Independent Tests of
Anti-Virus Software

Details of False Alarms

Appendix to the Malware Protection Test

TEST PERIOD:	SEPTEMBER 2019
LANGUAGE:	ENGLISH
LAST REVISION:	14TH OCTOBER 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. 20 FPs and another only 3, it is likely that the first product is more prone to FPs than the other. It doesn't mean the product with35 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 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 / Kaspersky

ESET and Kaspersky had zero false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
Dimio package	BDS/Backdoor.Gen	🟢

AVIRA had 1 false alarm.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
Elsa package	Suspect!3b4528c4ad1d	🟢
SUPER package	Suspect!cc514bba47e1	🟡

McAfee had 2 false alarms.

Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
Ebdac package	Gen:Variant.Ser.Razy.7489	🟢
Elsa package	Gen:Variant.Ser.Symmi.267	🟢
Feratel package	Gen:Variant.Johnnie.175731	🟡

Total Defense had 3 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
Dallas package	Suspicious:W32/Malware/DeepGuard.pg	🟢
Dimio package	Suspicious:W32/Malware/DeepGuard.pg	🟢
QuickTime package	Suspicious:W32/Malware/DeepGuard.p	🟢
Tiscali package	Suspicious:W32/Malware/DeepGuard.p	🟢

F-Secure had 4 false alarms.

Avast / AVG

False alarm found in some parts of	Detected as	Supposed prevalence
Ahnenforscher package	This file might be dangerous	🟢
Dimio package	Win32:MdeClass	🟢
GreenBrowser package	This file might be dangerous	🟢
GTA package	FileRepMalware	🟠
IntraPact package	This file might be dangerous	🟢
Norton package	This file might be dangerous	🟢
Sony package	This file might be dangerous	🟢

Avast and AVG had 7 false alarms.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
Bitdefender package	Malicious behaviour	🟢
Feratel package	Gen:Variant.Johnnie.175731	🟡
Registry package	Malicious application	🟢
Seulas package	Malicious application	🔴
SpeedCommander package	Malicious application	🟢
Tiscali package	Malicious application	🟢
Xmplay package	Gen:Suspicious.Cloud.8.qm0@ai@zmbgi	🟢

Bitdefender had 7 false alarms.

Symantec Norton

False alarm found in some parts of	Detected as	Supposed prevalence
CleanDisk package	Heur.AdvML.C	🟢
IntraPact package	Packed.Generic.535	🟢
LoginControl package	SONAR.Heuristic.170	🟢

Neko package	Suspicious.Epi.3	🟡
PaperOffice package	Heur.AdvML.B	🟢
ProcessExplorer package	Trojan.Gen.9	🟢
Telehandler package	Heur.AdvML.B	🟢

Symantec Norton had 7 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
ArchiCrypt package	Blocked	🟢
Baeume package	Blocked	🟢
CheckSig package	Blocked	🟢
Dimio package	Blocked	🟢
DVB package	Blocked	🟢
F1Challenge package	Blocked	🟢
FreshView package	Blocked	🟢
HTTPdown package	Blocked	🟢
IntraPact package	Blocked	🟢
Norton package	Blocked	🟢
QuickTime package	Blocked	🟢
Tio package	Blocked	🟢
Tiscali package	Blocked	🟢

Microsoft had 13 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Dallas package	Suspicious File Blocked	🟢
Dimio package	Suspicious File Blocked	🟢
GreenBrowser package	Suspicious File Blocked	🟢
HP package	Suspicious File Blocked	🟢
HTTPdown package	Suspicious File Blocked	🟢
Miranda package	Suspicious File Blocked	🟢
MP3Toys package	Suspicious File Blocked	🟢
MyUninstaller package	Suspicious File Blocked	🟢
Prog package	Suspicious File Blocked	🟢
RFA package	Suspicious File Blocked	🟢
ShareDirect package	Suspicious File Blocked	🟢
SipGate package	Suspicious File Blocked	🟢
Tiscali package	Suspicious File Blocked	🟢
VCL package	Suspicious File Blocked	🟢

Trend Micro had 14 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
ACER package	Suspicious	🟢
AsianInsta package	Trj/Genetic.gem	🔴
CheckSig package	Trj/Cl.A	🟢
CineMac package	Suspicious	🟢
Dallas package	Suspicious	🟢
Elsa package	Suspicious	🟢
FileSplitter package	Suspicious	🟢
GSTech package	Suspicious	🟢
HP package	Suspicious	🟢
IntraPact package	Suspicious	🟢
MP3Toys package	Suspicious	🟢
Phoenix package	Suspicious	🟢
PicEdit package	Suspicious	🟢
QuickTime package	Suspicious	🟢
RFA package	Suspicious	🟢
RoteAugen package	Suspicious	🟢
ShareDirect package	Suspicious	🟢
SipGate package	Suspicious	🟢
Tiscali package	Trj/Cl.A	🟢
XiceCube package	Suspicious	🟢
ZMV package	Suspicious	🟢

Panda had 21 false alarms.

Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Baywatch package	Dangerous activity detected	🟢
CDDVDburning package	Dangerous activity detected	🟢
Cerberus package	Dangerous activity detected	🟢
CineMac package	Dangerous activity detected	🟢
Dimio package	Dangerous activity detected	🟢
Ebdac package	Gen:Variant.Ser.Razy.7489	🟢
Elsa package	Dangerous activity detected	🟢
Emco package	Dangerous activity detected	🟢
Feratel package	Dangerous activity detected	🟡
HTTPdown package	Dangerous activity detected	🟢
HyperDesktop package	Dangerous activity detected	🟢
InstantPower package	Dangerous activity detected	🟢
Libro package	Dangerous activity detected	🟢
MailGuard package	Dangerous activity detected	🟢
MeldeMax package	Dangerous activity detected	🟢
Mueller package	Dangerous activity detected	🟢
MultiLauncher package	Dangerous activity detected	🟢
Paketmanager package	Dangerous activity detected	🟢
PDFme package	Dangerous activity detected	🟢
Picasa package	Dangerous activity detected	🟢

QuickTime package	Dangerous activity detected	🟢
Recovery package	Dangerous activity detected	🟢
SpeedCommander package	Dangerous activity detected	🟢
SteigEin package	Dangerous activity detected	🟢
Sumatra package	Dangerous activity detected	🟠
Tiscali package	Dangerous activity detected	🟢
UOM package	Dangerous activity detected	🟢

Tencent had 27 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Riskware (0040eff71)	🔴
Acrobat package	Riskware (0040eff71)	🔴
ArcSoft package	Virus (000000001)	🟡
ASUS package	Trojan (0047648f1)	🔴
ATI package	Riskware (0040eff71)	🔴
BittyProcess package	Riskware (0040eff71)	🟠
Cheat package	Riskware (0040eff71)	🔴
ColorPicker package	Virus (000000001)	🔴
DamageCleanup package	Riskware (0040eff71)	🔴
GRCD package	Riskware (0040eff71)	🟠
IbPro package	Riskware (0040eff71)	🟢
Lernassistent package	Virus (000000001)	🟢
Lexmark package	Riskware (0040eff71)	🟠
LG package	Riskware (0040eff71)	🔴
Logitech package	Virus (000000001)	🟠
MSOffice package	Riskware (0040eff71)	🔴
Nokia package	Riskware (0040eff71)	🔴
Opera package	Riskware (f15000051)	🟡
Phoenix package	Virus (0f1001091)	🟢
PicEdit package	Virus (0f1001091)	🟢
ShareDirect package	Riskware (0040eff71)	🟢
Skype package	Riskware (0040eff71)	🔴
SteigEin package	Trojan (0054315c1)	🟢
Sumatra package	Riskware (0040eff71)	🟠
TCPview package	Riskware (0040eff71)	🟡
Upack package	Trojan (003b1b581)	🟢
Wavosaur package	Virus (000000001)	🟡
WinAMP package	Riskware (0040eff71)	🟡
WLANinfo package	Riskware (0040eff71)	🟡

K7 had 29 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
ACER package	Blocked	🟢
ADAC package	Blocked	🟢
Anti-Trojan package	Blocked	🟢
Avago package	Blocked	🔴
AZFinder package	Blocked	🟢
Baywatch package	Blocked	🟢
Bitdefender package	Blocked	🟢
BlueOffice package	Blocked	🟢
CineMac package	Blocked	🟢
ColorPicker package	Blocked	🔴
Datron package	Blocked	🟢
Deskline package	Blocked	🟢
Dimio package	Blocked	🟢
eMerge package	Blocked	🟢
Feratel package	Gen:Variant.Johnnie.175731	🟡
GameCollection package	Blocked	🟢
Geburtstagsalarm package	Blocked	🟢
HTTPdown package	Gen:Variant.Fugrafe.5590	🟢
InstantPower package	Blocked	🟢
Libro package	Blocked	🟢
MailGuard package	Blocked	🟢
MP3Toys package	Blocked	🟢
MyUninstaller package	Blocked	🟢
Norton package	Blocked	🟢
ORF package	Blocked	🟡
Paketmanager package	Blocked	🟢
PCW package	Blocked	🟢
Recovery package	Blocked	🟢
Rikster package	Blocked	🟢
SaverInstaller package	Blocked	🟢
SeekFreak package	Blocked	🟢
Seulas package	Blocked	🔴
SipGate package	Blocked	🟡
SpamAI package	Blocked	🟢
Telehandler package	Blocked	🟢
Tiscali package	Malware (General)	🟢
Ultimate package	Blocked	🟡
Utility package	Blocked	🟢
Wistron package	Blocked	🟢
Xmplay package	Blocked	🟢

VIPRE had 40 false alarms. VIPRE have told us that their FP score in this test might be due to an unidentified bug.

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
(October 2019)