FEBRUARY 2019

virus BULLETIN

Covering the global threat landscape

VB100 CERTIFICATION REPORT FEBRUARY 2019

Martijn Grooten

Anti-malware products don't have an easy job these days. There are millions of malware samples – which tend to be written with the explicit goal of bypassing anti-malware products – to be detected and blocked, while at the same time there are millions of legitimate programs – which occasionally use some of the same techniques as malware – that *mustn't* be blocked. On top of that, there are dozens of competing products on the market.

Users are right to expect anti-malware products to satisfy a minimum standard of blocking malicious executables that have recently been seen in the wild, while blocking few to no legitimate programs.

For more than two decades, *Virus Bulletin* has set a minimum standard for anti-virus (or anti-malware) products, checking whether products live up to expectation and providing those that do with the VB100 'stamp of approval'.

This report details the performance of 30 such products from 28 different vendors during January and February 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.

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

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.

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.

Adaware Antivirus Free

Windows 7 version	12.6.997.11652
Windows 10 version	12.6.997.11652
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	97.44%

ISSN 1749-7027

Adaware Antivirus Pro

Windows 7 version	12.6.997.11652
Windows 10 version	12.6.997.11652
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	97.44%

AVG Internet Security

Windows 7 version	19.1.3075
Windows 10 version	19.1.3075
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

AhnLab V3 Internet Security 9.0

Windows 7 version	9.0.52.5
Windows 10 version	9.0.52.5
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Cynet 360

Windows 7 version	8.3.52.190
Windows 10 version	8.3.52.190
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Arcabit AntiVirus

Windows 7 version	2019.01.14
Windows 10 version	2019.01.10
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Cyren Command Anti-Malware

Windows 7 version	5.2.1
Windows 10 version	5.2.1
WildList detection	99.6%
False positive rate	0.002%
Diversity test rate	99.59%

Avast Free Antivirus

Windows 7 version	19.1.2360
Windows 10 version	19.1.2360
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Defenx Security Suite

Windows 7 version	15.1.0112
Windows 10 version	15.1.0112
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Emsisoft Anti-Malware

Windows 7 version	2018.12.1.9144
Windows 10 version	2018.12.1.9144
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Exosphere Endpoint Protection

Windows 7 version	V18121900
Windows 10 version	V19012400
WildList detection	99.9%
False positive rate	0.000%
Diversity test rate	100.00%

eScan Internet Security Suite for Windows

Windows 7 version	14.0.1400.2029
Windows 10 version	14.0.1400.2029
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Faronics Anti-Virus

Windows 7 version	4.12.3102.401
Windows 10 version	4.12.3102.401
WildList detection	100.0%
False positive rate	0.008%
Diversity test rate	100.00%

ESET Internet Security

Windows 7 version	12.0.31.0
Windows 10 version	12.0.31.0
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

FireEye Endpoint Security

Windows 7 version	27.31.0.0
Windows 10 version	27.31.0.0
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

ESTsecurity ALYac

Windows 7 version	3.0.1.3.31873
Windows 10 version	3.0.1.3.31873
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

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	100.00%

G DATA Antivirus

Windows 7 version	25.5.0.2
Windows 10 version	25.5.0.4
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	99.90%

IKARUS anti.virus

Windows 7 version	2.19.14
Windows 10 version	2.19.14
WildList detection	100.0%
False positive rate	0.002%
Diversity test rate	99.08%

K7 Total Security

Windows 7 version	15.1.0350
Windows 10 version	15.1.0350
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

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	99.69%

Rising Security Cloud Client

Windows 7 version	3.0.0.85
Windows 10 version	3.0.0.85
WildList detection	100.0%
False positive rate	0.003%
Diversity test rate	91.61%

TACHYON Endpoint Security

Windows 7 version	5.0.0.57
Windows 10 version	5.0.0.57
WildList detection	100.0%
False positive rate	0.007%
Diversity test rate	100.00%

TeamViewer Endpoint Protection

Windows 7 version	1.0.105328
Windows 10 version	1.0.129712
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

Tencent PC Manager

Windows 7 version	12.3.26600.901
Windows 10 version	12.3.26597.901
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	100.00%

Total Defense Unlimited V11

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

VIPRE Advanced Security

Windows 7 version	11.0.3.20
Windows 10 version	11.0.3.20
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	100.00%

VirIT eXplorer PRO

Windows 7 version	8.8.44
Windows 10 version	8.8.42
WildList detection	100.0%
False positive rate	0.000%
Diversity test rate	81.68%

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

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 *Adaware Antivirus Free* and *Adaware Antivirus Pro*, the results of the diversity test on *Windows 7* were discarded due to technical issues.
- For *TeamViewer Endpoint Protection*, the results of the diversity test on *Windows 10* were discarded due to technical issues.
- For *Rising Security Cloud Client*, the results of the first part of the certification test were discarded due to technical issues.

APPENDIX 3: SAMPLE SET SIZES

The WildList contained 2,908 samples. The set of clean files used for the false positive test contained 99,996 files, of which 29,217 were portable executable (PE) files. The set used for the Diversity Test contained 977 samples.

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

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com
Web: https://www.virusbulletin.com/