

Independent Tests of Anti-Virus Software



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

TEST PERIOD: MARCH 2019
LANGUAGE: ENGLISH
LAST REVISION: 9TH APRIL 2019

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. 30 FPs and another only 5, it is likely that the first product is more prone to FPs than the other. It doesn't mean the product with 5 FPs doesn't have more than 5 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 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.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
eKalkulator package	a variant of Generik.LHFDDIH trojan	





ESET had 1 false alarm.

Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
ADAC package	UDS:DangerousObject.Multi.Generic	
T2S package	UDS:Trojan.Win32.Mucc.sb	
Viena package	HEUR:Trojan-Dropper.Win32.Dapato.gen	


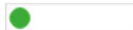
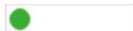



Kaspersky Lab had 3 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
MySermons package	HEUR/APC	
PDF2print package	HEUR/APC	
POIfinder package	HEUR/APC	
XWing package	HEUR/APC	









AVIRA had 4 false alarms.

Bitdefender / Total Defense / VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
Amok package	Trojan.GenericKD.31740927	
CheckSig package	DeepScan:Generic.Malware.SVWk!.E825438C	
Falucci package	Gen:Variant.Ursu.387943	
PCW package	VB:Trojan.Emeka.Inor.910	
SafeNSec package	Trojan.GenericKD.40500801	
UOM package	AIT.Downloader.2.Gen	










Bitdefender, Total Defense and VIPRE had 6 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
ACS package	Trojan:Win32/Fuery.B!cl	
Aptajm package	Trojan:Win32/Fuery.C!cl	
Dallascao package	Trojan:Win32/Bitrep.B	
DeltaForce package	Trojan:Win32/Fuery.C!cl	
GXTRanscoder package	Trojan:Win32/Vigorf.A	
ITpro package	Trojan:Win32/Fuery.B!cl	
Unreal package	Trojan:Win32/Azden.A!cl	
WinMHT package	Trojan:Win32/Fuery.C!cl	







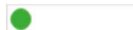








Microsoft had 8 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	JTI/Suspect.196612!5873dc365aa0	
Dallascao package	JTI/Suspect.196612!156ce81703dd	
Doppeldecker package	JTI/Suspect.262201!759d83a3dd67	
DrDivx package	JTI/Suspect.196612!6804df0678db	
FastRestore package	JTI/Suspect.196612!d269afcd49	
HyperDesktop package	JTI/Suspect.196612!b08b9919a803	
PlantvsZombies package	JTI/Suspect.196612!9d7ead13692f	
Spybot package	JTI/Suspect.196612!a9a5db6ac372	
YTdown package	JTI/Suspect.196612!10246cbd0ef1	

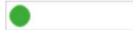
















McAfee had 9 false alarms.

Avast / AVG

False alarm found in some parts of	Detected as	Supposed prevalence
CheckSig package	FileRepMalware	
CleanDisk package	FileRepMalware	
EKalkulator package	FileRepMalware	
eMerge package	FileRepMalware	
FileWorks package	FileRepMalware	
FontInstaller package	This file may contain something bad.	
GPAC package	Win32:Evo-gen [Susp]	
GPI package	This file may contain something bad.	
HyperDesktop package	Win32:Malware-gen	
MeldeMax package	FileRepMalware	
NetCat package	This file may contain something bad.	
NetOP package	This file may contain something bad.	
PDF2print package	This file may contain something bad.	
UOM package	This file may contain something bad.	
YTdown package	Win64:Malware-gen	




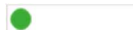






Avast and AVG had 15 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
ArchiCrypt package	Suspicious:W32/Malware/DeepGuard.pg	
CheckSig package	Suspicious:W32/Malware/DeepGuard.pg	
Dallascao package	Suspicious:W32/Malware/DeepGuard.pg	
EasyBurning package	Suspicious:W32/Malware/DeepGuard.pg	
eMerge package	Suspicious:W32/Malware/DeepGuard.pg	
F1Challenge package	Suspicious:W32/Malware/DeepGuard.pg	
Geburtstagsalarm package	Suspicious:W32/Malware/DeepGuard.pg	
Lazarus package	Suspicious:W32/Malware/DeepGuard.pg	
Maxxpi package	Suspicious:W32/Malware/DeepGuard.pg	
MySermons package	HEUR/APC	
Norton package	Heuristic.HEUR/AGEN.1005063	
POIfinder package	Heuristic.HEUR/AGEN.1030439	
PostTest package	Trojan:W32/Gen4715.8ddc063b2c!Online	
SexyMoment package	Trojan:W32/Generic.34e354aa49!Online	
StartTime package	Suspicious:W32/Malware/DeepGuard.pg	
WinCon package	Suspicious:W32/Malware/DeepGuard.pg	
XWing package	HEUR/APC	


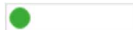
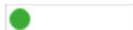

















F-Secure had 17 false alarms.






Symantec Norton

False alarm found in some parts of	Detected as	Supposed prevalence
BlueOffice package	Download Insight	
CheckSig package	Download Insight	
CommView package	Download Insight	
Dallascao package	Heur.AdvML.C	
Datron package	Download Insight	
DialUp package	Download Insight	
ExecuteIt package	Download Insight	
Facil package	Download Insight	
FontInstaller package	Download Insight	
MTG package	Download Insight	
NetCat package	Download Insight	
NSW package	Download Insight	
OpenOffice package	Download Insight	
PDF2print package	Download Insight	
PDFme package	Download Insight	
PSBeratung package	Download Insight	
UCSoftware package	Download Insight	
Website package	Download Insight	
WinCon package	Download Insight	

Symantec Norton had 19 false alarms.





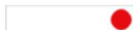
































Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Amok package	Dangerous activity detected	
Bitdefender package	Dangerous activity detected	
CDDVDburning package	Dangerous activity detected	
CheckSig package	DeepScan:Generic.Malware.SVWk!.E825438C	
ClearProg package	Dangerous activity detected	
Ctupdate package	Dangerous activity detected	
eMerge package	Dangerous activity detected	
FileSplitter package	Dangerous activity detected	
Iron package	Dangerous activity detected	
MaxPasswords package	Dangerous activity detected	
Maxxpi package	Dangerous activity detected	
MCF package	Dangerous activity detected	
MultiLauncher package	Dangerous activity detected	
Newsletter package	Dangerous activity detected	
PCW package	VB:Trojan.Emeka.Inor.910	
PDFme package	Dangerous activity detected	
PerfMenu package	Dangerous activity detected	
Picasa package	Dangerous activity detected	
SafeNSec package	Dangerous activity detected	
Settings package	Dangerous activity detected	

SKS package	Dangerous activity detected	
SpeedCommander package	Dangerous activity detected	
UnstopCopy package	Dangerous activity detected	
UOM package	AIT.Downloader.2.Gen	
WinTBS package	Dangerous activity detected	

Tencent had 25 false alarms.

K7













False alarm found in some parts of	Detected as	Supposed prevalence
AddButton package	Riskware (0040eff71)	
Anti-Trojan package	NetWorm (700000151)	
AppTune package	Riskware (0040eff71)	
Ashampoo package	Riskware (0040eff71)	
Avago package	Riskware (0040eff71)	
Broker package	Riskware (0040eff71)	
Ctupdate package	Riskware (0040eff71)	
CustomActions package	Riskware (0040eff71)	
Dallascao package	Riskware (0040eff71)	
Dia package	Trojan (005346f61)	
Ewido package	Riskware (0040eff71)	
F1Challenge package	Riskware (0040eff71)	
Firefox package	Riskware (0040eff71)	
GetIt package	Trojan (005458a71)	
GXTranscoder package	Trojan (004b76a61)	
Harry package	Riskware (0040eff71)	
HarrysFilters package	Riskware (0040eff71)	
Haushaltsbuch package	Riskware (0040eff71)	
HyperDesktop package	Riskware (0040eff71)	
Iron package	Riskware (0040eff71)	
Iw3 package	Riskware (0040eff71)	
Lotus package	Riskware (0040eff71)	
MyWxThing package	NetWorm (700000151)	
Norman package	Trojan (7000000f1)	
OpenOffice package	Trojan (003b1b581)	
Panda package	Riskware (0049f6ae1)	
PDFme package	EmailWorm (004c16271)	
PowerArc package	Riskware (0040eff71)	
Returnil package	Trojan (004906d41)	
SaverInstaller package	Riskware (0040eff71)	
Seulas package	Riskware (0040eff71)	
SimplyZip package	Trojan (7000000f1)	
Spryzip package	Riskware (0040eff71)	
Symantec package	Riskware (0040eff71)	
Teenage package	Riskware (0040eff71)	
Tunguska package	Riskware (0040eff71)	
TurboDebug package	Trojan (00000c9a1)	

TVgenial package	Riskware (0040eff71)	
UnstopCopy package	Riskware (0040eff71)	
WinBeta package	Riskware (0040eff71)	
WinMHT package	Riskware (0040eff71)	
WinPrefetch package	Riskware (0040eff71)	
WinSCP package	Riskware (0040eff71)	
WinXP package	Riskware (0040eff71)	

K7 had 44 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
ADAC package	Suspicious File Blocked	
Almeza package	Suspicious File Blocked	
Anti-Trojan package	Suspicious File Blocked	
ArchiCrypt package	Suspicious File Blocked	
AZFinder package	Suspicious File Blocked	
Bitdefender package	Suspicious File Blocked	
Blinkx package	Suspicious File Blocked	
BlueOffice package	Suspicious File Blocked	
Broker package	Suspicious File Blocked	
CFminibar package	Suspicious File Blocked	
CheckSig package	Suspicious File Blocked	
CleanDisk package	Suspicious File Blocked	
CloneModel package	Suspicious File Blocked	
ComfortUpdater package	Suspicious File Blocked	
CommView package	Suspicious File Blocked	
CompareFolder package	Suspicious File Blocked	
Dallascao package	Suspicious File Blocked	
Datenbankmanager package	Suspicious File Blocked	
Datron package	Suspicious File Blocked	
DialUp package	Suspicious File Blocked	
DriverGenius package	Suspicious File Blocked	
E-Calc package	Suspicious File Blocked	
EKalkulator package	Suspicious File Blocked	
eMerge package	Suspicious File Blocked	
Ewido package	Suspicious File Blocked	
ExecuteIt package	Suspicious File Blocked	
F1Challenge package	Suspicious File Blocked	
Facil package	Suspicious File Blocked	
Falcucci package	Suspicious File Blocked	
Febooti package	Suspicious File Blocked	
FileSplitter package	Suspicious File Blocked	
FileWorks package	Suspicious File Blocked	
GameInst package	Suspicious File Blocked	
Games package	Suspicious File Blocked	
Geburtstagsalarm package	Suspicious File Blocked	

GPI package	Suspicious File Blocked	
Impulsiv package	Suspicious File Blocked	
iPower package	Suspicious File Blocked	
Kaspersky package	Suspicious File Blocked	
Lazarus package	Suspicious File Blocked	
Libro package	Suspicious File Blocked	
LoginControl package	Suspicious File Blocked	
Maxa package	Suspicious File Blocked	
Medizin package	Suspicious File Blocked	
Menue package	Suspicious File Blocked	
MullerEDV package	Suspicious File Blocked	
MySermons package	Suspicious File Blocked	
MyWxThing package	Suspicious File Blocked	
NetCat package	Suspicious File Blocked	
NetOP package	Suspicious File Blocked	
Newsletter package	Suspicious File Blocked	
NSW package	Suspicious File Blocked	
OpenOffice package	Suspicious File Blocked	
Paragon package	Suspicious File Blocked	
PCW package	Suspicious File Blocked	
PDFme package	Suspicious File Blocked	
PerfMenu package	Suspicious File Blocked	
Pidgin package	Suspicious File Blocked	
PodTools package	Suspicious File Blocked	
PrivacyProtect package	Suspicious File Blocked	
PSBeratung package	Suspicious File Blocked	
Reichardt package	Suspicious File Blocked	
Reminder package	Suspicious File Blocked	
SaverInstaller package	Suspicious File Blocked	
ScreenAdjust package	Suspicious File Blocked	
SexyMoment package	Suspicious File Blocked	
SimplyZIP package	Suspicious File Blocked	
SL package	Suspicious File Blocked	
SpamAI package	Suspicious File Blocked	
T2 package	Suspicious File Blocked	
T2S package	Suspicious File Blocked	
UCSoftware package	Suspicious File Blocked	
Unreal package	Suspicious File Blocked	
UOM package	Suspicious File Blocked	
UpdateHelper package	Suspicious File Blocked	
VisualCD package	Suspicious File Blocked	
Webbit package	Suspicious File Blocked	
Website package	Suspicious File Blocked	
WinBeta package	Suspicious File Blocked	
WinnerTweak package	Suspicious File Blocked	
Wistron package	Suspicious File Blocked	

Trend Micro had 81 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
ABSoftware package	Suspicious	
ADAC package	Suspicious	
Almeza package	Suspicious	
Anlagenverbinder package	Suspicious	
Aptajm package	Suspicious	
ArchiCrypt package	Suspicious	
AZFinder package	Suspicious	
Baeume package	Suspicious	
Baywatch package	Suspicious	
Bitdefender package	Suspicious	
Blinkx package	Suspicious	
BlueOffice package	Suspicious	
Cfminibar package	Suspicious	
CheckSig package	Suspicious	
CleanDisk package	Suspicious	
ClearProg package	Suspicious	
CloneModel package	Suspicious	
ComfortUpdater package	Suspicious	
CommView package	Suspicious	
Ctupdate package	Suspicious	
Datenbankmanager package	Suspicious	
Datron package	Suspicious	
DialUp package	Suspicious	
Doppeldecker package	Suspicious	
DriverGenius package	Suspicious	
E-Calc package	Suspicious	
EDA package	Suspicious	
eMerge package	Suspicious	
Encryption package	Suspicious	
F1Challenge package	Suspicious	
Facil package	Suspicious	
Falcucci package	Suspicious	
Febooti package	Suspicious	
Files package	Suspicious	
FileSplitter package	Suspicious	
Freshdow package	Suspicious	
Games package	Suspicious	
Geburtstagsalarm package	Suspicious	
GPI package	Suspicious	
HyperDesktop package	Suspicious	
InstantOn package	Suspicious	
iPower package	Suspicious	
ITpro package	Suspicious	
Kaspersky package	Suspicious	

Lazarus package	Unknown name	
Libro package	Suspicious	
Logik package	Suspicious	
Macromedia package	Suspicious	
MailGuard package	Suspicious	
MailOut package	Suspicious	
Maxxpi package	Suspicious	
MeldeMax package	Malicious Packer	
MemZilla package	Suspicious	
MTG package	Suspicious	
MyWxThing package	Suspicious	
NetCat package	Suspicious	
NetOP package	Suspicious	
NSW package	Suspicious	
OpenOffice package	Suspicious	
OutlookTuner package	Suspicious	
PaperOffice package	Suspicious	
Paquet package	Suspicious	
PCW package	Suspicious	
PDFme package	Suspicious	
PerfektChicken package	Suspicious	
PerfMenu package	Suspicious	
PEview package	Suspicious	
Pipedown package	Suspicious	
PodTools package	Suspicious	
PostTest package	Suspicious	
PowerArc package	Suspicious	
PrivacyProtect package	Suspicious	
PSBeratung package	Suspicious	
Reichardt package	Suspicious	
Restore package	Suspicious	
RTFtoHTML package	Suspicious	
SaverInstaller package	Suspicious	
ScreenAdjust package	Suspicious	
Settings package	Suspicious	
ShootingRange package	Suspicious	
SlipStreamer package	Suspicious	
SnailGame package	Suspicious	
SpamAI package	Suspicious	
T2 package	Suspicious	
Tiscali package	Trj/CI.A	
TKKG package	Suspicious	
UCSoftware package	Suspicious	
Webbit package	Suspicious	
WinnerTweak package	Suspicious	
YAW package	Suspicious	

Panda had 90 false alarms.

Copyright and Disclaimer

This publication is Copyright © 2019 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 2019)