Independent Tests of
Anti-Virus Software

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD: MARCH 2022
LAST REVISION: 11TH APRIL 2022

WWW.AV-COMPARATIVES.ORG

Details of false alarms

In AV testing, it is important to measure not only detection capabilities but also reliability. One aspect of reliability is the ability to recognize clean files as such, and not to produce false alarms (false positives). No product is immune from false positives (FPs), but some produce more than others. False Positives Tests measure which programs do best in this respect, i.e. distinguish clean files from malicious files, despite their context. There is no complete collection of all legitimate files that exist, and so no "ultimate" test of FPs can be done. What can be done, and is reasonable, is to create and use a set of clean files which is independently collected. If, when using such a set, one product has e.g. 15 FPs and another only 2, it is likely that the first product is more prone to FPs than the other. It doesn't mean the product with 2 FPs doesn't have more than 2 FPs globally, but it is the relative number that is important.

All listed false alarms were encountered at the time of testing. False alarms caused by unencrypted data blocks in anti-virus related files were not counted. If a product had several false alarms belonging to the same application, it is counted here as only one false alarm. Cracks, keygens, or other highly questionable tools, including FPs distributed/shared primarily by vendors (which may be in the several thousands) or other non-independent sources are not counted here as false positives.

In order to give more information to the user about the false alarms, we try to rate the prevalence of the false alarms. Files which were digitally signed are considered more important. Due to that, a file with the lowest prevalence level (Level 1) and a valid digital signature is upgraded to the next level (e.g. prevalence "Level 2"). Extinct files which according to several telemetry sources had zero prevalence have been provided to the vendors in order to fix them, but have also been removed from the set and were not counted as false alarms.

The prevalence is given in five categories and labeled with the following colors: 🟢🟢🟡🟠🔴

Level		Presumed number of affected users	Comments
1	🟢	Probably fewer than a hundred users	Individual cases, old or rarely used files, very low prevalence
2	🟢	Probably several hundreds of users	Initial distribution of such files was probably much higher, but current usage on actual systems is lower (despite its presence), that is why also well-known software may now affect / have only a prevalence of some hundreds or thousands of users.
3	🟡	Probably several thousands of users	
4	🟠	Probably several tens of thousands (or more) of users	
5	🔴	Probably several hundreds of thousands or millions of users	Such cases are likely to be seen much less frequently in a false alarm test done at a specific time, as such files are usually either whitelisted or would be noticed and fixed very fast.

Most false alarms will probably (hopefully) fall into the first two levels most of the time.

In our opinion, anti-virus products should not have false alarms on any sort of clean files regardless of how many users are currently affected by them. While some AV vendors may play down the risk of false alarms and play up the risk of malware, we are not going to rate products based on what the supposed prevalence of false alarms is. We already allow a certain number of false alarms (currently 10) inside our clean set before we start penalizing scores, and in our opinion products which produce a higher number of false alarms are also more likely to produce false alarms with more prevalent files (or in other sets of clean files). The prevalence data we give for clean files is just for informational purpose. The listed prevalence can differ inside the report, depending on which file/version the false alarm occurred, and/or how many files of the same kind were affected.

There may be a variation in the number of false positives produced by two different programs that use the same engine (principal detection component). For example, Vendor A may license its detection engine to Vendor B, but Vendor A's product may have more or fewer false positives than Vendor B's product. This can be due to factors such as different internal settings being implemented, differences in other components and services such as additional or differing secondary engines/signatures/whitelist databases/cloud services/quality assurance, and possible time delay between the release of the original signatures and the availability of the signatures for third-party products.

False Positives (FPs) are an important measurement for AV quality. Furthermore, the test is useful and needed to avoid that vendors optimize products to score good in tests by looking at the context – this is why false alarms are being mixed and tested the same way as tests with malware are done. One FP report from a customer can result in large amount of engineering and support work to resolve the issue. Sometimes this can even lead to important data loss or system unavailability. Even "not significant" FPs (or FPs on older applications) deserve mention and attention because FPs are likely to be a result of principled rule detections. It just happened that the FP was on an insignificant file. The FP possibility is probably still in the product and could potentially cause an FP again on a more significant file. Thus, they still deserve mention and still deserve to be penalised. Below you will find some info about the false alarms we observed in our independent set of clean files. Red entries highlight false alarms on files that were digitally signed.

The detection names shown were taken mostly from pre-execution scan logs (where available). If a threat was blocked on/during/after execution (or no clear detection name was seen), we state "Blocked" in the column "Detected as".

ESET had zero false alarms.

Avira

False alarm found in some parts of	Detected as	Supposed prevalence
Xspy package	Blocked	🟢

Avira had 1 false alarm.

TotalAV

False alarm found in some parts of	Detected as	Supposed prevalence
Xspy package	TR/FakeAV.dtym.1	🟢

TotalAV had 1 false alarm.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
FileShredder package	UDS:Trojan-Downloader.Win32.Banload	🟢
PCviewer package	UDS:DangerousObject.Multi.Generic	🟢

Kaspersky had 2 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
CL package	Real Protect-LS!9959ef7e3cf2	🟢
Cleanerz package	Real Protect-LS!6cdcb20b70c6	🟢
Cubes package	Real Protect-LS!32eeed54f167	🟢

McAfee had 3 false alarms.

NortonLifeLock

False alarm found in some parts of	Detected as	Supposed prevalence
DirectX package	Trojan.Gen.X	🔴
Easo package	Trojan.Gen	🔴
MKV package	Trojan.FakeAV	🟡
Pyth package	Heur.AdvML.B	🟢

NortonLifeLock had 4 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
CL package	Trojan:Win32/Contebrew.A!ml	🟢
Elenco package	Trojan:Win32/Wacatac.B!ml	🟢
Polish package	Trojan:Win32/Sabsik.FL.B!ml	🟢
VirtualSkipper package	Trojan:Win32/Bearfoos.B!ml	🟢

Webber package	Trojan:Win32/Wacatac.B!ml	🟢

Microsoft had 5 false alarms.

Malwarebytes

False alarm found in some parts of	Detected as	Supposed prevalence
BitComet package	Blocked	🟡
DevArt package	Blocked	🟢
ExtensionManager package	MachineLearning/Anomalous.100%	🟢
Faronics package	MachineLearning/Anomalous.94%	🟢
GetNetwork package	MachineLearning/Anomalous.96%	🟢
VideoCodec package	MachineLearning/Anomalous.95%	🟢
Xspy package	URL-Block	🟢

Malwarebytes had 7 false alarms.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
DeskCalc package	Gen:Heur.Mint.Titirez.Hr0@6Gaaz57S	🟢
Faronics package	Blocked	🟢
Fotocolor package	Blocked	🟢
Gesangstrainer package	Blocked	🟢
Kalender package	Blocked	🟢
OpenImage package	Gen:Variant.Fugrafa.195558	🟢
TextImport package	Blocked	🟢
Videothek package	Blocked	🟢

Bitdefender had 8 false alarms.

Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
DeskCalc package	Gen:Heur.Mint.Titirez.Hr0@6Gaaz5	🟢
DevArt package	Blocked	🟢
Faronics package	Blocked	🟢
Fotocolor package	Blocked	🟢
Gesangstrainer package	Blocked	🟢
Kalender package	Blocked	🟢
OpenImage package	Gen:Variant.Fagrufa.195558	🟢
TextImport package	Blocked	🟢

Total Defense had 8 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Burst package	Suspicious	🟢
BuyerTools package	Suspicious	🟢
CueCard package	Suspicious	🟢
DialerControl package	Suspicious	🟢
Hamburg package	Suspicious	🟢
HDCleaner package	Suspicious	🟡
Mediapiraten package	Suspicious	🟢
Snorkel package	Suspicious	🟢
Tweakpower package	Suspicious	🟢

Trend Micro had 9 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
AVG package	Blocked	🟢
DeskCalc package	Blocked	🟢
DevArt package	Blocked	🟢
Faronics package	Blocked	🟢
Gesangstrainer package	Blocked	🟢
Kalender package	Blocked	🟢
ReaConverter package	Blocked	🟢
TextImport package	Blocked	🟢
Videothek package	Blocked	🟢

VIPRE had 9 false alarms.

Avast / AVG

False alarm found in some parts of	Detected as	Supposed prevalence
BinkVideo package	Blocked	🟢
Faronics package	Blocked	🟢
GetNetwork package	Blocked	🟢
MultiCommander package	FileRepMetagen	🟢
Polish package	Blocked	🟢
Preishai package	Blocked	🟢
QuickBatch package	Win32:Malware-gen	🟢
SubFun package	FileRepMalware	🟢
Tracer package	FileRepMetagen	🔴
Webbit package	Blocked	🟢

Avast and AVG had 10 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
AdwCleaner package	Suspicious Program (ID700019)	🔴
ArchiCrypt package	Suspicious Program (ID700021)	🟢
Archive package	Trojan (004943941)	🟡
BlazeMedia package	Suspicious Program (ID700017)	🟢
Burst package	Suspicious Program (ID700021)	🟢
CL package	Riskware (dec0049c1)	🟢
Clickr package	Trojan (0058dd021)	🟢
Commander package	Suspicious Program (ID700021)	🟢
Datenbank package	Riskware (0040eff71)	🟢
DiagramDesigner package	Suspicious Program (ID700021)	🟢
DialerControl package	Suspicious Program (ID700021)	🟢
DQSD package	Suspicious Program (ID700018)	🟡
ImDisk package	Suspicious Program (ID700021)	🟡
Jam package	Suspicious Program (ID700021)	🟢
Jdtricks package	Suspicious Program (ID700021)	🟢
Leadtek package	Suspicious Program (ID700021)	🟢
MrToolbox package	Suspicious Program (ID700022)	🟢
Overclock package	Suspicious Program (ID700021)	🟢
Pioneer package	Suspicious Program (ID700026)	🟡
Polish package	Suspicious Program (ID700021)	🟢
Smadav package	Suspicious Program (ID700027)	🔴
SPS package	Suspicious Program (ID700021)	🟢
TotalText package	Suspicious Program (ID700016)	🟢
UnPop package	Suspicious Program (ID700027)	🟢
Winboard package	Suspicious Program (ID700026)	🟢

K7 had 25 false alarms.

G Data

False alarm found in some parts of	Detected as	Supposed prevalence
Abfluege package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
AMP package	Win32.Heur.1E0E31ED (CyberDefenseCloud)	🟢
AutoHotKey package	Win32.Heur.D58919DD (CyberDefenseCloud)	🟡
AVG package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Bench package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
Biostar package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Calendar package	Win32.Heur.1E0E31ED (CyberDefenseCloud)	🟢
CDstart package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢

Challenger package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
CL package	Gen:Variant.Graftor.955535 (Engine A)	🟢
Clickr package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
CNC package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
CPUtest package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Crillion package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
CWK package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟠
Datenbank package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
Decrap package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟠
DeskCalc package	Gen:Heur.Mint.Titirez.Hr0@6Gaaz57S	🟢
DriverView package	Win32.Heur.828A692 (CyberDefenseCloud)	🟢
DrSoftware package	Win32.Heur.828A692 (CyberDefenseCloud)	🟢
Faronics package	Win32.Heur.7E6050EF (CyberDefenseCloud)	🟢
FFDshow package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Fileanalyser package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
FileZilla package	Win32.Heur.7E605EF (CyberDefenseCloud)	🔴
Floppy package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
GigaByte package	Win32.Heur.828A692 (CyberDefenseCloud)	🟡
Kalk package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
Karma package	Win32.Heur.8282A692 (CyberDefenseCloud)	🟢
LinkGenerator package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
MailAlert package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Max package	Win32.Heur.1E0E31ED (CyberDefenseCloud)	🟢
MSI package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
OpenImage package	Gen:Variant.Fugrafa.195558	🟢
OpenOffice package	Win32.Heur.FF49E01E (CyberDefenseCloud)	🟢
PCW package	JS.Heur.Calisto.3.D0313108.Gen	🟢
Pestblock package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Pioneer package	Win32.Heur.7E6050EF (CyberDefenseCloud)	🟢
Polish package	Win32.Trojan.PSE.F5TQRF (CyberDefenseCloud)	🟢
Preishai package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
ProDVD package	Gen:Trojan.Heur3.LPT.bmW@aW0svtbab	🟢
QuickBatch package	Win32.Heur.20BEE2002 (CyberDefenseCloud)	🟢
Regcool package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
RegSeeker package	Win32.Heur.FF49E01E (CyberDefenseCloud)	🟢
Service package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Spam package	Win32.heur.1E0E31ED (CyberDefenseCloud)	🟢
SPS package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
Startdelay package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢

Starttime package	Win32.Heur.1E0E31D (CyberDefenseCloud)	🟢
TextMaker package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Tiscali package	Win32.Heur.8282A692 (CyberDefenseCloud)	🟢
Toppler package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Tweakpower package	Win32.Heur.FF49E01E (CyberDefenseCloud)	🟢
UnPop package	Win32.Heur.1E0E31ED (CyberDefenseCloud)	🟢
URLfind package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Various package	Win32.Backdoor.Sakurel.DA30N8 (CyberDefenseCloud)	🟢
Winpatrol package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
WinTime package	Win32.Heur.7E605EF (CyberDefenseCloud)	🟢
Worms package	Win32.Heur.CD15437A (CyberDefenseCloud)	🟢
ZoomPlayer package	Win32.Heur.FF49E01E (CyberDefenseCloud)	🟢

G Data had 59 false alarms. According to the vendor, the product had more FPs than usual due to a bug they had in March 2022, which was fixed after the test.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
Abfluege package	Suspicious	🟢
Acronis package	Suspicious	🟢
Ageia package	Suspicious	🟢
AlZip package	Suspicious	🟢
Atomic package	Suspicious	🟢
Aviso package	Suspicious	🟢
AZN package	Suspicious	🟢
BCX package	Suspicious	🟢
BietButler package	Suspicious	🟢
Biostar package	Suspicious	🟢
Black package	Suspicious	🟢
BlazeMedia package	Suspicious	🟢
Bubble package	Suspicious	🟢
Calendar package	Suspicious	🟢
Call package	Suspicious	🟡
Checkmail package	Suspicious	🟢
CL package	Suspicious	🟢
Clock package	Suspicious	🟢
Clocx package	Suspicious	🟢
CNC package	Suspicious	🟢
Combine package	Suspicious	🟢
Czoomer package	Suspicious	🟢

DateInTray package	Suspicious	🟢
Disable package	Suspicious	🟢
DropIt package	Suspicious	🟢
Easo package	Trj/StartPage.DAW	🔴
Elenco package	Suspicious	🟢
ExtensionManager package	Suspicious	🟢
Faronics package	Suspicious	🟢
Feratel package	Malicious Packer	🟡
Flower package	Suspicious	🟢
Fototuning package	Suspicious	🟢
Foxit package	Trojan	🟢
Garrys package	Suspicious	🟢
GetNetwork package	Suspicious	🟢
Goowiba package	Suspicious	🟢
GTracing package	Suspicious	🟢
Hardalyzer package	Suspicious	🟢
HardwareInspector package	Suspicious	🟢
Haztek package	Suspicious	🟢
Hotkicks package	Suspicious	🟢
Intrapact package	Suspicious	🟢
Jam package	Suspicious	🟢
Jukebox package	Suspicious	🟢
Keyboardlink package	Suspicious	🟢
MagicText package	Suspicious	🟢
Menue package	Suspicious	🟢
Merchant package	Suspicious	🟢
Minitool package	Suspicious	🔴
Modem package	Suspicious	🟢
Moodbook package	Suspicious	🟢
Muenzen package	Suspicious	🟢
Munnin package	Suspicious	🟢
NetSMS package	Suspicious	🟢
Office package	Trj/Nabload.DMH	🔴
OpenOffice package	Suspicious	🟢
Outliner package	Suspicious	🟢
PCviewer package	Suspicious	🟢
PCW package	Suspicious	🟢
Pegasun package	Suspicious	🟢
PEtoUSB package	Suspicious	🟢

PNotes package	Suspicious	🟢
PrivacyExpert package	Suspicious	🟢
Puzzle package	Suspicious	🟢
Pyth package	Suspicious	🟢
QT package	Suspicious	🟢
QuickBatch package	Suspicious	🟢
Rage3D package	Suspicious	🟢
ReaConverter package	Suspicious	🟢
RJT package	Suspicious	🟢
Robot package	Suspicious	🟢
RogueSpear package	Suspicious	🟢
RSWE package	Suspicious	🟢
RTL package	Suspicious	🟢
Scumm package	Suspicious	🟢
Shark package	Suspicious	🟢
Spamihilator package	Suspicious	🟢
Speedify package	Suspicious	🟡
SSE package	Suspicious	🟢
Statusindicator package	Suspicious	🟢
SteuerCD package	Suspicious	🟢
SubFun package	Suspicious	🟢
Subtitle package	Trj/RnkBend.A	🟡
Sunbird package	Suspicious	🟢
System package	Suspicious	🟡
Tiscali package	Suspicious	🟢
Toppler package	Suspicious	🟢
UltraViewer package	Suspicious	🔴
UnPop package	Suspicious	🟢
Various package	Trj/GdSda.A	🟡
VideoFun package	Suspicious	🟢
VideoTool package	Suspicious	🟢
VirtualSkipper package	Suspicious	🟢
WinPIM package	Suspicious	🟢
Wsus package	Suspicious	🟡
XEditor package	Suspicious	🟢

Panda had 96 false alarms.

Copyright and Disclaimer

This publication is Copyright © 2022 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(April 2022)