

Details of False Alarms



Appendix to the Anti-Virus Comparative March 2017

Language: English

March 2017

Last Revision: 14th April 2017


www.av-comparatives.org



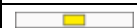
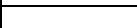

Details of false alarms

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. 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"). 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, unknown 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 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.

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 old 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 cause an FP again on a more significant file. Thus, they still deserve mention and still deserve to be penalised. Below you will find the false alarms we observed in our independent set of clean files. Red entries highlight false alarms on files that were digitally signed.



ESET and **Microsoft** had zero false alarms on the used set of clean files.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
SafeNSec package	Trj/CI.A	



Panda had 1 false alarm.

Adaware

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	Gen:Variant.Symmi.71281	
XFire package	Gen:Variant.Razy.95563	



Adaware had 2 false alarms.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	Gen:Variant.Symmi.71281	
XFire package	Gen:Variant.Razy.95563	



Bitdefender had 2 false alarms.

eScan

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	Gen:Variant.Symmi.71281 (DB)	
XFire package	Gen:Variant.Razy.95563 (DB)	




eScan had 2 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
AutoIt package	TR/SelfDel.hvov Trojan	
Vuex package	HEUR/APC (Cloud)	




AVIRA had 2 false alarms.

BullGuard

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	Gen:Variant.Symmi.71281	
SevenRemix package	Trojan.NSIS.Androm.3	
XFire package	Gen:Variant.Razy.95563	




BullGuard had 3 false alarms.

Seqrite

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	EE:Malwr.Heur.Symmi.71281	
SevenRemix package	EE:Trojan.NSIS.Androm.3	
XFire package	EE:Malwr.Heur.Razy.95563	




Seqrite had 3 false alarms.

Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	Gen:Variant.Symmi.71281	
SevenRemix package	Trojan.NSIS.Androm.3	
XFire package	Gen:Variant.Razy.95563	





Tencent had 3 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
PDFexperte package	Gen:Variant.Symmi.71281	
SevenRemix package	Trojan.NSIS.Androm.3	
XFire package	Gen:Variant.Razy.95563	





VIPRE had 3 false alarms.

Emsisoft

False alarm found in some parts of	Detected as	Supposed prevalence
GXTranscoder package	Trojan.Generic.7464985 (B)	
OrangeGem package	Trojan.Sinowal.Gen.1 (B)	
PDFExperte package	Gen:Variant.Symmi.71281 (B)	
XFire package	Gen:Variant.Razy.95563 (B)	





Emsisoft had 4 false alarms.

Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
AVG package	Trojan.Win32.Gofot.fch	
Clipboard package	Trojan-Dropper.Win32.Dapato.olhj	
FiveWin package	UDS:DangerousObject.Multi.Generic	
KonfKit package	Trojan-Dropper.Win32.Agent.bjsczl	







Kaspersky Lab had 4 false alarms.

Fortinet

False alarm found in some parts of	Detected as	Supposed prevalence
FileViewer package	PossibleThreat.SB	
Matrox package	PossibleThreat.SB	
PaperOffice package	W32/Injector.CVRZ!tr	
Tram package	W32/Bouiben.OLE!tr	






Fortinet had 4 false alarms.





F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
Frisk package	Trojan:W32/Gen4135.984577c56d!Online	
GXTranscoder package	Trojan.Generic.7464985	
OrangeGem package	Trojan.Sinowal.Gen.1	
PDFExperte package	Gen:Variant.Symmi.71281	
SevenRemix package	Trojan.NSIS.Androm.3	
XFire package	Gen:Variant.Razy.95563	

F-Secure had 6 false alarms.











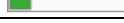




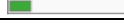

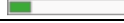


McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
ALZip package	Artemis!21095C3ECA72	
CyberLink package	Artemis!45A71AA1FD0A	
GameAccelerator package	Artemis!E05D6ECAC7EC	
Komfort package	GenericRXAV-IV!87E29BAC562F	
PCWizard package	Artemis!D9ED2981F363	

Shanghai package	GenericRXAS-FB!6DF44A88D27C	
TheSettlers package	Artemis!32C50B75BE89	
ToolLoader package	Artemis!D80D89C8AFCB	
Tris package	Artemis!1AB75BD08E97	









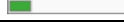

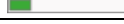


McAfee had 9 false alarms.

Avast

False alarm found in some parts of	Detected as	Supposed prevalence
AON package	Win32:DH-A1	
Apfelman package	Win32:Malware-gen	
ASUS package	Win32:DH-A1	
Ausfuellen package	FileRepMalware	
Browster package	Win32:DH-A1	
Deenes package	Win32:DH-A1	
EasyPAK package	Win32:Evo-gen	
F-Secure package	Win32:DH-A1	
GMER package	Win32:DH-A1	
Google package	Win32:DH-A1	
Horse package	Win32:Evo-gen	
HP package	Win32:DH-A1	
Kaffeepause package	Win32:DH-A1	
Kicker package	Win32:DH-A1	
NetInfo package	Win32:Evo-gen	
OpenOffice package	Win32:Evo-gen	
Puzzle package	Win32:DH-A1	
SunBird package	Win32:Evo-gen	
WinAmp package	Win32:Evo-gen	
XPburn package	Win32:DH-A1	

Avast had 20 false alarms.

AVG

False alarm found in some parts of	Detected as	Supposed prevalence
AON package	Win32:DH-A1	
Apfelman package	Win32:Malware-gen	
ASUS package	Win32:DH-A1	
Ausfuellen package	FileRepMalware	
Browster package	Win32:DH-A1	
Deenes package	Win32:DH-A1	
EasyPAK package	Win32:Evo-gen	
F-Secure package	Win32:DH-A1	
GMER package	Win32:DH-A1	
Google package	Win32:DH-A1	
Horse package	Win32:Evo-gen	
HP package	Win32:DH-A1	
Kaffeepause package	Win32:DH-A1	

Kicker package	Win32:DH-A1	
NetInfo package	Win32:Evo-gen	
OpenOffice package	Win32:Evo-gen	
Puzzle package	Win32:DH-A1	
SunBird package	Win32:Evo-gen	
WinAmp package	Win32:Evo-gen	
XPburn package	Win32:DH-A1	

AVG had 20 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Adobe package	Suspicious File	
Bluefish package	Suspicious File	
Busch package	Suspicious File	
ClearProg package	Suspicious File	
ClikcMedia package	Suspicious File	
Core2Max package	Suspicious File	
Deeenes package	Suspicious File	
FireStorm package	Suspicious File	
FiveWin package	Suspicious File	
Floppy package	Suspicious File	
FreeSpa package	Suspicious File	
Frisk package	Suspicious File	
F-Secure package	Suspicious File	
GMER package	Suspicious File	
Grub2Win package	Suspicious File	
GXTranscoder package	Suspicious File	
IconHider package	Suspicious File	
Kalenderpack package	Suspicious File	
Opera package	Suspicious File	
Puzzle package	Suspicious File	
RegBrowser package	Suspicious File	
RegCool package	Suspicious File	
TennisMaster package	Suspicious File	
ToolLoader package	Suspicious File	
Tram package	Suspicious File	
Tris package	Suspicious File	
VistaMizer package	Suspicious File	
XFire package	Suspicious File	
Zup package	Suspicious File	

Trend Micro had 29 false alarms.

Symantec Norton







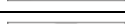
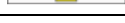
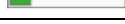









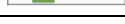








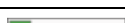

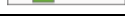


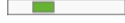





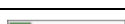

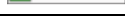
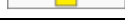





False alarm found in some parts of	Detected as	Supposed prevalence
3Dtweak package	Suspicious.Epi.3	

AAMS package	Suspicious.Epi.3	
ActivePixels package	Suspicious.Epi.3	
Amok package	Infostealer.Gampass	
AppStarter package	Trojan.Gen.8	
ASuite package	Suspicious.Epi.3	
AutoHotKey package	Suspicious.Epi.3	
AverTV package	Suspicious.Epi.3	
BOM package	Heur.AdvML.C	
CallSearch package	Suspicious.Epi.3	
CamStudio package	Suspicious.Epi.3	
ClearProg package	Suspicious.Epi.3	
ClickClean package	Suspicious.Epi.3	
Clickster package	Suspicious.Epi.3	
Clipboard package	Suspicious.Epi.3	
CopyToDV package	Suspicious.Epi.3	
Daphne package	Suspicious.Epi.3	
DateiCommander package	Suspicious.Epi.3	
Datenabgleich package	Suspicious.Epi.3	
DisableWinTracking package	Heur.AdvML.C	
Disconnect package	Suspicious.Epi.3	
DiskCleaner package	Suspicious.Epi.3	
DriveScan package	Suspicious.Epi.3	
DVdisaster package	Suspicious.Epi.3	
Ewido package	Trojan.ADH.2	
FileSync package	Heur.AdvML.C	
FinalBurner package	Suspicious.Epi.3	
FinePrint package	Suspicious.Epi.3	
Floppy package	Suspicious.Epi.3	
FreeCommander package	Suspicious.Epi.3	
FreshDow package	Suspicious.Epi.3	
FreshUI package	Suspicious.Epi.3	
GigaByte package	SAPE.Heur.B96DB	
GrabIt package	Suspicious.Epi.3	
GrandPrix package	Suspicious.Epi.3	
GXTranscoder package	Suspicious.Epi.3	
HTMLdoc package	Suspicious.Epi.3	
Hugin package	Suspicious.Epi.3	
HyperSnap package	SAPE.Heur.38b4	
IconHider package	Suspicious.Epi.3	
Imagine package	Suspicious.Epi.3	
InfraRecorder package	Suspicious.Epi.3	
Jpegr package	Suspicious.Epi.3	
Kaspersky package	Trojan.Tooso!gen	
Kismet package	Suspicious.Epi.3	
Koolader package	Suspicious.Epi.3	
MediaInfo package	Suspicious.Epi.3	
MegaCamManager package	Suspicious.Epi.3	
Megui package	Suspicious.Epi.3	
MouseButton package	Suspicious.Epi.3	
Mozilla package	Suspicious.Epi.3	

MultiStage package	Suspicious.Epi.3	
PeaZip package	Suspicious.Epi.3	
PhotoMatix package	Suspicious.Epi.3	
PingPlotter package	Suspicious.Epi.3	
Polarr package	SAPE.Heur.8D331	
QuizPro package	Suspicious.Epi.3	
RainMeter package	Heur.AdvML.C	
RegBrowser package	Suspicious.Epi.3	
RegCool package	Suspicious.Cloud.2.A	
RegistryFirstAid package	Infostealer.Gampass	
RestoreNatur package	Trojan.Gen.2	
Sandboxie package	Suspicious.Epi.3	
Screamer package	Suspicious.Epi.3	
ScreenshotCaptor package	Suspicious.Epi.3	
SevenRemix package	Suspicious.Epi.3	
Shutdown package	Suspicious.Epi.3	
SimplyZip package	Infostealer.Gampass	
SmartMorph package	Suspicious.Epi.3	
Snowflakes package	Suspicious.Epi.3	
SSC package	Suspicious.Epi.3	
StationRipper package	Suspicious.Epi.3	
Sylpheed package	Suspicious.Epi.3	
Tagscan package	Suspicious.Epi.3	
TeraCopy package	Suspicious.Epi.3	
TheBestMovie package	Suspicious.Epi.3	
Tintii package	Heur.AdvML.C	
TweakPower package	Heur.AdvML.C	
USBwatcher package	Suspicious.Epi.3	
VHDattach package	Suspicious.Epi.3	
VideoInspector package	Suspicious.Epi.3	
VirtualMoon package	Suspicious.Epi.3	
VistaMizer package	Suspicious.Cloud.2.A	
VistaServices package	Suspicious.Epi.3	
VisualTask package	Suspicious.Epi.3	
Vundofix package	Suspicious.Cloud.9.B	
WinAmp package	Suspicious.Epi.3	
Winboard package	Suspicious.Epi.3	
WindowHiding package	Trojan.Gen.8	
WinPlus package	Suspicious.Epi.3	
WinRAR package	Suspicious.Epi.3	
WiseDiskCleaner package	Suspicious.Epi.3	
XBbrowser package	Heur.AdvML.C	
Xenu package	Suspicious.Epi.3	
XPprome package	Suspicious.Epi.3	
Zar package	Suspicious.Epi.3	

Symantec Norton had 96 false alarms. Symantec is a new re-entry in our tests – it is to be expected that their number of false alarms will be much lower next time.

CrowdStrike

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	High (Activity Prevented)	
Adobe package	High (Activity Prevented)	
AmericanConquest package	High (Activity Prevented)	
AncientSpider package	High (Activity Prevented)	
ASUS package	High (Activity Prevented)	
AutoFlowChart package	High (Activity Prevented)	
BigFish package	High (Activity Prevented)	
BIMexplorer package	High (Activity Prevented)	
BloodRayne package	High (Activity Prevented)	
BlueFish package	High (Activity Prevented)	
BrainTwister package	High (Activity Prevented)	
Busch package	High (Activity Prevented)	
CDSearch package	High (Activity Prevented)	
ClickMedia package	High (Activity Prevented)	
CloneDVD package	High (Activity Prevented)	
Cobra11 package	High (Activity Prevented)	
Compare package	High (Activity Prevented)	
Comtest package	High (Activity Prevented)	
Core2Max package	High (Activity Prevented)	
Daemon package	High (Activity Prevented)	
Databecker package	High (Activity Prevented)	
DataNation package	High (Activity Prevented)	
DeltaForce package	High (Activity Prevented)	
DiaShow package	High (Activity Prevented)	
DieSiedler package	High (Activity Prevented)	
DTB package	High (Activity Prevented)	
Duden package	High (Activity Prevented)	
EasyBurning package	High (Activity Prevented)	
EmailPro package	High (Activity Prevented)	
eMedia package	High (Activity Prevented)	
eRightSoft package	High (Activity Prevented)	
ESET package	High (Activity Prevented)	
ESreg package	High (Activity Prevented)	
EuroRechner package	High (Activity Prevented)	
FileTime package	High (Activity Prevented)	
Findus package	High (Activity Prevented)	
FireStorm package	High (Activity Prevented)	
Flyakite package	High (Activity Prevented)	
Fotofit package	High (Activity Prevented)	
Fotograf package	High (Activity Prevented)	
FreeCrypt package	High (Activity Prevented)	
FreeSpa package	High (Activity Prevented)	
FTCheck package	High (Activity Prevented)	
Fujitsu package	High (Activity Prevented)	
FunnyMemo package	High (Activity Prevented)	
GoogleClean package	High (Activity Prevented)	
Groove package	High (Activity Prevented)	

Grub2Win package	High (Activity Prevented)	
Harrys package	High (Activity Prevented)	
HDCleaner package	High (Activity Prevented)	
Helper package	High (Activity Prevented)	
Horseshoe package	High (Activity Prevented)	
HP package	High (Activity Prevented)	
HPV package	High (Activity Prevented)	
IceAge package	High (Activity Prevented)	
IconXtractor package	High (Activity Prevented)	
IDman package	High (Activity Prevented)	
IMG package	High (Activity Prevented)	
ImperialGlory package	High (Activity Prevented)	
InstallShield package	High (Activity Prevented)	
JoWood package	High (Activity Prevented)	
Kalenderpack package	High (Activity Prevented)	
Kao package	High (Activity Prevented)	
Keller package	High (Activity Prevented)	
Kreed package	High (Activity Prevented)	
Lexikon package	High (Activity Prevented)	
Loop package	High (Activity Prevented)	
MathCAD package	High (Activity Prevented)	
Maulwurf package	High (Activity Prevented)	
Miui package	High (Activity Prevented)	
Moorhuhn package	High (Activity Prevented)	
MPBrowser package	High (Activity Prevented)	
MSI package	High (Activity Prevented)	
MusicMaker package	High (Activity Prevented)	
Nero package	High (Activity Prevented)	
NetPing package	High (Activity Prevented)	
NNG package	High (Activity Prevented)	
Nokia package	High (Activity Prevented)	
OOBE package	High (Activity Prevented)	
Opera package	High (Activity Prevented)	
Othello package	High (Activity Prevented)	
OutlookTuner package	High (Activity Prevented)	
PartyGaming package	High (Activity Prevented)	
PCG package	High (Activity Prevented)	
PerfWatch package	High (Activity Prevented)	
Printy package	High (Activity Prevented)	
Raetsel package	High (Activity Prevented)	
RAMid package	High (Activity Prevented)	
RegCool package	High (Activity Prevented)	
RegSnap package	High (Activity Prevented)	
RegToy package	High (Activity Prevented)	
RSW package	High (Activity Prevented)	
Sidebar package	High (Activity Prevented)	
Simkl package	High (Activity Prevented)	
SkiRacing package	High (Activity Prevented)	

StartDelay package	High (Activity Prevented)	
StyleSelector package	High (Activity Prevented)	
Sudoku package	High (Activity Prevented)	
TagesAnzeiger package	High (Activity Prevented)	
Tankwart package	High (Activity Prevented)	
TennisMasters package	High (Activity Prevented)	
Texiterator package	High (Activity Prevented)	
Tierpension package	High (Activity Prevented)	
TrackWin package	High (Activity Prevented)	
TrendMicro package	High (Activity Prevented)	
TrueCrypt package	High (Activity Prevented)	
TweakNow package	High (Activity Prevented)	
TweakPower package	High (Activity Prevented)	
UltimateSudoku package	High (Activity Prevented)	
Uniextract package	High (Activity Prevented)	
Unitype package	High (Activity Prevented)	
Unreal package	High (Activity Prevented)	
USBagent package	High (Activity Prevented)	
Wanyawoord package	High (Activity Prevented)	
Warcraft package	High (Activity Prevented)	
WesternDigital package	High (Activity Prevented)	
WildlifePark package	High (Activity Prevented)	
Wildtangent package	High (Activity Prevented)	
WinAmp package	High (Activity Prevented)	
WinDVD package	High (Activity Prevented)	
WinSecurityGate package	High (Activity Prevented)	
Withopf package	High (Activity Prevented)	
Wobram package	High (Activity Prevented)	
Zup package	High (Activity Prevented)	
zWetter package	High (Activity Prevented)	

CrowdStrike had 125 false alarms. Please note that CrowdStrike Falcon Prevent is a product made for corporate users. Many of the FP's encountered in this test would not cause a big problem in such an environment; for example, several of them are game-related files which would not be allowed in a corporate network anyway. CrowdStrike is also a new entry in our tests - it is to be expected that their number of false alarms will be much lower next time.

Copyright and Disclaimer

This publication is Copyright © 2017 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 2017)