Independent Tests of
Anti-Virus Software

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD: SEPTEMBER 2025
LAST REVISION: 7TH OCTOBER 2025

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. In our view, antivirus products should not generate false alarms on any clean files, irrespective of the number of users affected. While some antivirus vendors may downplay the risk of false alarms and exaggerate the risk of malware, we do not base product ratings solely on the supposed prevalence of false alarms. We currently tolerate a certain number of false alarms (currently 10) within our clean set before penalizing scores. Products that yield a higher number of false alarms are more likely to trigger false alarms with more prevalent files or in other sets of clean files. The prevalence data we provide for clean files is purely for informational purposes. The listed prevalence may vary within the report, depending on factors such as which file/version triggered the false alarm or how many files of the same kind were affected. There can be disparities in the number of false positives produced by two different programs utilizing the same detection engine. For instance, Vendor A may license its detection engine to Vendor B, yet Vendor A's product may exhibit more or fewer false positives than Vendor B's product. Such discrepancies could stem from various factors, including differences in internal settings, additional or varying secondary engines/signatures/whitelist databases/cloud services/quality assurance, and potential delays in making signatures available to third-party products.

Sometimes, a few vendors attempt to dispute why some clean or non-malicious software/files are blocked or detected. Explanations may include: the software being unknown or too new and awaiting whitelisting, detection of non-current/old versions due to newer software version availability, limited usage within their userbase, complete absence of any user reports on false positives (thus suggesting false positives are non-existent for them), bugs in the clean software (e.g., an application crashing under certain circumstances), errors or missing information in End User License Agreements making it illegal in some countries (like a missing/unclear disclosure of data transmission), subjective user interface usability issues (e.g., missing the option to close the program in the system tray), software being available only in specific languages (e.g., Chinese), assumptions that the file must be malware because other vendors detect it according to a multi-scanning service (copycat behaviour we increasingly observe, unfortunately), or issues with unrelated software from the same vendor/distributor many years ago. If these rules were consistently applied, almost every clean software would be flagged as malware at some point. Such dispute reasons often lack validity and are therefore rejected. Antivirus products could enhance user control and understanding by offering options such as filtering based on language or EULA validity and providing clear explanations for detections rather than blanket classification as malware. This would empower users to manage and understand detection reasons more effectively. Ultimately, it's not about which specific file is misclassified but that it is misclassified. Achieving a high malware score is effortless if done with lax signatures/heuristics at the expense of false positives. Although we even list here the prevalence of the files, the same detection rules causing those FPs on some rare files can as well be the cause for a major FP case if the detection signatures/heuristics are not properly fixed/adapted.

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, 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 labelled with the following colours:

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.

False Positives (FPs) serve as a critical measurement for assessing antivirus quality. Moreover, such testing is necessary to prevent vendors from optimizing products solely to perform well in tests. Hence, false alarms are assessed and tested in the same manner as malware tests. A single FP report from a customer can trigger a significant amount of engineering and support work to resolve the issue, sometimes resulting in data loss or system unavailability. Even seemingly insignificant FPs (or FPs on older applications) warrant attention because they may still indicate underlying issues in the product that could potentially cause FPs on more significant files. Below, you'll find information about the false alarms observed in our independent set of clean files. Entries highlighted in red denote false alarms on files that were digitally signed.

The detection names presented were primarily obtained from pre-execution scan logs, where available. If a threat was blocked during or after execution, or if no clear detection name was identified, we indicate "Blocked" in the "Detected as" column.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
Cefkit package	HEUR:Trojan-PSW.Win32.Pycoon.gen	
Eosmsg package	Trojan.Win32.Dynara.awtk	
Gui package	HEUR:Trojan.MSIL.Generic	

Kaspersky had 3 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Boosterx package	Threat	
Idealtec package	Threat	
Kgdmnprn package	Threat	
Listiger package	Threat	
Soffidesso package	Threat	
Speedtest package	Threat	

Trend Micro had 6 false alarms.

Bitdefender / Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
Apmadmin package	Trojan.GenericKD.76789611	
Chifaofficine package	Gen:Variant.MSILHeracles.236266	
Hexbindeal package	Gen:Variant.Midie.162034	
Rolltest package	Gen:Variant.Fugrafa.336472	
Rustfmt package	Gen:Variant.Zusy.597252	
Soffidesso package	Gen:Trojan.Heur.JP.bOW@a0tYQSni	
Spectrasonics package	Trojan.GenericKD.72434518	

Bitdefender and Total Defense had 7 false alarms.

Avast / AVG / Norton

False alarm found in some parts of	Detected as	Supposed prevalence
Acta package	Win32:MalwareX-gen [Trj]	
Actualizar package	Win32:Malware-gen	
Boosterx package	Win32:Malware-gen	
Eosmsg package	Win32:Malware-gen	
Lidar package	FileRepMalware [Misc]	
Rustfmt package	FileRepMalware [Misc]	
Seeds package	FileRepMalware [Misc]	
Unikey package	Win64:Malware-gen	

Avast, AVG and Norton had 8 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
Devdetect package	Suspicious Program (ID700026)	
Diskinternals package	Suspicious Program (ID709004)	
Eosmsg package	is a Trojan (005c9f851)	
Freestylegunz package	Suspicious Program (ID700021)	
Frodspayment package	is a Trojan (700000201)	
Perfectsystem package	Suspicious Program (ID700021)	
Soffidesso package	Suspicious Program (ID30013)	
Xtick package	is a Trojan-Downloader (005779501)	

K7 had 8 false alarms.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
Apmadmin package	Blocked	
Fastfill package	Suspicious	
Freestylegunz package	Blocked	
Greenhat package	Suspicious	
Kgdmnprn package	Blocked	
Opencage package	Blocked	
Sswait package	Suspicious	
Switchy package	a variant of Win64/Agent_AGen.FLS trojan	
Unikey package	Suspicious	
Vbhxhsigning package	Blocked	

ESET had 10 false alarms.

G Data

False alarm found in some parts of	Detected as	Supposed prevalence
Acta package	Win32.Trojan.Agent.AHSDEN (Engine B)	
Apmadmin package	Trojan.GenericKD.76789611 (Engine A)	
Chifaofficine package	Gen:Variant.MSILHeracles.236266 (Engine A)	
Frodspayment package	MSIL.Trojan.PSE.G1U5XF (Engine B)	
Hexbindeal package	Gen:Variant.Midie.162034 (Engine A)	
Rolltest package	Gen:Variant.Fugrafa.336472 (Engine A)	
Rustfmt package	Gen:Variant.Zusy.597252 (Engine A)	
Soffidesso package	Gen:Trojan.Heur.JP.bOW@a0tYQSni (Engine A)	
Spectrasonics package	Trojan.GenericKD.72434518 (Engine A)	
Winwart package	Win32.Trojan.Agent.00GBOV (Engine B)	

G Data had 10 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
AntiPhishing package	Malware (General)	
Apmadmin package	Trojan.GenericKD.76789611	
Chifaofficine package	Gen:Variant.MSILHeracles.236266	
Corel package	Malware (General)	
Hexbindeal package	Gen:Variant.Midie.162034	
Hhesolver package	Malware (General)	
Inabexerp package	Malware (General)	
PreuzmiFarm package	Malware (General)	
Rolltest package	Gen:Variant.Fugrafa.336472	
Rustfmt package	Gen:Variant.Zusy.597252	
Soffidesso package	Gen:Trojan.Heur.JP.bOW@a0tYQSni	
Spectrasonics package	Trojan.GenericKD.72434518	
Sswait package	Virus.Generic	
Testapp package	Malware (General)	
Tip2012 package	Malware (General)	
Vl700license package	Malware (General)	
WinSecurityGate package	Malware (General)	

VIPRE had 17 false alarms.

Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
Actualizar package	Trojan.Ghanarava	
Addition package	Heuristics.ML	
Analisisisr package	Trojan.Ghanarava	
Apmadmin package	Trojan.Ghanarava	
Censorsql package	Trojan.Ghanarava	
Devdetect package	Trojan.Ghanarava	
EASYBURN package	Trojan.Ghanarava	
Freestylegunz package	Trojan.Ghanarava	
Inabexerp package	Heuristics.ML	
Kgdmnprn package	Trojan.Ghanarava	
Kuebler package	Heuristics.ML	
Listiger package	Trojan.Ghanarava	
Matrixcom package	Trojan.cloudsig	
Mitupdate package	Trojan.Crimload	
Msworks package	Trojan.Ghanarava	
QCP package	Heuristics.ML	
Registraraura package	Trojan.Ghanarava	
Sh4da package	Trojan.Ghanarava	

Sigame package	Trojan.Ghanarava	
Spectrasonics package	Trojan.Ghanarava	
Vl700license package	Trojan.Ghanarava	
Xaudio package	Trojan.Ghanarava	
YabeBrowser package	Heuristics.ML	

Quick Heal had 23 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
5mcontest package	Trojan:Win32/Tnega!ml	
Actualizar package	Trojan:Win32/Wacatac.H!ml	
Apmadmin package	Program:Win32/Wacapew.C!ml	
Appd package	Trojan:Win32/Bearfoos.A!ml	
Autocfg package	Trojan:Win32/Wacatac.H!ml	
Awstypes package	Program:Win32/Wacapew.A!ml	
Boosterx package	Trojan:Win32/Wacatac.H!ml	
Chifaofficine package	Trojan:Win32/Wacatac.B!ml	
Chronicler package	Trojan:Win32/Wacatac.B!ml	
Connecttest package	Trojan:Script/Wacatac.B!ml	
Cosmos package	Trojan:Win32/Wacatac.B!ml	
Dateikatalog package	Trojan:Win32/Fimal!rfn	
Despulante package	Trojan:Win32/Wacatac.H!ml	
Dnepr7 package	Trojan:Win32/Wacatac.B!ml	
Kgdmnprn package	Trojan:Win32/Wacatac.H!ml	
Microfarma package	Trojan:Win32/Wacatac.H!ml	
MPlus package	Trojan:Win32/Wacatac.C!ml	
OneClickStarter package	Trojan:Win32/Wacatac.B!ml	
Otlphttptest package	Trojan:Win32/Wacatac.B!ml	
Regex package	Trojan:Win32/Bearfoos.A!ml	
Rolltest package	Trojan:Win32/Phonzy.B!ml	
Selectors package	Trojan:Win32/Bearfoos.A!ml	
Sh4da package	Trojan:Win32/Wacatac.B!ml	
Spam package	Trojan:Win32/Fimal!rfn	
Spicetify package	Trojan:Win32/Wacatac.H!ml	
Testsecurecomm package	Trojan:Win32/Wacatac.B!ml	
Usbid package	Trojan:Win32/Wacatac.C!ml	

Microsoft had 27 false alarms.

Malwarebytes

False alarm found in some parts of	Detected as	Supposed prevalence
Acta package	Generic.Malware/Suspicious	
Censorsql package	Malware.AI	
Chronicler package	Generic.Malware/Suspicious	
Clonyxl package	Malware.AI	
Dacris package	Malware.Sandbox.28	
Devdetect package	Generic.Malware.AI.DDS	
Ekasuv package	MachineLearning/Anomalous.95%	
Emerge package	Malware.Sandbox.28	
Eosmsg package	Trojan.Crypt	
Faststone package	Malware.Heuristic	
Gotcha package	Malware.AI	
Gui package	Trojan.MalPack.PNG.Generic	
Hexbindeal package	Malware.Heuristic	
Ibox package	Malware.AI	
Inabexerp package	Malware.AI	
Jtalert package	Malware.Sandbox.17	
Listiger package	Generic.Malware/Suspicious	
Logagent package	Malware.AI	
Microfarma package	Malware.AI	
Pmsounds package	Malware.AI	
Registraraura package	Generic.Malware/Suspicious	
Sh4da package	Generic.Malware/Suspicious	
Sigame package	Malware.AI	
SIMKL package	Malware.AI	
Soffidesso package	Malware.AI	
Vanderlee package	Malware.Sandbox.4	
Vl700license package	Malware.AI	
ZoomPlayer package	Malware.AI	

Malwarebytes had 28 false alarms.

Avira / F-Secure / TotalAV

False alarm found in some parts of	Detected as	Supposed prevalence
5mcontest package	HEUR/APC	
Acta package	HEUR/APC.AVADL	
Actualizar package	Drop.Win32.ScoreExeDrop.181	
Appd package	HEUR/APC	
Autocfg package	HEUR/APC	
Bdatdecode package	HEUR/APC	
Benchmark package	HEUR/APC	

Boosterx package	TR/Downloader.Gen	
Configtoolsolar package	HEUR/APC	
Connecttest package	HEUR/APC	
Despulante package	HEUR/APC	
Devdetect package	Drop.Win32.ScoreKiller.520	
Dynamixcontroller package	HEUR/APC	
Ekasuv package	HEUR/APC	
Eosmsg package	HEUR/APC	
Extractmessages package	HEUR/APC	
Frodspayment package	HEUR/APC	
Guanjia package	HEUR/APC	
Hc9xxmanager package	HEUR/APC	
Jkcnsl package	HEUR/APC	
Lidar package	HEUR/AGEN.1379797	
Lpprjgen package	HEUR/APC	
Luart package	HEUR/APC	
Managedir package	HEUR/APC	
OpenEvent package	HEUR/APC	
Otlphttptest package	HEUR/APC	
Photobooth package	HEUR/APC	
Rawsteam package	HEUR/APC	
Registraraura package	TR/Mepaow.fsmds	
Relay package	HEUR/APC	
Repositionericons package	HEUR/APC	
Rocksdb package	HEUR/APC	
Rustfmt package	HEUR/APC.AVADL	
Seeds package	HEUR/AGEN.1380308	
Speecandnn package	HEUR/APC	
Speedtest package	HEUR/APC	
Spicetify package	HEUR/APC	
Svcwatchdog package	HEUR/APC	
Switch package	HEUR/APC	
Testsecurecomm package	HEUR/APC	
Transposer package	HEUR/APC	
Treeperformance package	HEUR/APC	
Ueics package	HEUR/APC	
Unikey package	TR/AVI.Agent.bkgku	
Websocat package	HEUR/APC	

Avira, F-Secure and TotalAV had 45 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
5mcontest package	hti!6d74a8b9	
Acta package	ti!D1BA3C0DDD69	
Apmadmin package	ti!787DB55218A6	
Augusta package	ti!CF9F0ADB8557	
Bdatdecode package	ti!07E4AEB1273E	
Chifaofficine package	Real Protect-LS!de4cffeb39b3	
Configtoolsolar package	ti!3DE07695439D	
Despulante package	ti!31194C0984BC	
Devdetect package	ti!5A3ED44300AB	
Dynamixcontroller package	ti!DF767999BF2E	
Elkontrol package	ti!879A663334A8	
Eosmsg package	ti!632AC73DF144	
Fastfill package	ti!A60953BC4DE5	
Freestylegunz package	ti!EC7DED49FE7B	
Frodspayment package	ti!997533CA4D72	
Guanjia package	ti!7BB942E05CAC	
Gui package	ti!0601BBB69F73	
Hexbindeal package	ti!04E6C9CBB1EE	
Jkcnsl package	ti!A87543D3D59D	
Kgdmnprn package	ti!F5D832470C5F	
Libc package	ti!47F09EB42A48	
Logagent package	ti!27424E5020C4	
Managedir package	ti!47F09EB42A48	
Mitupdate package	ti!E6CBD5CB9A22	
Perfectsystem package	ti!8E3822AA0044	
Pmsounds package	ti!B1E39E42BCCA	
Qode package	ti!689C23A0CFAD	
Registraraura package	ti!E6E1F4E4E0DD	
Repositionericons package	ti!B4BADF9F86F8	
Rolltest package	ti!B79F3F48BD97	
Sh4da package	hti!bcbaa7bd	
Sistemafacturacion package	ti!C14E12225D83	
Spectrasonics package	ti!7B28B0C4AA71	
Spicetify package	ti!ECDB03EBE454	
Sswait package	ti!E977EF7F36E0	
Sutula package	ti!A67D4CC789D0	
Switch package	ti!A0E0E0B280D5	
Switchy package	hti!3817df61	
Testapp package	ti!FD9558AAE048	
Testsecurecomm package	ti!26B4333F98E7	

Treeperformance package	ti!24A4423982FB	
Unikey package	Real Protect-HT.aa-1!d5ab0d6a9519	
Usbid package	ti!FD9558AAE048	
Vbhxhsigning package	Real Protect-LS!10afae5711d2	
Vl700license package	ti!628E75E8ADB6	
Xaudio package	ti!150B5DD3F2C5	

McAfee had 46 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
5mcontest package	Suspicious	
Acta package	Trj/Chgt.AD	
Actualizar package	Suspicious	
Appd package	Suspicious	
Audiocodes package	Trj/RnkBend.A	
Augusta package	Suspicious	
Awstypes package	Suspicious	
Bdatdecode package	Suspicious	
Benchmark package	Suspicious	
Boosterx package	Trj/Chgt.AD	
Cefkit package	Suspicious	
Censorsql package	Trj/Chgt.AD	
Chifaofficine package	Suspicious	
Chronicler package	Suspicious	
Clearwater package	Suspicious	
Configtoolsolar package	Suspicious	
Cosmos package	Suspicious	
Dacris package	Trj/Agent.PHX	
Despulante package	Suspicious	
Dynamixcontroller package	Suspicious	
Eduroam package	Suspicious	
Ekasuv package	Suspicious	
Elkontrol package	Suspicious	
Extractmessages package	Suspicious	
Faststone package	Trj/Chgt.AD	
Filemove package	Suspicious	
Freestylegunz package	Suspicious	
Greenhat package	Suspicious	
Gui package	Suspicious	
Hcfruntime package	Suspicious	
Hexbindeal package	Suspicious	

Hhesolver package	Suspicious	
Httparse package	Suspicious	
Ibox package	Trj/GdSda.A	
Inabexerp package	Suspicious	
Jkcnsl package	Trj/Chgt.AD	
Jtalert package	Trj/RnkBend.A	
Kdpsuite package	Suspicious	
Kgdmnprn package	Trj/Chgt.AD	
Kkchara package	Suspicious	
Libc package	Suspicious	
Lidar package	Suspicious	
Listiger package	Trj/Chgt.AD	
Logagent package	Suspicious	
Lpprjgen package	Suspicious	
Luart package	Suspicious	
Managedir package	Suspicious	
Matrixcom package	Suspicious	
Mitupdate package	Suspicious	
Muupdater package	Suspicious	
Opencage package	Suspicious	
Openevent package	Suspicious	
Otlphttptest package	Suspicious	
Pmsounds package	Suspicious	
PreuzmiFarm package	Suspicious	
Quran package	Suspicious	
Rasdeleteentry package	Suspicious	
Regex package	Suspicious	
Repositionericons package	Suspicious	
Rocksdb package	Suspicious	
Rolltest package	Suspicious	
Romflasher package	Trj/RansomGen.A	
Rustfmt package	Suspicious	
Seeds package	Suspicious	
Selectors package	Suspicious	
Sistemafacturacion package	Suspicious	
Soffidesso package	Trj/Chgt.AD	
Spectrasonics package	Trj/Chgt.AD	
Speedtest package	Suspicious	
Spicetify package	Suspicious	
Sswait package	Suspicious	

Svcwatchdog package	Suspicious	
Tailbound package	Suspicious	
Taxgov package	Suspicious	
Testapp package	Suspicious	
Testsecurecomm package	Suspicious	
Thumbnail package	Trj/Agent.PHX	
Transposer package	Suspicious	
Treeperformance package	Suspicious	
Usbid package	Suspicious	
Vbhxhsigning package	Suspicious	
Vl700license package	Suspicious	
Websocat package	Suspicious	
Xtick package	Trj/Chgt.AD	
YabeBrowser package	Malware	

Panda had 85 false alarms.

Copyright and Disclaimer

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

AV-Comparatives
(October 2025)