Independent Tests of
Anti-Virus Software

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD: MARCH 2025
LAST REVISION: 4TH APRIL 2025

WWW.AV-COMPARATIVES.ORG

Details of False Alarms

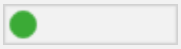
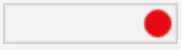
In AV testing, it is important to measure not only detection capabilities but also reliability. One aspect of reliability is the ability to recognize clean files as such, and not to produce false alarms (false positives). No product is immune from false positives (FPs), but some produce more than others. 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.

G Data / Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
Actualizar package	Gen:Variant.Marsilia.103237	
Chronicler package	Gen:Variant.Marsilia.137224	
Soffidesso package	Gen:Variant.Jaik.225543	

G Data and Total Defense had 3 false alarms.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
Actualizar package	VHO:Trojan-Downloader.MSIL.Stantinko.gen	
AntiPhishing package	UDS:Trojan.Win32.Agent.gen	
VirtualSkipper package	VHO:Trojan.Win32.Sdum.gen	

Kaspersky had 3 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Metatrader package	HEU_AEGISCS901T	
SimpleMachine package	HEU_AEGISCS901T	
Soffidesso package	HEU_AEGISCS912	
WSA package	HEU_AEGISCS901T	

Trend Micro had 4 false alarms.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
Actualizar package	Gen:Variant.Marsilia.103237	
Chronicler package	Gen:Variant.Marsilia.137224	
Ghost package	Blocked	
Sigame package	Blocked	
Soffidesso package	Gen:Variant.Jaik.225543	

Bitdefender had 5 false alarms.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
Chronicler package	Suspicious Object	
Kdpsuite package	Suspicious Object	
Metatrader package	Win64/Packed.VMProtect.AC	
Operagx package	Suspicious Object	
Privacy package	Blocked	
Simulator package	Suspicious Object	

ESET had 6 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
Alfaebooks package	Suspicious Program (ID709001)	
Backup package	Suspicious Program (ID700026)	
Faststone package	Suspicious Program (ID709001)	
IDE package	Suspicious Program (ID700021)	
Kdpsuite package	Suspicious Program (ID700021)	
Nuclei package	Suspicious Program (ID700022)	
Soffidesso package	Riskware (00584baa1)	

K7 had 7 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
Actualizar package	Virus.Generic	
Amlmaple package	Malware (General)	
Chronicler package	Virus.Generic	
Faststone package	Malware (General)	
Mailus package	Malware (General)	
Remotecontrol package	Malware (General)	
Soffidesso package	Virus.Generic	
Tip package	Malware (General)	

VIPRE had 8 false alarms.

Avast / AVG / Norton

False alarm found in some parts of	Detected as	Supposed prevalence
Capfirelist package	Win32:MalwareX-gen [Trj] (0)	
Censorsql package	FileRepMalware [Misc]	
Chronicler package	Win64:SpywareX-gen [Trj] (0)	
Eldenringmod package	Win64:Malware-gen (0)	
Ggleap package	Win32:MalwareX-gen [Trj] (0)	
Inabexerp package	Win32:Evo-gen [Trj] (0)	
Operagx package	FileRepMalware [Misc]	
Quickd package	Win32:MalwareX-gen [Trj] (0)	
Ramsay package	IDP.Generic	
Soffidesso package	Win32:TrojanX-gen [Trj] (0)	

Avast, AVG and Norton had 10 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
Chronicler package	Program:Win32/Wacapew.C!ml	
Dateikatalog package	Trojan:Win32/Wacatac.B!ml	
Ghost package	Backdoor:Win32/Bladabindi!ml	
Inabexerp package	Trojan:Win32/Wacatac.H!ml	
Listiger package	Trojan:Win32/Conteban.A!ml	
Mailus package	Backdoor:Win32/Bladabindi!ml	
Simkl package	Trojan:Win32/Wacatac.B!ml	
Soffidesso package	Trojan:Win32/UnusualASEP	
Spam package	Trojan:Win32/Wacatac.B!ml	
Staffexpressbank package	Trojan:Win32/Wacatac.B!ml	

Microsoft had 10 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
Actualizar package	ti!88DD183F1791	
Alfaebooks package	ti!8FCF183C3B1C	
Backup package	ti!3EA11B954417	
Bpsconf package	ti!A3B2DF578D37	
Chronicler package	ti!6B106722826F	
Claritysuccess package	ti!bf3d0c76cc07	
Clearwater package	ti!F53F8EB6CAB1	
Countertrack package	Real Protect-HT.aa-1!295276ba827e	
Eldenringmod package	Trojan:Win/PythonDownloader.JA	
Faststone package	ti!E5A77C9B5BEB	
H2mmod package	ti!80F858239789	
Inabexerp package	ti!E58D5C145648	
Modestmovie package	ti!DDA62F139F09	
Soffidesso package	ti!A67D4CC789D0	
Staffexpressbank package	ti!EF1D09D09BB2	

McAfee had 15 false alarms.

Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
Addition package	Heuristics.ML	
Addtime package	Heuristics.ML	
Censorsql package	Trojan.Ghanarava	
CleanDisk package	Heuristics.ML	
DOomsday package	Blocked	
EasyBurn package	Trojan.Ghanarava	

Go2PDF package	Heuristics.ML	
Inabexerp package	Heuristics.ML	
Kuebler package	Heuristics.ML	
Listiger package	Trojan.Ghanarava	
Mitupdate package	Trojan.Crimload	
Passmark package	Win32.Heur.MUE	
QCP package	Heuristics.ML	
Sigame package	Trojan.Ghanarava	
Works package	Trojan.Ghanarava	
YabeBrowser package	Heuristics.ML	

Quick Heal had 16 false alarms.

AVIRA / TotalAV

False alarm found in some parts of	Detected as	Supposed prevalence
Aicommit package	HEUR/APC	
Backup package	HEUR/APC	
Bpsconf package	HEUR/APC	
Browsercheck package	HEUR/APC	
Chronicler package	HEUR/APC	
Clearwater package	HEUR/APC	
Comcontrol package	HEUR/APC	
Csvtool package	HEUR/APC	
Dashmpdcli package	HEUR/APC	
Direxplorer package	HEUR/APC	
Elkontrol package	HEUR/APC	
Enroll package	HEUR/APC	
Faststone package	HEUR/APC	
Ggleap package	TR/Kryptik.iwcgm	
Ghost package	HEUR/APC	
Inabexerp package	HEUR/APC	
K4nikon package	HEUR/APC	
Kdpsuite package	HEUR/APC	
Meanalyzer package	HEUR/APC	
Operagx package	TR/Redcap.b1e39e	
Papi package	HEUR/APC	
Regressiontest package	HEUR/APC	
Salarii package	HEUR/APC	
Soffidesso package	HEUR/APC	
Staffexpressbank package	HEUR/APC	
Sysinfo package	HEUR/APC	

Tui package	HEUR/APC	
Ultimatewindowstweaker package	Drop.Win32.ScoreExeDrop.171	

AVIRA and TotalAV had 28 false alarms.

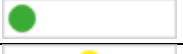
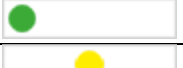
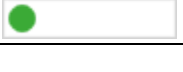
Panda

False alarm found in some parts of	Detected as	Supposed prevalence
Aicommit package	Suspicious	
Aidfile package	Suspicious	
Bpsconf package	Suspicious	
Censorsql package	Trj/Chgt.AD	
Chronicler package	Suspicious	
Clearwater package	Suspicious	
Comcontrol package	Suspicious	
Csvtool package	Suspicious	
Dacris package	Trj/Agent.PHX	
Direxplorer package	Suspicious	
Elkontrol package	Suspicious	
Faststone package	Suspicious	
FoxIt package	Malware	
Ggleap package	Suspicious	
Inabexerp package	Suspicious	
Jtalert package	Trj/RnkBend.A	
Kdpsuite package	Suspicious	
Keystates package	Suspicious	
Mailus package	Suspicious	
Meanalyzer package	Suspicious	
Metatrader package	Suspicious	
Papi package	Suspicious	
Regressiontest package	Suspicious	
Reliefvalve package	Suspicious	
Remindme package	Trj/Agent.PHX	
Remotecontrol package	Suspicious	
Romflasher package	Trj/RansomGen.A	
Simulator package	Suspicious	
Soffidesso package	Trj/Chgt.AD	
Thumbnail package	Trj/Agent.PHX	
Tip package	Suspicious	
Tui package	Suspicious	
Uartassist package	Suspicious	
Ultimatewindowstweaker package	Suspicious	

YabeBrowser package	Malware	

Panda had 35 false alarms.

Malwarebytes

False alarm found in some parts of	Detected as	Supposed prevalence
Ace package	Malware.Sandbox	
ActiveKeys package	Malware.Heuristic	
AutoFlowChart package	Malware.AI	
Automaster package	Malware.AI	
Bitdefender package	Malware.AI	
Calculation package	Malware.Heuristic	
Cat package	Malware.Sandbox	
Censorsql package	Malware.Heuristic	
ClonyXL package	Malware.Sandbox	
Dacris package	Malware.Sandbox	
Databurn package	Malware.AI	
DrDivx package	Malware.AI	
DVBviewer package	Malware.AI	
EasyBurn package	Malware.AI	
Elkontrol package	MachineLearning/Anomalous	
EMerge package	Malware.Sandbox	
ERight package	Malware.AI	
Faststone package	Malware.AI	
Finanz package	Malware.AI	
Formac package	Malware.AI	
Ggleap package	Trojan.FakeSig	
GPU package	Malware.AI	
Grub2win package	Malware.Sandbox	
Inabexerp package	Malware.Heuristic	
Jtalert package	Malware.AI	
Kdpsuite package	Malware.AI	
Keystates package	Malware.AI	
Linkgenerator package	Malware.Sandbox	
Listiger package	Generic.Malware/Suspicious	
Loop package	Malware.AI	
MAF package	Malware.AI	
Max package	Malware.AI	
Maxpasswords package	Malware.Sandbox	
Metatrader package	Malware.Heuristic	
MSWorks package	Malware.Sandbox	

NAS package	Malware.AI	
Pcanalyzer package	Malware.Sandbox	
Popdvd package	Malware.AI	
Pyxis package	Malware.AI	
Ramsay package	Malware.Sandbox	
Safe package	Malware.Sandbox	
Scuba package	Malware.AI	
Simkl package	Malware.AI	
SimpleMachine package	Malware.AI	
Soffidesso package	Malware.AI	
TinyTask package	Malware.AI	
TubeMate package	Malware.Sandbox	
Uartassist package	Malware.Sandbox	
UBCD package	Malware.AI	
Uvkultra package	Malware.AI	
Vanderlee package	Malware.Sandbox	
Virtualbox package	Malware.Heuristic	
Zabkat package	Malware.AI	

Malwarebytes had 53 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
Ace package	Suspicious:W32/Malware!DeepGuard.pg	
AdKiller package	Suspicious:W32/Malware!DeepGuard.p	
Aicommit package	HEUR/APC	
Amlmaple package	Suspicious:W32/Malware!DeepGuard.pg	
Autostartmanager package	Suspicious:W32/Malware!DeepGuard.p	
AutoZip package	Suspicious:W32/Malware!DeepGuard.pg	
Azguard package	Suspicious:W32/Malware!DeepGuard.pg	
Backup package	HEUR/APC	
BGTimer package	Suspicious:W32/Malware!DeepGuard.pg	
BlackJack package	Suspicious:W32/Malware!DeepGuard.p	
Boer package	Suspicious:W32/Malware!DeepGuard.pg	
Bpsconf package	HEUR/APC	
Browsercheck package	HEUR/APC	
Budget package	Suspicious:W32/Malware!DeepGuard.pg	
Chronicler package	HEUR/APC	
Clearwater package	HEUR/APC	
Comcontrol package	HEUR/APC	
Csvtool package	HEUR/APC	

Dashmpdcli package	HEUR/APC	
Dateikatalog package	Suspicious:W32/Malware!DeepGuard.p	
Direxplorer package	HEUR/APC	
DrHobby package	Suspicious:W32/Malware!DeepGuard.pg	
DrSoftware package	Suspicious:W32/Malware!DeepGuard.p	
EasyVideo package	Suspicious:W32/Malware!DeepGuard.pg	
EBook package	Suspicious:W32/Malware!DeepGuard.pg	
Elkontrol package	HEUR/APC	
Enroll package	HEUR/APC	
Erotik package	Suspicious:W32/Malware!DeepGuard.pg	
Explor package	Suspicious:W32/Malware!DeepGuard.pg	
Finkler package	Suspicious:W32/Malware!DeepGuard.pg	
Freshdow package	Suspicious:W32/Malware!DeepGuard.p	
Ggleap package	TR/Kryptik.iwcgm	
Girokonto package	Suspicious:W32/Malware!DeepGuard.pg	
Inabexerp package	HEUR/APC	
K4nikon package	HEUR/APC	
Kdpsuite package	HEUR/APC	
Linkgenerator package	Suspicious:W32/Malware!DeepGuard.p	
Lizenzomat package	Suspicious:W32/Malware!DeepGuard.pg	
Lotus package	Suspicious:W32/Malware!DeepGuard.pg	
Mandelbrot package	Suspicious:W32/Malware!DeepGuard.p	
Mash package	Suspicious:W32/Malware!DeepGuard.pg	
Meanalyzer package	HEUR/APC	
Morsen package	Suspicious:W32/Malware!DeepGuard.pg	
MPEG package	Suspicious:W32/Malware!DeepGuard.pg	
NotesBrowser package	Suspicious:W32/Malware!DeepGuard.pg	
Papi package	HEUR/APC	
Passwordgenerator package	Suspicious:W32/Malware!DeepGuard.pg	
Pcanalyzer package	Suspicious:W32/Malware!DeepGuard.p	
PowerEditor package	Suspicious:W32/Malware!DeepGuard.p	
Processengineering package	Suspicious:W32/Malware!DeepGuard.pg	
ProjectTimer package	Suspicious:W32/Malware!DeepGuard.pg	
Regressiontest package	HEUR/APC	
RHF package	Suspicious:W32/Malware!DeepGuard.p	
Salarii package	HEUR/APC	
Simkl package	Suspicious:W32/Malware!DeepGuard.pg	
Soffidesso package	HEUR/APC	
Staffexpressbank package	HEUR/APC	
Sysinfo package	HEUR/APC	

SysPad package	Suspicious:W32/Malware!DeepGuard.p	
Tage package	Suspicious:W32/Malware!DeepGuard.pg	
TrojanRemover package	Suspicious:W32/Malware!DeepGuard.p	
Tui package	HEUR/APC	
Warner package	Suspicious:W32/Malware!DeepGuard.p	
Wtrate package	Suspicious:W32/Malware!DeepGuard.p	
YabeBrowser package	Suspicious:W32/Malware!DeepGuard.p	

F-Secure had 65 false alarms.

Copyright and Disclaimer

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

AV-Comparatives
(April 2025)