

Independent Tests of Anti-Virus Software



Details of False Alarms Appendix to the Malware Protection Test

TEST PERIOD: MARCH 2020
LANGUAGE: ENGLISH
LAST REVISION: 15TH APRIL 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. 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 with 35 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.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
Emsisoft package	TROJ_GEN.R03BC0WGK19	

Trend Micro had 1 false alarm.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
MessengerHistory package	ML/Augur trojan	
Schnapper package	ML/Augur trojan	

ESET had 2 false alarms.

G DATA

False alarm found in some parts of	Detected as	Supposed prevalence
AltTab package	Gen:Heur.Dreidel.gm0@w0TcLHQi	
HTTPdown package	Trojan.GenericKD.41780427	
STOP package	Trojan.GenericKD.41630944	

G DATA had 3 false alarms.

Total Defense

False alarm found in some parts of	Detected as	Supposed prevalence
AltTab package	Gen:Heur.Dreidel.gm0@w0TcLHQi	
ArchiCAD package	Malicious Application Blocked	
CRL package	Malicious Application Blocked	
Hex2Dw package	Gen:Variant.Midie.70649	
HTTPdown package	Trojan.GenericKD.41780427	
Stop package	Trojan.GenericKD.41630944	

Total Defense had 6 false alarms.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
AltTab package	Gen:Heur.Dreidel.gm0@w0TcLHQi	
Enter package	Detected threat	
HTTPdown package	Trojan.GenericKD.41780427	
Nobu package	Detected threat	
STOP package	Trojan.GenericKD.41630944	
Xlite package	Detected threat	

Bitdefender had 7 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
AltTab package	Gen:Heur.Dreidel.gm0@w0TcLHQi	
Enter package	Malware (General)	
Haushalt package	Malware (General)	
Hex2Dw package	Gen:Variant.Midie.70649	
HTTPdown package	Trojan.GenericKD.41780427	
Norton package	Malware (General)	
Pretorians package	Malware (General)	
Stop package	Trojan.GenericKD.41630944	

VIPRE had 8 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
AhnenForscher package	Exploit:097M/CVE-2017-8570.A	
CleanGP package	Threats found	
Coe package	Threats found	
Google package	Threats found	
Gunrox package	Threats found	
PCW package	Threats found	
Rkill package	Trojan:Win32/Bluteal!rfn	
Spamihilator package	Trojan:Win32/Vigorf.A	
WildTangent package	Threats found	

Microsoft had 9 false alarms.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
ChromeBackup package	UDS:Trojan-Spy.MSIL.KeyLogger	
eMedia package	HEUR:Trojan.Win32.Generic	
Encarta package	HEUR:Trojan.Win32.Agent.gen	
EsReg package	HEUR:Trojan.Win32.Generic	
PowerTools package	UDS:Trojan.Win32.Agent.gen	
PrettyMay package	UDS:DangerousObject.Multi.Generic	
Quiz package	HEUR:Trojan.Win32.Generic	
Steganos package	Trojan-Spy.Win32.Keylogger.bfib	
Vancouver package	File deleted	
VistaCodecs package	UDS:Trojan-Ransom.Win32.Blocker	

Kaspersky had 10 false alarms.

Avast / AVG

False alarm found in some parts of	Detected as	Supposed prevalence
AvancePaint package	Win32:Malware-gen	
CloneMaster package	Win32:Evo-gen [Susp]	
DiskRescue package	Win32:Malware-gen	
EFProcess package	FileRepMalware	
ExtractNow package	Win32:Malware-gen	
Fujitsu package	FileRepMalware	
Gunrox package	Win32:Malware-gen	
Image package	FileRepMetagen [Malware]	
Lame package	Win32:Malware-gen	
MPlayer package	FileRepMalware	
SerwerCharger package	FileRepMetagen [Malware]	
TrojanHunter package	Win32:Malware-gen	
Vancouver package	FileRepMalware	

VIPRE package	Win32:Malware-gen		
VirtualDub package	Win32:Trojan-gen		

Avast and AVG had 15 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
AvancePaint package	TR/Gendal.2110729 (Cloud)	
BMC package	HEUR/APC	
Books package	HEUR/APC (Cloud)	
Code2 package	BDS/Backdoor.Gen7	
Dungeon package	TR/Crypt.XPACK.Gen	
Enter package	TR/Rogue.11580780 (Cloud)	
FastNet package	HEUR/APC (Cloud)	
GhostX package	TR/Agent.399872.12 (Cloud)	
GP package	TR/Drop.Unruy.B	
Konwerter package	TR/Gendal.162304.D (Cloud)	
Moorhunt package	TR/Dropper.MSIL.43342	
NetworkFile package	HEUR/APC (Cloud)	
PCW package	HEUR/APC (Cloud)	
Prosto package	TR/PSW.OnlineGames.xmim.1 (Cloud)	
Przerwa package	TR/PSW.Agent.yda (Cloud)	
Savage package	TR/Dropper.Gen8	
StuffIt package	TR/Crypt.CFI.Gen	
TheBards package	TR/Crypt.ZPACK.Gen	
Tribes package	TR/Crypt.ZPACK.imevs	
VideoTeka package	HEUR/APC (Cloud)	
Wesnoth package	TR/Crypt.PEPM.Gen	
WinGuard package	DR/Dldr.VB.ilr (Cloud)	
WTW package	TR/Yarwi.cylci (Cloud)	
Zombie package	TR/Clicker.hlkm (Cloud)	

AVIRA had 24 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
ArcConvert package	Suspicious:W32/Malware!DeepGuard.p	
AvancePaint package	DR/Dldr.VB.vsc	
DiskTuna package	HEUR/APC	
Dungeon package	Trojan.TR/Crypt.XPACK.Gen	
EasyPing package	Trojan.TR/Drop.Unruy.B	
Enter package	TR/Rogue.11580780.529b0d732c!fsocap	
GhostX package	TR/Agent.399872.12	
Konwerter package	TR/Gendal.162304.D	

Lame package	TR/Gendal.5618461		
Moorhunt package	Trojan.TR/Dropper.MSIL.43342		
Odkurzacz package	Heuristic.HEUR/AGEN.1041088		
Outlook package	Backdoor.BDS/Backdoor.Gen7		
PCW package	HEUR/APC		
ProcessManager package	TR/PSW.OnlineGames.xmim.1.fbb0df7ef2!fsocap		
Przerwa package	TR/PSW.Agent.yda.84b14d8b61!fsocap		
RogueKiller package	Trojan:W32/Gen4135.a0a97083b1!Online		
Savage package	Trojan.TR/Dropper.Gen8		
StuffIt package	Heuristic.HEUR/AGEN.1007053		
TheBards package	Trojan.TR/Crypt.ZPACK.Gen		
Tribes package	TR/Crypt.ZPACK.imevs		
Wesnoth package	Trojan.TR/Crypt.PEPM.Gen		
WinGuard package	DR/Dldr.VB.ilr		
WTW package	TR/Yarwi.cylci		
Zombie package	TR/Clicker.hlkw		

F-Secure had 24 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
ACFB package	Suspect!b7bbce6eb5a2	
AvancePaint package	Suspect!9930c9bd6332	
Checksig package	Suspect!444b290283bf	
CleanGP package	Suspect!f7a20bc0df8b	
CleanMgr package	Suspect!565d20aa7102	
Controler package	Suspect!540ee00a2576	
DeskLine package	Suspect!f4c69f4aa0f1	
Enter package	Suspect!5b5ff0a64112	
File package	JTI/Suspect.262201!ce9aa0f4a2fb	
GGTuner package	Suspect!11cd5d5dce45	
Image package	Suspect!88b2b41ba5c9	
Lame package	Suspect!7fdc8cb35613	
NetScan package	Suspect!dacc0584d81e	
NetServer package	Suspect!3dd02329f096	
Patrician package	Suspect!2beba7912086	
RegistryWorkshop package	Suspect!288e42aae9ca	
SipGate package	GenericRXHT-BN!4C44A4935628	
Spectrum package	Suspect!cf7f1be6ee8a	
Sqirlz package	Suspect!d71093b18f7c	
Stop package	Suspect!1cadb0641fe1	
Swieta package	Suspect!6c496c2462ab	
SysPad package	Suspect!492e568aefdb	
UltraDefrag package	Suspect!621dec30b678	

USIM package	Suspect!62b284cc1bcf	
--------------	----------------------	--

McAfee had 24 false alarms.

NortonLifeLock

False alarm found in some parts of	Detected as	Supposed prevalence
AutoMKV package	Trojan.FakeAV	
AvancePaint package	Trojan.Gen	
Babylon package	Heur.AdvML.C	
Brothers package	Heur.AdvML.C	
CarJacker package	Suspicious.Epi.3	
CleanGP package	Suspicious.Epi.3	
Controler package	Suspicious.Epi.3	
Dimio package	Heur.AdvML.C	
DirectX package	Trojan.Gen.X	
Dooble package	Suspicious.Epi.3	
Dowcip package	Suspicious.Epi.3	
Earth package	Suspicious.Epi.3	
Easo package	Trojan.Gen	
FastHide package	Trojan.Gen.2	
Hardcopy package	Trojan.Gen.2	
Juarez package	Suspicious.Epi.3	
Konwerter package	Trojan.ADH	
Lame package	Suspicious.Epi.3	
ProcessMonitor package	Heur.AdvML.C	
RMCA package	Heur.AdvML.C	
SysPad package	Trojan.ADH.2	
TeamViewer package	Trojan Horse	
Wesnoth package	Suspicious.Epi.3	
XiceCube package	Suspicious.Epi.3	
Xion package	Suspicious.Epi.3	

NortonLifeLock had 25 false alarms.

TotalAV

False alarm found in some parts of	Detected as	Supposed prevalence
Access package	Threat Prevented (Url)	
AvancePaint package	TR/Gendal.2110729	
BMC package	HEUR/APC	
Dungeon package	TR/Crypt.XPACK.Gen.544	
EasyPing package	TR/Drop.Unruly.B	
eBooks package	HEUR/APC	
Enter package	TR/Rogue.11580780	
FastNet package	HEUR/APC	

GhostX package	TR/Agent.399872.12		
JFX package	HEUR/APC		
Konwerter package	TR/Gendal.162304.D		
Lame package	HEUR/APC		
Moorhunt package	TR/Dropper.MSIL.43342		
NetworkFile package	HEUR/APC		
Odkuzacz package	HEUR/APC		
Outlook package	BDS/Backdoor.Gen7		
ProcessManager package	TR/PSW.OnlineGames.xmim.1		
Savage package	TR/Dropper.Gen8		
ServiceCenter package	HEUR/APC		
StuffIt package	HEUR/AGEN.1007053		
TheBards package	TR/Crypt.ZPACK.Gen		
Tribes package	TR/Crypt.ZPACK.imevs		
VideoTeka package	HEUR/APC		
Wesnoth package	TR/Crypt.PEPM.Gen		
WinGuard package	DR/Dldr.VB.ilr		

TotalAV had 25 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
3D package	NetWorm (700000151)	
ActOfWar package	Trojan (0055e4051)	
Audapad package	NetWorm (700000151)	
AudioConverter package	Suspicious Program	
AutoHotKey package	P2PWorm (0055e3ea1)	
AutoMKV package	Suspicious Program	
B2DD package	Virus (000000001)	
Battlefield package	Riskware (0040eff71)	
CleanMgr package	Suspicious Program	
CopyPod package	Suspicious Program	
CRL package	Suspicious Program	
Defrag package	Riskware (0040eff71)	
DiaShow package	Suspicious Program	
Dogma package	Spyware (0055e3db1)	
DTC package	Virus (000000001)	
FastStone package	Riskware (0040eff71)	
GMER package	Riskware (0040eff71)	
GTA package	Riskware (0040eff71)	
Hosts package	Suspicious Program	
InstallAware package	Suspicious Program	
JkDefrag package	Riskware (0040eff71)	
Kaspersky package	Backdoor (000d6e3c1)	

Kidzy package	Suspicious Program		
Killbox package	Riskware (0040eff71)		
Kurt package	Suspicious Program		
Mailbox package	Suspicious Program		
MyUninstaller package	Trojan (0017a8521)		
Nattyware package	Suspicious Program		
NetworkFile package	Suspicious Program		
Odk package	Trojan-Downloader (000560ee1)		
Office package	Riskware (0040eff71)		
Opera package	Riskware (f15000051)		
PCconnectivity package	Trojan (0047648f1)		
PCInspector package	Riskware (0040eff71)		
Plastic package	Suspicious Program		
Platform package	Suspicious Program		
PrintService package	Virus (000000001)		
RedEyes package	Suspicious Program		
ReplayParser package	Suspicious Program		
RP package	Riskware (0040eff71)		
SkiRacing package	Suspicious Program		
Spamihilator package	Suspicious Program		
Super package	Riskware (0040eff71)		
TagesAnzeiger package	Suspicious Program		
Trine package	Suspicious Program		
Wavosaur package	Virus (000000001)		
XuPlayer package	Riskware (0040eff71)		

K7 had 47 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
ArcConvert package	Blocked	
AVIopen package	Blocked	
Battery package	Blocked	
Bestellbuch package	Blocked	
Brothers package	Blocked	
CheckSig package	Trj/CI.A	
Cue package	Blocked	
Decryptor package	Blocked	
DirSaver package	Blocked	
Dowcip package	Blocked	
EA package	Blocked	
eBooks package	Blocked	
Elster package	Blocked	
eMedia package	Blocked	

EQSecure package	Blocked		
FileSplitter package	Trj/GdSda.A		
Fraps package	Trj/GdSda.A		
GhostX package	Blocked		
Google package	Blocked		
Grub package	Blocked		
Interfacelift package	Blocked		
Keen package	Blocked		
MalwareBytes package	Blocked		
Microsoft package	Blocked		
Nexus package	Blocked		
NoteCase package	Blocked		
Orca package	Blocked		
Password package	Blocked		
PCW package	Blocked		
Preatorians package	Blocked		
ProcessMonitor package	Blocked		
Schnaepchen package	Blocked		
Shredder package	Blocked		
SK package	Blocked		
SortMenu package	Blocked		
Tawerna package	Blocked		
Techland package	Blocked		
TFT package	Blocked		
TheBard package	Blocked		
Tiscali package	Trj/CI.A		
Tribes package	Blocked		
Trine package	Blocked		
Ulead package	Blocked		
Uninstall package	Blocked		
Vancouver package	Blocked		
Wisco package	Blocked		
XiceCube package	Blocked		
Xlite package	Blocked		
Zchron package	Blocked		

Panda had 48 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
(April 2020)