Independent Tests of
Anti-Virus Software

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD:	SEPTEMBER 2020
LANGUAGE:	ENGLISH
LAST REVISION:	12TH OCTOBER 2020

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 3 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 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".

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
ComfortUpdater package	MSIL/TrojanDropper.Agent.AYP.Gen trojan	🟢
UnitedPlanet package	a variant of Win32/Injector.BNGG trojan	🟢

ESET had 2 false alarms.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
CheckSig package	HEUR:Trojan-Ransom.Win32.Gen.gen	🟢
ESET package	Trojan.Win32.Staser.coah	🔴
SwiftSwing package	HEUR:Trojan.Win32.Generic	🟢

Kaspersky had 3 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Boot package	Blocked	🟢
ESET package	TROJ_GEN.R002C0DFB20	🔴
Opera package	Blocked	🟢
Preme package	Blocked	🟢
Swiftswing package	TROJ_GEN.R03BC0WH820	🟢

Trend Micro had 5 false alarm.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
AutoDarkMode package	Blocked	🟢
CenterMail package	Gen:Variant.Ursu.813676	🟢
Delphi package	Trojan.GenericKD.33569199	🟢
Lucent package	Blocked	🟢
TrialReminder package	Blocked	🟢
Warner package	Blocked	🟢

Bitdefender had 6 false alarms.

G DATA

False alarm found in some parts of	Detected as	Supposed prevalence
AutoKMV package	Blocked	🟡
CenterMail package	Gen:Variant.Ursu.813676	🟢
DHTPC package	Gen:Variant.Ursu.728736	🟢
ESET package	Blocked	🔴
Howard package	Blocked	🟢
VideoRescue package	Gen:Variant.Jacard.167275	🟢

G DATA had 6 false alarms.

Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
CenterMail package	Gen:Variant.Ursu.813676	🟢
Delphi package	Trojan.GenericKD.33569199	🟢
DWSIM package	Blocked	🟢
Fujitsu package	Blocked	🟢
GeniusConnect package	Blocked	🟢
TrialReminder package	Blocked	🟢

Total Defense had 6 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
DamnNation package	HEUR/APC	🟢
Delphi package	HEUR/APC	🟢
DuplicateFinder package	HEUR/APC	🟢
ESET package	TR/Muldrop.whnqj	🔴
GuessTheNumber package	HEUR/APC	🟢
Milo package	HEUR/APC	🟡
Swiftswing package	HEUR/AGEN.1133632	🟢
WinUAE package	TR/AD.NsisInject.kaouc	🟢

AVIRA had 8 false alarms.

Total AV

False alarm found in some parts of	Detected as	Supposed prevalence
DamnNation package	HEUR/APC	🟢
Delphi package	HEUR/APC	🟢
DuplicateFinder package	HEUR/APC	🟢
ESET package	TR/Muldrop.whnqj	🔴
GuessTheNumber package	HEUR/APC	🟢
Milo package	HEUR/APC	🟡
Swiftswing package	HEUR/AGEN.1133632	🟢
WinUAE package	TR/AD.NsisInject.kaouc	🟢

Total AV had 8 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
DamnNation package	Blocked	🟢
ESET package	TR/Muldrop.whnqj	🔴
Glace package	Blocked	🟢
GuessTheNumber package	Blocked	🟢

ProcX package	Blocked	🔴
Samurize package	Trojan-Downloader:JS/TeslaCrypt.C	🟢
SwiftSwing package	Heuristic.HEUR/AGEN.1133632	🟢
Warner package	Blocked	🟢
WinUAE package	Trojan.TR/AD.NsisInject.kaouc	🟢

F-Secure had 9 false alarms.

Avast / AVG

False alarm found in some parts of	Detected as	Supposed prevalence
Dateicommander package	Win32:Malware-gen	🟢
Delphi package	Win32:Malware-gen	🟢
Diel package	FileRepMalware	🟢
ESET package	Win32:Malware-gen	🔴
Kotato package	Blocked	🟢
Opera package	FileRepMalware	🟢
Pharmacy package	Blocked	🟢
PNotes package	FileRepMalware	🟢
SafeErase package	FileRepMalware	🟢
SwiftSwing package	Win32:Malware-gen	🟢

Avast and AVG had 10 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
AvancePaint package	JTI/Suspect.196612!255d333c6dd1	🟢
CleanGP package	Blocked	🟢
Delphi package	JTI/Suspect.196612!3a288ba63e64	🟢
ESET package	JTI/Suspect.196612!3dd5d756b80e	🔴
MemReduct package	JTI/Suspect.196612!25db35058f16	🔴
Opera package	JTI/Suspect.196612!bc5289917846	🟢
PCW package	JTI/Suspect.196612!325b8510ae22	🟢
SipGate package	JTI/Suspect.196612!4c44a4935628	🟢
Spectrum package	JTI/Suspect.196612!cf7f1be6ee8a	🔴
SwiftSwing package	JTI/Suspect.196612!1cc75a72a223	🟢

McAfee had 10 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
7zip package	Blocked	🟢
AmericanConquest package	Blocked	🟡
Aukcji package	Blocked	🟢
AvancePaint package	Blocked	🟢
Bandit package	Blocked	🟢
Boo package	Blocked	🟡
DamnNation package	Blocked	🟢
Delphi package	Blocked	🟢
ESET package	Trojan:Win32/Esulat.A!rfn	🔴
FourthRay package	Blocked	🟢
HelpVideo package	Blocked	🟢
Image2PDF package	Blocked	🟢
JetBrains package	Blocked	🟢
Lottoziehung package	Blocked	🟢
Opera package	Blocked	🟢
QuickKey package	TrojanDownloader:Win32/Upatre	🟢
Swiftswing package	Trojan:Win32/Wacatac.D6!ml	🟢
Syncios package	Blocked	🟡
Unity package	Blocked	🟡
WinPIM package	Blocked	🟢
YTdownloader package	Blocked	🔴

Microsoft had 21 false alarms.

Vipre

False alarm found in some parts of	Detected as	Supposed prevalence
Assist package	Blocked	🟢
AutoDarkMode package	Blocked	🟢
CashTallyOne package	Blocked	🟢
CenterMail package	Gen:Variant.Ursu.813676	🟢
DiagramDesigner package	Gen:Variant.Jacard.192711	🟢
DWSIM package	Blocked	🟢
GIFmaker package	Blocked	🟢
GTA package	Blocked	🟢
JumpingBytes package	Blocked	🟢
Lucent package	Blocked	🟢
NetworkChat package	Gen:Trojan.Heur.EKY@Y23uNvn	🟢
PCW package	Gen:Variant.Ursu.784989	🟢

Preme package	Blocked	🟢
Transitions package	Blocked	🟢
TrialReminder package	Blocked	🟢
VideoRescue package	Gen:Variant.Jacard.167275	🟢
Warner package	Blocked	🟢
WinPIM package	Blocked	🟢

Vipre had 18 false alarms.

NortonLifeLock

False alarm found in some parts of	Detected as	Supposed prevalence
AutoMKV package	Heur.AdvML.C	🟡
AvancePaint package	Suspicious.Epi.3	🟢
Bonkenc package	Heur.AdvML.B	🟢
Boot package	Suspicious.Epi.3	🟢
BrothersinArms package	Heur.AdvML.C	🟢
Calendars package	Suspicious.Epi.3	🟢
CarJacker package	Suspicious.Epi.3	🟢
CleanGP package	Suspicious.Epi.3	🟢
Delphi package	Trojan.Gen.2	🟢
Deskman package	Suspicious.Epi.3	🟢
DeusEx package	Heur.AdvML.C	🟢
Dimio package	Suspicious.Epi.3	🟢
DirectX package	Suspicious.Epi.3	🔴
Dooble package	Suspicious.Epi.3	🟢
Dowcip package	Suspicious.Epi.3	🟢
Earth2160 package	Suspicious.Epi.3	🟡
Easo package	Suspicious.Epi.3	🔴
EvilPlayer package	Heur.AdvML.B	🔴
FastHide package	Suspicious.Epi.3	🟡
GTA package	Heur.AdvML.C	🟢
Hardcopy package	Suspicious.Epi.3	🟢
Konwerter package	Suspicious.Epi.3	🟡
Lame package	Suspicious.Epi.3	🟢
MacAddress package	Heur.AdvML.B	🟡
MySermons package	Suspicious.Epi.3	🟢
NetworkFile package	Heur.AdvML.A	🟢
NPython package	Heur.AdvML.B	🟢
Reaper package	Heur.AdvML.C	🟢
RegDefrag package	Heur.AdvML.B	🟢

RMCA package	Suspicious.Epi.3	🟢
Serwer package	Heur.AdvML.C	🟢
SipGate package	Heur.AdvML.C	🟢
Swiftswing package	Heur.AdvML.C	🟢
Syspad package	Suspicious.Epi.3	🟢
Tawerna package	Heur.AdvML.C	🟢
TerminPlaner package	Heur.AdvML.B	🟢
TrafficMonitor package	Heur.AdvML.B	🟢
Warner package	Heur.AdvML.B	🟢
Wesnoth package	Suspicious.Epi.3	🟢
XiceCube package	Suspicious.Epi.3	🟢
Xion package	Trojan.Gen.2	🟠

NortonLifeLock had 41 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
AdiIRC package	Blocked	🟢
AirExplorer package	Blocked	🟡
Alice package	Blocked	🟡
Alternate package	Blocked	🟢
AmericanConquest package	is a Riskware (0040eff71)	🟡
Ascora package	Blocked	🟠
Autodesk package	is a Riskware (0049f6ae1)	🔴
AvancePaint package	Blocked	🟢
AVG package	is a Riskware (0040eff71)	🟠
BearShare package	is a Riskware (0040eff71)	🔴
BenQ package	is a Riskware (0040eff71)	🔴
BestAddress package	Blocked	🟢
Binaeruhr package	Blocked	🟢
BlueSky package	Blocked	🟢
BonBon package	Blocked	🟡
Citrix package	Blocked	🔴
CleanGP package	Blocked	🟢
ComfortUpdater package	Blocked	🟢
Comix package	Blocked	🟢
CompuGroup package	Blocked	🟢
CPUid package	Blocked	🔴
Dateicommander package	Blocked	🟢
DeDupler package	Blocked	🟡

Delphi package	Blocked	🟢
Deskman package	Blocked	🟢
DeusEx package	Blocked	🟢
DHTPC package	Blocked	🟢
DWSIM package	Blocked	🟢
eMerge package	Blocked	🟢
EnWeb package	Blocked	🟢
ESET package	is a Riskware (0040eff71)	🟠
HelpVideo package	Blocked	🟢
Image2PDF package	Blocked	🟢
Indigo package	Blocked	🟢
Innovative package	Blocked	🟠
Inventor package	is a Riskware (0040eff71)	🔴
JetBrains package	Blocked	🟡
Kartell package	is a Riskware (0040eff71)	🟢
LeaderTask package	Blocked	🟡
LmByte package	Blocked	🟢
M2T package	Blocked	🟢
MacAddress package	Blocked	🟡
MailBird package	Blocked	🟢
Manager package	Blocked	🟢
MetaTogger package	Blocked	🟢
Mozilla package	Blocked	🟢
MSN package	Blocked	🟡
MultiCore package	Blocked	🔴
MuteMe package	Blocked	🟢
MySermons package	Blocked	🟢
Nobu package	Blocked	🔴
NX package	Blocked	🟢
PCessentials package	is a Riskware (0040eff71)	🟠
PCW package	Blocked	🟢
PDFviewer package	Blocked	🟢
Playnite package	Blocked	🟡
Preme package	Blocked	🟢
QuickPicture package	Blocked	🟢
RegDefrag package	Blocked	🟢
RemoteMouse package	Blocked	🟢
RMCA package	Blocked	🟢
SafeInCloud package	Blocked	🟡

SAR package	is a Trojan (003b1b581)	🟢
Serwer package	Blocked	🟢
SharpKeys package	Blocked	🟢
Sordum package	Blocked	🟡
SQL package	Blocked	🟢
Symantec package	is a Riskware (004bbad11)	🔴
Thundersave package	Blocked	🟡
UltraViewer package	Blocked	🔴
UnstopCopy package	is a Riskware (0040eff71)	🟠
Warner package	Blocked	🟡
Webroot package	Blocked	🟡
Wesnoth package	Blocked	🟢
Wetterfroschi package	Blocked	🟢
WinGuard package	Blocked	🟡
WPD package	Blocked	🟡
YTdownloader package	Blocked	🟠

K7 had 78 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
7zip package	Blocked	🟢
Abacre package	Blocked	🟢
AdiIRC package	Blocked	🟢
AmericanConquest package	Trj/Swizzor.S	🟡
Apache package	Blocked	🟢
Argon package	Blocked	🟢
ArtMoney package	Blocked	🟢
Assembly package	Blocked	🟡
Assist package	Blocked	🟢
Assistant package	Blocked	🟢
AudioSplit package	Blocked	🟢
Aukcji package	Blocked	🟢
Barcode package	Blocked	🟢
BestAddress package	Blocked	🟢
Bestellbuch package	Blocked	🟢
BlueSky package	Blocked	🟢
BluRay package	Blocked	🟢
BMS package	Blocked	🟢
BonBon package	Blocked	🟡

Boo package	Blocked	🟡
BookReader package	Blocked	🟢
BrightFort package	Blocked	🔴
BrothersInArms package	Blocked	🟢
Calendars package	Blocked	🟢
CaptureFile package	Blocked	🟢
CDrunner package	Blocked	🟢
CharView package	Blocked	🟢
CheckSig package	Blocked	🟢
ClipFinder package	Blocked	🟡
CloneAP package	Blocked	🟢
CompuGroup package	Blocked	🟢
DamnNation package	Blocked	🟢
Delphi package	Blocked	🟢
DeusEx package	Blocked	🟢
Diel package	Blocked	🟢
DirMonitor package	Blocked	🟢
DWSIM package	Blocked	🟢
Easo package	Trj/CI.A	🔴
EasyCode package	Blocked	🟢
Emma package	Blocked	🟢
ESET package	Blocked	🔴
FairStars package	Blocked	🟢
FFVPN package	Blocked	🟢
FlashPeak package	Blocked	🟢
FMOD package	Trj/Genetic.gen	🟢
FourthRay package	Blocked	🟢
FreeGifMaker package	Blocked	🟢
Gemini package	Blocked	🟢
GeniusConnect package	Blocked	🟢
GetText package	Blocked	🟢
GifMaker package	Blocked	🟢
Glace package	Trj/CI.A	🟢
Howard package	Blocked	🟢
Image2PDF package	Blocked	🟢
ImageList package	Blocked	🟢
JumpingBytes package	Blocked	🟢
LmByte package	Blocked	🟢
LottoExperte package	Blocked	🟢

Lottoziehung package	Blocked	🟢
MailEnable package	Blocked	🟢
MedXpert package	Blocked	🟢
Merge package	Blocked	🟢
MetaTogger package	Blocked	🟢
MikTeX package	Blocked	🟢
Monkey package	Blocked	🟢
Monolinker package	Blocked	🟡
Mozilla package	Blocked	🟢
MySermons package	Blocked	🟢
NetServer package	Blocked	🟢
NPython package	Blocked	🟢
Opera package	Blocked	🟢
OrangeCD package	Blocked	🟢
PathToCopy package	Blocked	🟢
PCAP package	Blocked	🟢
PCinfo package	Blocked	🟢
PCW package	Blocked	🟢
PDFwatermark package	Blocked	🟢
PersonalBackup package	Blocked	🟢
Playnite package	Blocked	🟡
PNotes package	Blocked	🟢
Python package	Blocked	🟢
QT package	Blocked	🟡
QuickKey package	Blocked	🟢
QuickPicture package	Blocked	🟢
Ravensburger package	Blocked	🟢
Rooster package	Blocked	🟢
RoverData package	Blocked	🟢
SAM package	Blocked	🟢
SDL package	Blocked	🟡
Serwer package	Blocked	🟢
SibCode package	Blocked	🟢
SipGate package	Blocked	🟢
Slideshow package	Blocked	🟢
Snapshot package	Blocked	🟢
SoftDeluxe package	Blocked	🟢
SQL package	Blocked	🟢
Swiftswing package	Blocked	🟢

SyntaxEditor package	Blocked	🟢
SysRestore package	Blocked	🟢
TapinRadio package	Blocked	🟢
Tomabo package	Blocked	🟢
Transitions package	Blocked	🟢
TrialReminder package	Blocked	🟢
TryCast package	Blocked	🟢
TVtunner package	Blocked	🟢
UnitedPlanet package	Blocked	🟢
Unity package	Blocked	🟡
USBsuite package	Blocked	🟢
VideoRescue package	Blocked	🟢
VLC package	Blocked	🟢
WinPIM package	Blocked	🟢
WinRAR package	Trj/Genetic.gen	🔴
XiceCube package	Blocked	🟢
YTdownloader package	Blocked	🟢

Panda had 114 false alarms.

Copyright and Disclaimer

This publication is Copyright © 2020 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 2020)