Independent Tests of
Anti-Virus Software

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD: SEPTEMBER 2022
LAST REVISION: 10TH OCTOBER 2022

WWW.AV-COMPARATIVES.ORG

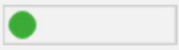
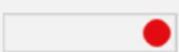
Details of false alarms

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".

Avira, ESET and **Kaspersky** had zero false alarms.

TotalAV

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

TotalAV had 1 false alarm.

NortonLifeLock

False alarm found in some parts of	Detected as	Supposed prevalence
Crillion package	Blocked	
PrinceOfPersia package	Generic.Malware/Suspicious	
WinterGames package	Generic.Malware/Suspicious	

NortonLifeLock had 3 false alarms.

G Data

False alarm found in some parts of	Detected as	Supposed prevalence
Auszeit package	Gen:Variant.Babar.53768	
LinkChecker package	Blocked	
TestDrive package	Generic.Malware/Suspicious	
WinterGames package	Generic.Malware/Suspicious	

G Data had 4 false alarms.

Avast / AVG

False alarm found in some parts of	Detected as	Supposed prevalence
FinalHit package	Generic.Malware/Suspicious	
NAS package	FileRepMalware [Trj]	
TigerWoods package	FileRepMalware [Trj]	
UFM package	Win32:Malware-gen	
WinterGames package	Generic.Malware/Suspicious	

Avast and AVG had 5 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Buyertools package	Blocked	
DialerControl package	Blocked	
Hamburg package	Blocked	
Puzzle package	Blocked	
Snorkel package	Blocked	
SPS package	Blocked	

Trend Micro had 6 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
ASMlessons package	Real Protect-LS!cb65b6e8e904	
CL package	Blocked	
Cleanerz package	Blocked	
FinalHit package	Blocked	
FixWin package	Blocked	
Polish package	Blocked	
TestDrive package	Blocked	

McAfee had 7 false alarms.

Bitdefender / Total Defense / VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Blocked	
Auszeit package	Gen:Variant.Babar.53768	
Barcode package	Blocked	
CoypToWin package	Blocked	
DVBviewer package	Blocked	
Gesangstrainer package	Blocked	
TestDrive package	Generic.Malware/Suspicious	
WinterGames package	Generic.Malware/Suspicious	

Bitdefender, Total Defense and VIPRE had 8 false alarms.

Malwarebytes

False alarm found in some parts of	Detected as	Supposed prevalence
AdKiller package	MachineLearning/Anomalous.100%	
Alpx package	Malware.AI.3566915212	
Arcsoft package	Malware.AI.1484920161	
Clara package	Malware.AI.1806035075	
Databurn package	MachineLearning/Anomalous.96%	
Defrag package	Malware.Sandbox.1	
Desert package	Trojan.Dropper	
Duden package	Malware.AI.4137526555	
FinalHit package	Generic.Malware/Suspicious	
Freshdow package	MachineLearning/Anomalous.100%	
NAS package	Malware.AI.4261013023	
NeverWinter package	Malware.AI.2471604693	
Skiracing package	Malware.AI.4099104802	
Tweaker package	Trojan.Agent	
Various package	Gen:Trojan.Heur.Dropper.bm0@a4fqYrPi	

WinterGames package	Generic.Malware/Suspicious	

Malwarebytes had 16 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
Animator package	Blocked	
Auszeit package	Blocked	
Brockhaus package	Blocked	
Camera package	Blocked	
Clickr package	Blocked	
Combine package	Blocked	
EasyBurning package	Blocked	
FFDshow package	Blocked	
FoxIt package	Blocked	
Hamburg package	Blocked	
IMU package	Blocked	
Linkgenerator package	Blocked	
Mediapiraten package	Blocked	
Merant package	Blocked	
Miranda package	Blocked	
PDFmailer package	Blocked	
TestDrive package	Blocked	
Tweakpower package	Blocked	
ZipGenius package	Blocked	

Microsoft had 19 false alarms.

K7

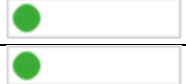
False alarm found in some parts of	Detected as	Supposed prevalence
Aid package	Blocked	
AllSync package	Blocked	
Archicrypt package	Blocked	
Archive package	Trojan (004943941)	
BestMovie package	Blocked	
Clickr package	Trojan (0058dd021)	
DialerControl package	Blocked	
E-Calc package	Blocked	
Elevate package	Blocked	
FK package	Blocked	
Hyperdesktop package	Blocked	
Imdisk package	Blocked	
Mailbox package	Blocked	

Maxx package	Blocked	
Miranda package	Blocked	
MP4 package	Blocked	
Musicmaker package	Blocked	
Orange package	Blocked	
Orangegem package	Blocked	
PhotoMatix package	Blocked	
Pioneer package	Blocked	
Polish package	Blocked	
Postguard package	Blocked	
Puzzle package	Blocked	
Smadav package	Blocked	
SPS package	Blocked	
Tiscali package	Blocked	
UnPop package	Blocked	
URLfind package	Blocked	
ZipGenius package	Blocked	

K7 had 30 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
Addressbar package	Blocked	
AdKiller package	Blocked	
Alpx package	Blocked	
AnyVideo package	Blocked	
ATI package	Blocked	
AudioSplit package	Blocked	
Auszeit package	Blocked	
Barcode package	Blocked	
BBL package	Blocked	
Call package	Suspicious file	
CFOS package	Blocked	
Cleanerz package	Blocked	
ClearProg package	Blocked	
Crillion package	Blocked	
CueMaker package	Blocked	
DataRecovery package	Blocked	
Developers package	Blocked	
DirSaver package	Blocked	

Disable package	Blocked	
DiskInternals package	Blocked	
Easo package	Trj/StartPage.DAW	
Easybuch package	Blocked	
eBlinkx package	Blocked	
Email package	Blocked	
Feratel package	Malicious Packer	
Firewall package	Blocked	
Floola package	Blocked	
Forms package	Blocked	
FoxIt package	Trojan	
Freshdow package	Blocked	
FritzBox package	Blocked	
IMU package	Blocked	
MeldeMax package	Malicious Packer	
MultiCommander package	Blocked	
MyPCbackup package	Trj/Chgt.L	
NetSMS package	Blocked	
Northstar package	Blocked	
Office package	Trj/Nabload.DMH	
Outlook package	Blocked	
Preishai package	Blocked	
RegSnap package	Blocked	
Sim package	Blocked	
Simple package	Blocked	
SipGate package	Blocked	
Skype package	Blocked	
Spam package	Blocked	
StatusIndicator package	Blocked	
Subtitle package	Trj/RnkBend.A	
Teracopy package	Blocked	
TestDrive package	Blocked	
Theses package	Blocked	
Tiscali package	Blocked	
Tweakpower package	Blocked	
UFM package	Blocked	
Updater package	Blocked	
Various package	Trj/GdSda.A	
WA package	Blocked	

Zabkat package	Blocked	
Zortam package	Blocked	

Panda had 59 false alarms.

Copyright and Disclaimer

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

AV-Comparatives
(October 2022)