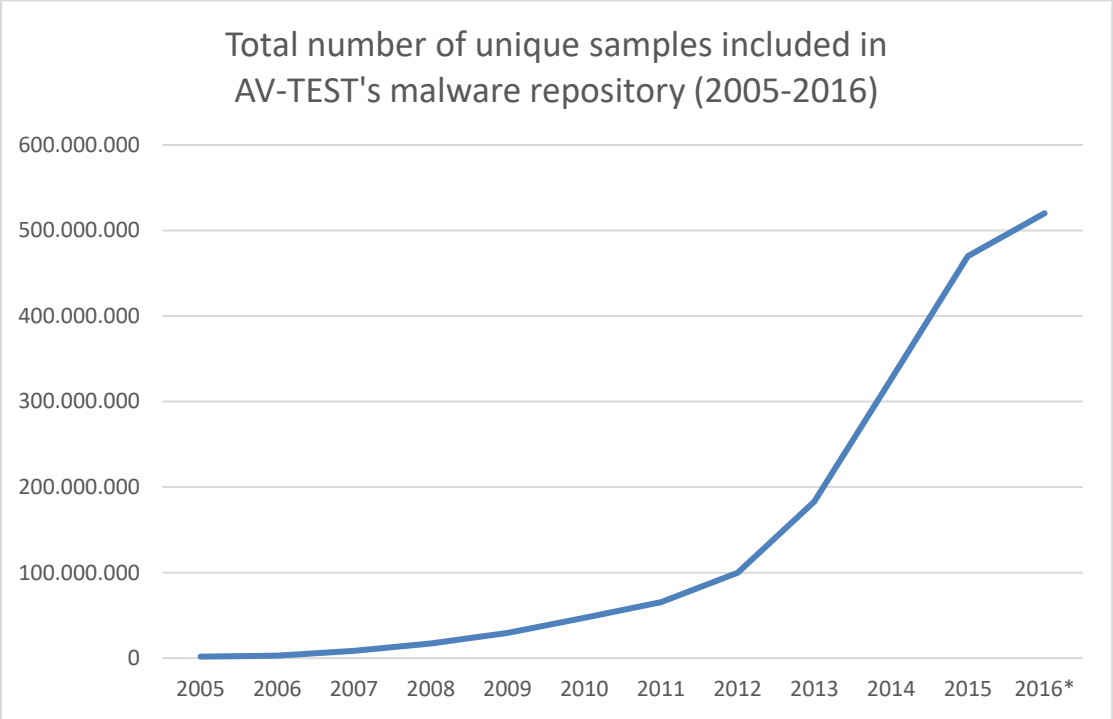


**Figure 1: New samples added per year**

In the year 2000, AV-Test received more than 170,000 new samples, and in 2013, the number of new samples grew to over 80,000,000 new samples. The numbers continue to grow in the year 2016. The growth of these numbers is displayed in Figure 1. AV-TEST currently has over 500 million malware samples in its database.

The volume of new samples that have to be processed by anti-malware vendors in order to protect their customers can create problems. It is not always possible to successfully protect a PC in time. It is possible that a PC can get infected, even if up-to-date anti-malware software is installed because signatures are provided only every few hours, which sometimes may be too late. Infections create financial loss, either because sensitive data is stolen or because the PC cannot be used for productive work anymore until the malware has completely removed from the system. And on the other hand more protection layers need more resources on the PC which can in turn influence the performance.

## Products Tested

The testing occurred in July 2016. AV-Test used the latest releases available at the time of the test of the following two products:

(1) Microsoft Windows Security Essentials 4.9
(2) Symantec Norton Security 2016
(3) Trend Micro Virusbuster 8
(4) Trend Micro Virusbuster 10
(5) Trend Micro Virusbuster 11

## Methodology and Scoring

### Platform

All tests have been performed on identical PCs equipped with the following hardware:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB Ram
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

The operating system was Windows 7 Professional with all patches that were available on August 1st 2016.

### General Approach

1. **Clean system for each sample**. The test systems should be restored to a clean state before being exposed to each malware sample.
2. **Physical Machines**. The test systems used should be actual physical machines. No Virtual Machines should be used.
3. **Product Cloud/Internet Connection**. The Internet should be available to all tested products that use the cloud as part of their protection strategy.
4. **Product Configuration**. All products were run with their default, out-of-the-box configuration.
5. **Sample Cloud/Internet Accessibility**. If the malware uses the cloud/Internet connection to reach other sites in order to download other files and infect the system, care should be taken to make sure that the cloud access is available to the malware sample in a **safe** way such that the testing network is not under the threat of getting infected.

### Exploit Test

**The exploit test has been performed according to the methodology explained below.**

The exploit samples were initialized on the system by using Fiddler.

The individual steps to run the test were as follows:

1. The exploit has been played back by Fiddler

2. If there were any notifications from the anti-virus software they have been noted and documented (e.g. by creating screenshots or storing report files)
    a. Furthermore it was checked whether the exploit was able to execute the payload
    b. If there was a detection by the product and no payload was executed then this was counted as successful block
    c. If there was no detection and the payload was executed then this was counted as miss
    d. In case there was no detection and no execution of the payload either, this indicated an error and the test has been repeated or the test case had to be removed from the results

The client has been reimaged and the next test starts with point 1 again.

## Ransomware Test

**The ransomware test has been performed according to the methodology explained below.**

The individual steps to run the test were as follows:

1. Copy the sample to the local disk and execute it
2. If there were any notifications from the anti-virus software they have been noted and documented (e.g. by creating screenshots or storing report files)
    a. Furthermore it was checked whether the malware was running
    b. If there was a detection by the product and no harm remains on the system then this was counted as successful block
    c. If there was also a detection but some dropped files are left on the system then it was counted as partial miss
    d. And finally if there was no detection and the malware is still active on the system then this was counted as miss

## Samples

The set contained 11 exploit samples and 15 ransomware samples that were able to infect Windows 7 (SP1, 64-bit).

## Test Results

### Exploit Test

The test shows how well the security solutions are capable of blocking exploit attacks. The following figure shows the overall score of the five tested solutions.

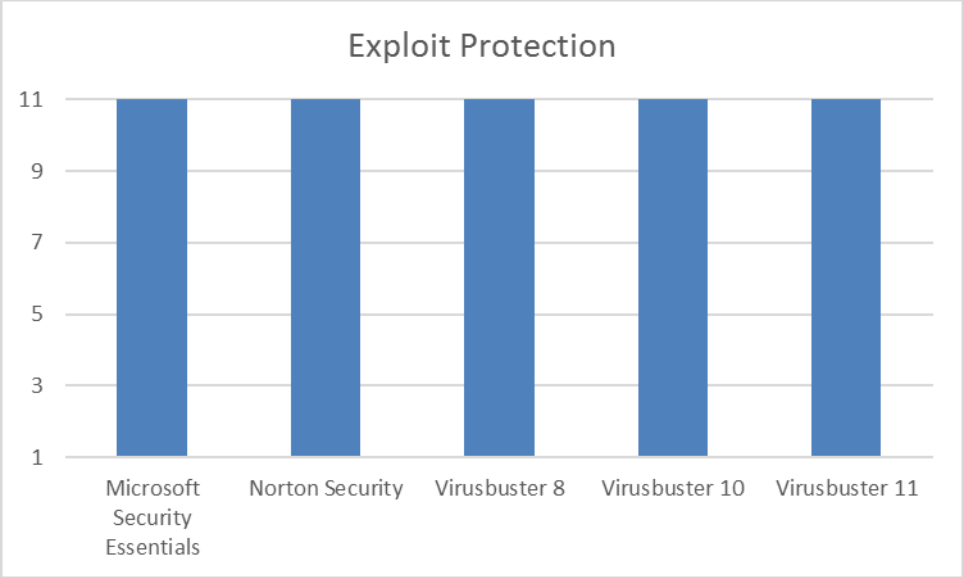


Figure 2: Exploit Protection

All products with one exception perform the test without problems and achieved the best possible score in the test blocking all attacks. Only Microsoft Security Essentials missed 4 attacks and blocked 7 of the 11 test cases in this setup.

### Ransomware Test

These kinds of attacks are becoming increasingly popular and it is important to protect the user against possible damage. The test figures out how the products scored against the latest infection waves of CryptoWall, CryptTesla and Locky.

Here all tested products scored perfectly and detected 15 of 15 tested samples and protected the user against harm.

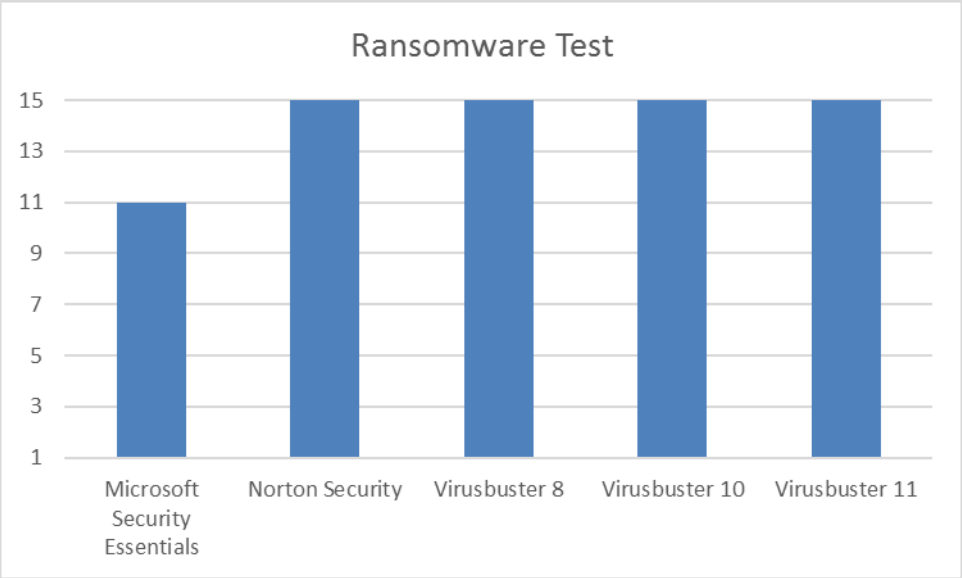


**Figure 3: Ransomware Detection**

# Appendix

## Version information of the tested software

| Developer, Distributor | Product name | Program version | Engine/ signature version |
|---|---|---|---|
| **Microsoft** | Microsoft Security Essentials 4.9 | 4.9.218.0 | 1.1.12902.0/1.225.1338.0 |
| **Symantec** | Norton Security | 22.7.0.76 | n/a |
| **Trend Micro** | Trend Micro Virusbuster 8 | 8.0.2064 | 9.850.1008/12.651.00 |
| **Trend Micro** | Trend Micro Virusbuster 10 | 10.0.1265 | 9.850.1008/12.645.00 |
| **Trend Micro** | Trend Micro Virusbuster 11 | 11.0.1102 | 9.895.1014/12.651.00 |

## List of used malware samples (Exploit and Ransomware)

| Exploit Samples |
|---|
| * 0x06-02-2016_WALTRIX_C606 |
| * 0x06-02-2016_WALTRIX_EFD2 |
| * 0x06-03-2016_WALTRIX_2186 |
| * 0x06-03-2016_WALTRIX_9781 |
| * 0x5-26-2016_WALTRIX_76E0 |
| * 0x5-30-2016_WALTRIX_3D85 |
| * 0x6_01_2016_WALTRIX_F590.tmp |
| * 0x06-07-2016_WALTRIX_rad39D95_NEUTRINO |
| * 0x06-08-2016_WALTRIX_NEUTRINO_2nd |
| * 0x06-09-2016_WALTRIX_NEUTRINO_v3 |
| * 0x06-10-2016_WALTRIX_NEUTRINO_v2 |

| Ransomware Samples (SHA 1) |
|---|
| * 0x11b7ce2d31a94d2458e190822c23c0ad80aa6232 |
| * 0x26d157032a151ba6101c8f5e225f62cb96059f45 |
| * 0x4f555ba23051f548b05b7516161621a2e3c5a164 |
| * 0x4fdc9b326537c83cf7148a69c9033d384082865e |
| * 0x6502eaaecc168dd58fd7efca671f15734e12f958 |
| * 0x68faef81d958f74450ff7b32794f41f5a8158e33 |
| * 0x920ba9c21b519ad7dfb9075c3860d85061cede15 |
| * 0xadce8cf4c31f1980c2b1d952a5a931d7c8dcdd8c |
| * 0xaf0167f963c88c56928fbafdf7ad281401b430d0 |
| * 0xce3e472198a424ec6e3608289ee5b4ff1f25d35b |
| * 0xd4a20d26742dbf1a62d4bd2ab8a294c92f7521e4 |
| * 0x b328ed982a59ce91ec999d912da594fb020a7719 |
| * 0xe2ebefed3b71950dfa553ac3b2053cd0aad664a9 |
| * 0x5775dcd46f09194ffdf32b9ba8f3d18189d04152 |
| * 0xb328ed982a59ce91ec999d912da594fb020a7719 |