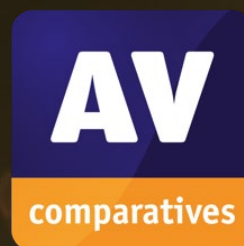


Independent Tests of Cybersecurity Solutions



Details of False Alarms **Appendix to the Malware Protection Test**

TEST PERIOD: MARCH 2026
LAST REVISION: 7TH APRIL 2026

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	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.
5 	Probably several hundreds of thousands or millions of users	

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
Trueep package	HEUR:Trojan.Win32.Agent.gen	
Yealink package	HEUR:Trojan-PSW.Win32.Agent.gen	

Kaspersky had 2 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	Trojan:Win32/Yomal!rfn	
Otterpayment package	Trojan:Script/Wacatac.C!ml	
Traceorder package	Trojan:Win32/Wacatac.B!ml	

Microsoft had 3 false alarms.

Bitdefender, Total Defense, VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
Credentialvault package	Trojan.GenericKD.77657047	
G5Cconfig package	Blocked	
Square package	Trojan.Heur.FU.ae0@aKFnlleG	
Thinkgrinder package	Trojan.GenericKDZ.115473	

Bitdefender, Total Defense and VIPRE had 4 false alarms.

G Data

False alarm found in some parts of	Detected as	Supposed prevalence
Credentialvault package	Trojan.GenericKD.77657047	
Square package	Trojan.Heur.FU.ae0@aKFnlleG	
Thinkgrinder package	Trojan.GenericKDZ.115473	
Traceorder package	IL:Trojan.MSILZilla.226407	
Yealink package	MSIL.Trojan.PSE.17COF18	

G Data had 5 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	Threat	
Ipv6Enable package	Threat	
Numbergame package	Threat	
Operagx package	Threat	
Pioasm package	Threat	
Rtcharts package	Threat	
Smarthdd package	Threat	
Thinkgrinder package	Threat	

Trend Micro had 8 false alarms.

Avast, AVG, Norton

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	Win32:MalwareX-gen [Pws]	
Altodesck package	Blocked	
Motorconfig package	Blocked	
Officeplan package	Win32:MalwareX-gen [Drp]	
Pkvall package	Blocked	
Ritualcaster package	Blocked	
Singbox package	Blocked	
Thinkgrinder package	Win32:MalwareX-gen [Trj]	
Traceorder package	Win32:MalwareX-gen [Trj]	

Avast, AVG and Norton had 9 false alarms.




Fortect

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	TR/W32.MalwareX	
Altodesck package	HEUR/AGEN.1378740	
Officeplan package	DR/W32.MalwareX	
Rabbitmq package	HEUR/APC	
Regex package	HEUR/APC	
Ritualcaster package	HEUR/APC	
Singbox package	TR/Agent.khhbz	
Thinkgrinder package	TR/W32.MalwareX	
Traceorder package	TR/W32.MalwareX	
Trueep package	HEUR/APC	

Fortect had 10 false alarms.

















McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	ti!1349B0599A14	
Activationmanager package	ti!9A9E3798D547	
Adtool package	ti!4B46DA2BBD2A	
Connectiontest package	ti!5601FE9C2CC3	
Dshowmon package	ti!5298EFE26CEA	
Ipv6Enable package	ti!D69F837282FD	
Jtalert package	ti!9665EAE407A6	
Klickwin package	ti!5E3AD924D167	
Pcnp package	ti!E29F76388F4C	
Pioasm package	ti!4D9576858B29	
Ritualcaster package	ti!1E04DC3B42F9	

Rtcharts package	ti!1A5BC34EC5B7	
Thinkgrinder package	ti!0BC8B40A6BC3	
Traceorder package	ti!C8391B09A8F6	














McAfee had 14 false alarms.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	Suspicious	
Adpb package	Suspicious	
Credentialvault package	Suspicious	
Doesnotbelong package	Suspicious	
Httpstest package	Suspicious	
Imagespider package	Blocked	
Ipv6Enable package	Suspicious	
Motorconfig package	Suspicious	
Quran package	Win32/Injector_Agen.ATZ	
Rabbitmq package	Suspicious	
Scriptbuild package	Suspicious	
Spaceshooter package	Suspicious	
Thinkgrinder package	Suspicious	
Userstatus package	Suspicious	
Vrcworlds package	Suspicious	
Wiremock package	Suspicious	

ESET had 16 false alarms.

Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	Blocked	
29Palms package	Blocked	
Alfaecare package	Trojan.Generic.TRFH1573	
Altodesck package	Trojan.Generic.TRFH1338	
Credentialvault package	Blocked	
Dshowmon package	Trojan.Agent	
Exium package	Trojan.Generic.TRFH1562	
Freestylegunz package	Browsing Protection	
Fujida package	Blocked	
Jtalert package	Blocked	
Netgear package	Trojan.Generic.TRFH535	
Passorder package	Blocked	
Pioasm package	Blocked	

Tfrispecify package	Blocked	
Thinkgrinder package	Blocked	
Yealink package	Trojan.Generic.TRFH1565	

Quick Heal had 16 false alarms.

F-Secure, TotalAV

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	TR/W32.MalwareX	
Adtool package	Drop.Win64.ScoreExeDrop.4120	
Alfaecare package	HEUR/APC.AVADL	
Altodesck package	HEUR/AGEN.1378740	
Avltree package	HEUR/APC	
Credentialvault package	HEUR/APC.AVADL	
Dattowatchdog package	HEUR/APC.AVADL	
G5Cconfig package	HEUR/APC.AVADL	
Officeplan package	DR/W32.MalwareX	
Otterpayment package	HEUR/APC	
Rabbitmq package	HEUR/APC	
Regex package	HEUR/APC	
Ritualcaster package	HEUR/APC.AVADL	
Singbox package	TR/Agent.khhbz	
Thinkgrinder package	TR/W32.MalwareX	
Traceorder package	TR/W32.MalwareX	
Trueep package	HEUR/APC	
Wiremock package	HEUR/APC	
Yesclick package	HEUR/APC	

F-Secure and TotalAV had 19 false alarms.

Sophos

False alarm found in some parts of	Detected as	Supposed prevalence
Connectiontest package	Mal/Generic-S	
Dshowmon package	Mal/Generic-S	
Ffptokenmng package	Mal/Generic-S	
Freestylegunz package	Generic ML	
Fujida package	Mal/Generic-S	
G5Cconfig package	Mal/Generic-S	
Imagespider package	Mal/Generic-S	
Ipv6Enable package	Mal/Generic-S	
Otterpayment package	Generic ML	
Pyxis package	Generic ML	

Rabbitmq package	Mal/Generic-S	
Rtcharts package	Mal/Generic-S	
Theotown package	Mal/Generic-S	
Thinkgrinder package	Mal/Generic-S	
Traceorder package	Mal/Generic-S	
Volcanoapp package	Generic ML	
Webapi package	Generic ML	
Xtick package	Mal/Generic-S	
Yealink package	Generic ML	

Sophos had 19 false alarms.

Malwarebytes

False alarm found in some parts of	Detected as	Supposed prevalence
1Cstart package	Generic.Malware/Suspicious	
Aidfile package	URL Block	
Autohotkey package	Malware.AI	
Avltree package	Malware.Heuristic.266	
Credentialvault package	Generic.Malware/Suspicious	
Dattowatchdog package	Malware.AI	
Despulante package	Malware.Heuristic.266	
Dshowmon package	Trojan.Crypt.Generic	
Exium package	Blocked	
Ffptokenmng package	Malware.Heuristic.205	
Freestylegunz package	MachineLearning/Anomalous	
G5Cconfig package	Malware.AI	
Ipip package	Trojan.MalPack.MSIL	
Jtalert package	MachineLearning/Anomalous	
Klickwin package	Malware.Sandbox.17	
Operagx package	Malware.Heuristic.205	
Passorder package	Trojan.Agent.E	
Quran package	Malware.Heuristic.2141	
Spicetify package	Malware.Heuristic.266	
Theotown package	Malware.Heuristic.2075	
Traceorder package	Trojan.Agent.E	
Wormhole package	Malware.Heuristic.205	
Xenon package	Malware.AI	

Malwarebytes had 23 false alarms.

K7




False alarm found in some parts of	Detected as	Supposed prevalence
Accountkeep package	Suspicious Program (ID700022)	
Activationmanager package	Trojan (700000211)	
Adpb package	Backdoor (005ce0d91)	
Adtool package	Trojan (700000201)	
Avltree package	Suspicious Program (ID709003)	
Brazilland package	Suspicious Program (ID700026)	
Credentialvault package	Trojan (700000201)	
Dattowatchdog package	Trojan (700000201)	
Dshowmon package	Trojan (005b3ef91)	
Gsacontact package	Trojan (005d2a5a1)	
Gsaurredirect package	Trojan (005d2a5a1)	
Guanjia package	Suspicious Program (ID709003)	
Imagespider package	Trojan (005d2a5a1)	
Ipip package	Trojan (004d3cb81)	
Ipv6Enable package	Trojan (700000201)	
Ltsvc package	Trojan (700000201)	
Pioasm package	Trojan (005d35af1)	
Pkvall package	Suspicious Object in Program (ID700021)	
Rtcharts package	Trojan (700000201)	
Stopwatchvbnet package	Suspicious Program (ID709000)	
Switchy package	Trojan (005d65a01)	
Theotown package	Trojan (005d01cf1)	
Vpnmanager package	Trojan (700000201)	
Xxcp package	Trojan (700000201)	

K7 had 24 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
Accountkeep package	Suspicious	
Activationmanager	Suspicious	
Adpb package	Suspicious	
Adtool package	Suspicious	
Aidfile package	Suspicious	
Altodesck package	Suspicious	
Autohotkey package	Suspicious	
Avltree package	Suspicious	
Brazilland package	Suspicious	
Connectiontest package	Suspicious	
Credentialvault package	Suspicious	

Despulante package	Suspicious	
Doesnotbelong package	Suspicious	
Faststone package	Malware	
Ffptokenmng package	Suspicious	
Fujida package	Suspicious	
G5Cconfig package	Suspicious	
Gui package	Suspicious	
Httpstest package	Suspicious	
Ibox package	Suspicious	
Ipip package	Suspicious	
Ipv6Enable package	Suspicious	
Jtalert package	Suspicious	
Kdpsuite package	Suspicious	
Keysystems package	Suspicious	
Klickwin package	Suspicious	
Ltsvc package	Suspicious	
Masmeditor package	Suspicious	
Numbergame package	Suspicious	
Officeplan package	Suspicious	
Operagx package	Trojan Trj/Genetic.gen	
Passorder package	Suspicious	
Passwordadmin package	Suspicious	
Quran package	Suspicious	
Rabbitmq package	Suspicious	
Resulthtml package	Suspicious	
Rtcharts package	Suspicious	
Scriptbuild package	Suspicious	
Simulator package	Suspicious	
Smarthdd package	Suspicious	
Spaceshooter package	Suspicious	
Spicetify package	Suspicious	
Square package	Suspicious	
Tfrispecify package	Suspicious	
Theotown package	Suspicious	
Traceorder package	Suspicious	
Trueep package	Suspicious	
Userstatus package	Suspicious	
Visomat package	Suspicious	
Vrcworlds package	Suspicious	
Webapi package	Suspicious	

Xxcp package	Suspicious		
Yealink package	Suspicious		
Yesclick package	Suspicious		

Panda had 54 false alarms.



Copyright and Disclaimer

This publication is Copyright © 2026 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 2026)