Independent Tests of
Anti-Virus Software

AV
comparatives

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD: SEPTEMBER 2023
LAST REVISION: 12TH OCTOBER 2023

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".

TotalAV had zero false alarms.

Avast / AVG

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

Avast and AVG had 1 false alarm.

Avira

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

Avira had 1 false alarm.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
Fotograf package	ML/Augur trojan	🟢

ESET had 1 false alarm.

G Data

False alarm found in some parts of	Detected as	Supposed prevalence
Kuebler package	Win32.Trojan.PSE.RYYJMQ	🟢
Spybot package	Win32.Trojan.PSE.P9P6IR	🟢

G Data had 2 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Jujitsu package	Blocked	🟢
Tennis package	Blocked	🟡

Trend Micro had 2 false alarms.

Bitdefender / Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
Maple package	Blocked	🟢
Moorhuhn package	Blocked	🔴
Screensaver package	Blocked	🟢
Start package	Blocked	🟡

Bitdefender and Total Defense had 4 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
AutoHotKey package	Blocked	🟢
Databecker package	Blocked	🟢
GTRacing package	Blocked	🟢
Infernal package	Blocked	🟢
WinPower package	Blocked	🟢

Microsoft had 5 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
Feratel package	Security risk detected Unknown name	🟡
FoxIT package	Trojan detected Unknown name	🟢
Kyokumi package	Blocked	🟢
Meldemax package	Security risk detected Unknown name	🟢
Pause package	Blocked	🟢

Panda had 5 false alarms.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
Autoconnect package	Trojan.Win32.Generic	🟢
HostLib package	Trojan.Win32.Generic	🟢
HP package	Trojan.Win32.Generic	🟠
KTE package	Trojan.Win32.Generic	🟢
Muehle package	Trojan.Win32.Generic	🟢
Tiscali package	UDS:DangerousObject.Multi.Generic	🟢

Kaspersky had 6 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
Arcsoft package	ti!4FCFFD6D7836	🟡
Brockhaus package	ti!703947EDFA7D	🟢
Databecker package	ti!34DB112587F4	🟢
DeltaForce package	Real Protect-LS!3d09a9653c18	🟢
EA package	ti!7000FE74349F	🟢
Execute package	ti!34101C3B6DFE	🟢
FineReader package	Real Protect-LS!876549f2c659	🟢
JoWood package	ti!8CF4CB8FBF11	🟢
PaperOffice package	ti!AB0E8DFDC02E	🟢
Tennis package	Blocked	🟡

McAfee had 10 false alarms.

Norton

False alarm found in some parts of	Detected as	Supposed prevalence
Alpx package	Heur.AdvML.B	●○○○○
BioRythm package	Heur.AdvML.B	●○○○○
CDDVDburner package	Heur.AdvML.B	○●○○○
Databecker package	Blocked	○●○○○
EvilPlayer package	Heur.AdvML.B	○●○○○
Musicbase package	Blocked	●○○○○
NeverWinter package	Heur.AdvML.C	○●○○○
PCW package	Blocked	●○○○○
Tennis package	Blocked	○○●○○
Trans package	Heur.AdvML.B	●○○○○
USBaccess package	Blocked	●○○○○
Zabkat package	Heur.AdvML.B	○●○○○

Norton had 12 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
Aston package	Blocked	○○○●○
ComTest package	Blocked	●○○○○
CoolPlayer package	Trojan (005a42411)	●○○○○
Dreikampf package	Blocked	●○○○○
Fotograf package	Blocked	●○○○○
JoWood package	Blocked	○●○○○
KTE package	Blocked	○●○○○
LG package	Blocked	○●○○○
Macrorecorder package	Blocked	○○○○●
Macrovision package	Blocked	○●○○○
Mathcad package	Blocked	●○○○○
Maxx package	Blocked	●○○○○
PDFmachine package	Riskware (0040eff71)	●○○○○
PEtoUSB package	Blocked	●○○○○
Shareware package	Blocked	●○○○○
Unreal package	Blocked	○●○○○
Wonderfox package	Blocked	○●○○○

K7 had 17 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
AAMS package	Blocked	🟢
Boer package	Blocked	🟢
Dallas package	Blocked	🟢
DLLscan package	Blocked	🟢
DpZip package	Blocked	🟢
DrSoftware package	Blocked	🟢
EasyVideo package	Blocked	🟢
ExtraKeys package	Blocked	🟢
Freshdow package	Blocked	🟢
GetMP3 package	Packed:MSIL/SmartIL.A	🟢
Kyokumi package	Blocked	🟢
LG package	Blocked	🟢
Maple package	Blocked	🟢
Maxxpi package	Blocked	🟢
Musicbase package	Blocked	🟢
Samurize package	Trojan-Downloader:JS/TeslaCrypt.C	🔴
Starttime package	Blocked	🟢
StartupStar package	Blocked	🟢
SyncEXP package	Blocked	🟢
TakeColor package	Blocked	🟢
Tiscali package	Blocked	🟢
TrojanRemover package	Blocked	🟢
USBaccess package	Blocked	🟢
Warner package	Blocked	🟢
Wsarc package	Blocked	🟢

F-Secure had 25 false alarms.

Copyright and Disclaimer

This publication is Copyright © 2023 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
(October 2023)