virus

BULLETIN

Covering the global threat landscape

VB100 CERTIFICATION REPORT OCTOBER 2018

Martijn Grooten

INTRODUCTION

Virus Bulletin has been testing anti-virus (or anti-malware) products for more than two decades. A lot has changed during that time: threats have evolved greatly, as have the products. Yet, one thing has remained constant: people expect the security products they use to keep up with the latest malware.

The VB100 certification tests check whether products live up to that expectation, providing those that do with the VB100 stamp of approval.

This report details the performance of 28 of such products, from 27 different vendors, tested during September and October 2018, each of which achieved a VB100 award.

THE VB100 SET-UP

In the VB100 test, a copy of the product to be tested is installed on two platforms: *Windows 10* and *Windows 7*. On each platform, and at three different times in the test, the product is asked to scan both the latest version of the WildList[1] and a selection of clean files taken from *Virus Bulletin*'s own set of files belonging to widely used legitimate software.

A legitimate file that is blocked at least once is considered a false positive, while a WildList file that isn't blocked is considered a miss.

A product achieves a VB100 certification if:

  • No more than 0.5% of WildList samples are missed

and

  • No more than 0.01% of legitimate files are blocked

---

[1] The WildList is an extremely well-vetted set of malware recently observed in the wild by researchers: http://www.wildlist.org/.

For full details, we refer to the VB100 methodology on the *Virus Bulletin* website: https://www.virusbulletin.com/testing/vb100/vb100-methodology/vb100-methodology-ver1-1/. This test used version 1.1 of the VB100 methodology.

DIVERSITY TEST

The malware part of the VB100 certification test uses the WildList, a regularly updated list of extremely well-vetted malware samples, guaranteed to have been spotted in the wild multiple times. This makes them very suitable for a certification test like VB100.

The 'Diversity Test' looks at products' detection of another set of recent malware samples, to acknowledge the fact that products detect malware samples beyond a standard set of samples, and provides a measure of that detection.

PRODUCTS & RESULTS

Products were allowed to download updates during the course of the test. The version numbers listed in the results that follows refer to those at the start of the test.

AhnLab V3 Internet Security 9.0

Windows 7 version	9.0.49.2
Windows 10 version	9.0.49.2
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	N/A

vb 100 VIRUS
Oct 2018
virusbtn.com

vb

Arcabit AntiVirus

Windows 7 version	2018.09.04
Windows 10 version	2018.09.05
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.52%

vb 100 VIRUS
Oct 2018
virusbtn.com

Defenx Security Suite

Windows 7 version	15.1.0111
Windows 10 version	15.1.0111
WildList detection	100.0%
False positive rate	0.001%
Diversity test rate	98.33%

vb 100 VIRUS
Oct 2018
virusbtn.com

Avast Free Antivirus

Windows 7 version	18.6.2349
Windows 10 version	18.6.2349
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.64%

vb 100 VIRUS
Oct 2018
virusbtn.com

Emsisoft Anti-Malware

Windows 7 version	2018.8.0.9810
Windows 10 version	2018.8.0.8910
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.64%

vb 100 VIRUS
Oct 2018
virusbtn.com

AVG Internet Security

Windows 7 version	18.6.3066
Windows 10 version	18.6.3066
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.64%

vb 100 VIRUS
Oct 2018
virusbtn.com

eScan Internet Security Suite for Windows

Windows 7 version	14.0.1400.2029
Windows 10 version	14.0.1400.2029
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.88%

vb 100 VIRUS
Oct 2018
virusbtn.com

Cyren Command Anti-Malware

Windows 7 version	5.1.38
Windows 10 version	5.1.38
WildList detection	100.0%
False positive rate	0.003%
Diversity test rate	99.17%

vb 100 VIRUS
Oct 2018
virusbtn.com

ESET Internet Security

Windows 7 version	11.2.49.0
Windows 10 version	11.2.49.0
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

vb 100 VIRUS
Oct 2018
virusbtn.com

ESTsecurity ALYac

Windows 7 version	3.0.1.3
Windows 10 version	3.0.1.3
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.52%

Faronics Anti-Virus

Windows 7 version	4.12.3102.401
Windows 10 version	4.12.3102.401
WildList detection	100.0%
False positive rate	0.005%
Diversity test rate	100.00%

FireEye Endpoint Security

Windows 7 version	26.21.8
Windows 10 version	26.21.8
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.52%

Fortinet FortiClient

Windows 7 version	5.6.2.1117
Windows 10 version	5.6.2.1117
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.88%

G DATA Antivirus

Windows 7 version	25.4.0.4
Windows 10 version	25.4.0.4
WildList detection	100.0%
False positive rate	0.001%
Diversity test rate	100.00%

IKARUS anti.virus

Windows 7 version	2.19.9
Windows 10 version	2.16.20
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	97.98%

K7 Total Security

Windows 7 version	15.1.0342
Windows 10 version	15.1.0342
WildList detection	100.0%
False positive rate	0.001%
Diversity test rate	98.45%

Kaspersky Endpoint Security 10 for Windows

Windows 7 version	11.0.0.6499
Windows 10 version	11.0.0.6499
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.76%

NANO Antivirus

Windows 7 version	1.0.126.89281
Windows 10 version	1.0.126.89281
WildList detection	100.0%
False positive rate	0.001%
Diversity test rate	99.76%

TeamViewer ITbrain Anti-Malware

Windows 7 version	1.0.105328
Windows 10 version	1.0.105328
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.52%

Rising Security Cloud Client

Windows 7 version	3.0.0.82
Windows 10 version	3.0.0.82
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	77.86%

Tencent PC Manager

Windows 7 version	12.3.26577.901
Windows 10 version	12.3.26577.901
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

SafeCentral Security Suite

Windows 7 version	2.0.1430
Windows 10 version	2.0.1430
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Total Defense Premium

Windows 7 version	9.0.0.747
Windows 10 version	9.0.0.747
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.52%

TACHYON Endpoint Security

Windows 7 version	5.0.0.57
Windows 10 version	5.0.0.57
WildList detection	100.0%
False positive rate	0.006%
Diversity test rate	99.76%

TotalAV

Windows 7 version	4.6.19
Windows 10 version	4.9.36
WildList detection	99.9%
False positive rate	0.000%
Diversity test rate	N/A

VIPRE Advanced Security

Windows 7 version	10.1.4.33
Windows 10 version	10.3.4.2
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

VirIT eXplorer PRO

Windows 7 version	8.7.55
Windows 10 version	8.7.54
WildList detection	100.0%
False positive rate	0.001%
Diversity test rate	40.83%

Zemana EndPoint Security

Windows 7 version	6.6.1.36
Windows 10 version	6.6.1.36
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

APPENDIX 1: PRODUCTS NOT CERTIFIED

All tested products were certified.

APPENDIX 2: EXCLUDED PARTS

Technical and other issues can render the data we collect insufficient or otherwise unsuitable for accurate reporting. In such cases, the methodology allows us to discard the affected test part and record the event below. Two healthy test parts out of three are required for the certification to be issued.

- For *AhnLab V3 Internet Security 9.0*, the results of the Diversity Test were discarded due to technical issues.
- For *FireEye Endpoint Security*, the results of the second part of the certification test were discarded due to technical issues.
- For *TotalAV*, the results of the Diversity Test were discarded due to technical issues.

APPENDIX 3: SAMPLE SET SIZES

The WildList contained 1,580 samples. The set of clean files used for the false positive test contained 100,000 files, of which 29,235 were portable executable (PE) files. The set used for the Diversity Test contained 840 samples.