DECEMBER 2019

virus BULLETIN

Covering the global threat landscape

VB100 CERTIFICATION REPORT DECEMBER 2019

Martijn Grooten

The VB100 certification scheme provides a stamp of quality and competence for anti-malware products that satisfy a minimum standard of detecting malicious executables that have recently been seen in the wild, while blocking few to no legitimate programs.

This report details the VB100 certification results of 39 such products from 33 different vendors during November and December 2019.

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

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 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.

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

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.

Ad-Spider

Windows 7 version	2019.11.01
Windows 10 version	2019.11.01
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Adaware Antivirus Free

Windows 7 version	12.6.1005.11662
Windows 10 version	12.6.1005.11662
WildList detection	99.9%
False positive rate	0.000%
Diversity Test rate	100.00%

ISSN 1749-7027

Adaware Antivirus Pro

Windows 7 version	12.6.1005.11662
Windows 10 version	12.6.1005.11662
WildList detection	99.9%
False positive rate	0.000%
Diversity Test rate	100.00%

AVG Internet Security

Windows 7 version	19.8.3108
Windows 10 version	19.8.3108
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

AhnLab V3 Internet Security 9.0

Windows 7 version	9.0.57.3
Windows 10 version	9.0.57.3
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Cynet 360

Windows 7 version	8.3.54.124
Windows 10 version	8.3.54.124
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

Arcabit AntiVirus

Windows 7 version	2019.11.03
Windows 10 version	2019.11.04
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Defenx Security Suite

Windows 7 version	1.4.0.7
Windows 10 version	1.4.0.7
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

Avast Free Antivirus

Windows 7 version	19.8.2393
Windows 10 version	19.8.2393
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Emsisoft Anti-Malware

Windows 7 version	2019.10.0.9803
Windows 10 version	2019.10.0.9803
WildList detection	99.9%
False positive rate	0.000%
Diversity Test rate	100.00%

eScan Internet Security Suite for Windows

Windows 7 version	14.0.1400.2175
Windows 10 version	14.0.1400.2175
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

ESET Internet Security

Windows 7 version	13.0.22.0
Windows 10 version	13.0.22.0
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

ESET Smart Security Premium

Windows 7 version	13.0.22.0
Windows 10 version	13.0.22.0
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

ESET Endpoint Security

Windows 7 version	7.1.2053.0
Windows 10 version	7.1.2053.0
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

ESTsecurity ALYac

Windows 7 version	4.0.2.23116
Windows 10 version	4.0.2.23116
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Exosphere Endpoint Protection *(see notes in Appendix 2)*

Windows 7 version	8.3.54.124
Windows 10 version	8.3.54.128
WildList detection	99.9%
False positive rate	0.000%
Diversity Test rate	99.70%

Faronics Anti-Virus

Windows 7 version	4.20.3102.471
Windows 10 version	4.20.3102.471
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

FireEye Endpoint Security

Windows 7 version	30.19.3
Windows 10 version	30.19.3
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Fortinet FortiClient

Windows 7 version	6.0.8.0261
Windows 10 version	6.0.8.0261
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

G DATA Antivirus

Windows 7 version	25.5.4.21
Windows 10 version	25.5.4.21
WildList detection	99.9%
False positive rate	0.000%
Diversity Test rate	100.00%

Heimdal Thor Vigilance

Windows 7 version	2.5.222
Windows 10 version	2.5.222
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

IKARUS anti.virus

Windows 7 version	3.1.6
Windows 10 version	3.1.6
WildList detection	100.0%
False positive rate	0.001%
Diversity Test rate	100.00%

ITL Total Security *(see notes in Appendix 2)*

Windows 7 version	1.0.0.11
Windows 10 version	1.0.0.11
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

K7 Total Security

Windows 7 version	16.0.0122
Windows 10 version	16.0.0120
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.80%

Kaspersky Endpoint Security 11 for Windows *(see notes in Appendix 2)*

Windows 7 version	11.1.1.126
Windows 10 version	11.1.1.126
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	-

NANO Antivirus

Windows 7 version	1.0.134.90395
Windows 10 version	1.0.134.90395
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	98.39%

PCProtect

Windows 7 version	4.14.31
Windows 10 version	4.14.31
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

Rising Security Cloud Client

Windows 7 version	3.0.0.93
Windows 10 version	3.0.0.93
WildList detection	100.0%
False positive rate	0.006%
Diversity Test rate	86.48%

SentinelOne Endpoint Security Platform

(see notes in Appendix 2)

Windows 7 version	3.2.4.54
Windows 10 version	3.2.4.54
WildList detection	99.9%
False positive rate	0.001%
Diversity Test rate	-

Scanguard

Windows 7 version	4.14.31
Windows 10 version	4.14.31
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

TACHYON Endpoint Security

Windows 7 version	5.0.0.57
Windows 10 version	5.0.0.57
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

TeamViewer Endpoint Protection

Windows 7 version	1.4.207175
Windows 10 version	1.4.207175
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Tencent PC Manager

Windows 7 version	12.3.26607.901
Windows 10 version	12.3.26607.901
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.60%

Total Defense Premium

Windows 7 version	11.5.2.28
Windows 10 version	11.5.2.28
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

Total Defense Unlimited

Windows 7 version	11.5.2.28
Windows 10 version	11.0.0.775
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

TotalAV

Windows 7 version	4.14.31
Windows 10 version	4.14.31
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	99.50%

VIPRE Advanced Security

Windows 7 version	11.0.4.2
Windows 10 version	11.0.4.2
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

VirIT eXplorer PRO

Windows 7 version	9.0.36
Windows 10 version	9.0.52
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	68.01%

Wontok SafeCentral Security Suite

Windows 7 version	2.0.1548
Windows 10 version	2.0.1548
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	100.00%

APPENDIX 1: PRODUCTS NOT CERTIFIED

Cyren Command Anti-Malware did not achieve VB100 certification in this test.

APPENDIX 2: TESTING NOTES

- Test results for *Exosphere Endpoint Protection* are based on *Windows 10* data only, as data inconsistencies rendered the *Windows 7* test results unreliable.
- *ITL Total Security* was tested in on-demand test mode. At the request of the vendor, we also note that real-time protection behaviour was also observed, if not tested.
- The Diversity Test results for *Kaspersky Endpoint Security 11 for Windows* were considered unreliable due to an engineering error on *VB*'s behalf, and were discarded.
- The Diversity Test results for *SentinelOne Endpoint Security Platform* were invalidated due to technical issues on both test platforms.

APPENDIX 3: SAMPLE SET SIZES

The WildList (certification) set contained 2,471 malicious samples. The set of clean samples used for the false positive test contained 100,000 files, of which 29,175 were portable executable (PE) files. The set used for the Diversity Test contained 991 malicious samples.

Editor: Martijn Grooten
Head of Testing: Peter Karsai
Security Test Engineers: Gyula Hachbold, Adrian Luca, Csaba Mészáros, Tony Oliveira, Ionuţ Răileanu
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin

© 2019 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com
Web: https://www.virusbulletin.com/