Details about the discovered False Alarms

Appendix to the Anti-Virus Comparative September 2016

Language: English

September 2016
Last Revision: 10th October 2016

www.av-comparatives.org

Details about the discovered false alarms

With 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 produce false alarms (false positives). No product is immune from false positives (FPs), but some produce more than others, and the our goal is to find out 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 with 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 FP's 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 software, it is counted here as only one false alarm. Cracks, keygens, etc. 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 users 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 e.g. prevalence "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 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	
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 amount of false alarms (currently 10) inside our clean set before we start penalizing scores, and in our opinion products which produce a higher amount of false alarms are also more likely to produce false alarms on more prevalent files (or in other sets of clean files). The prevalence data we give about 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.

Some products using third-party engines/signatures may have fewer or more false alarms than the licensed engine has by its own, e.g. due to different internal settings implemented, the additional checks/engines/clouds/signatures, whitelist databases, time delay between the release of the original signatures and the availability of the signatures for third-party products, additional quality assurance of signatures before release, etc. 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, **Fortinet** and **Trend Micro** had zero false alarms on the used set of clean files.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
Herold package	Gen:Variant.Symmi.67713	
Sony package	Gen:Variant.Razy.30991	

Bitdefender had 2 false alarms.

Lavasoft

False alarm found in some parts of	Detected as	Supposed prevalence
Herold package	Gen:Variant.Symmi.67713	
Sony package	Gen:Variant.Razy.30991	

Lavasoft had 2 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
AutoIt package	TR/SelfDel.ec1900	
Igel package	HEUR/APC	
Vuex package	TR/Agent.89584.12	

AVIRA had 3 false alarms.

BullGuard

False alarm found in some parts of	Detected as	Supposed prevalence
Herold package	Gen:Variant.Symmi.67713	
Rapid package	Gen:Variant.Symmi.64277	
Sony package	Gen:Variant.Razy.30991	

BullGuard had 3 false alarms.

eScan

False alarm found in some parts of	Detected as	Supposed prevalence
Herold package	Gen:Variant.Symmi.67713 (DB)	
Rapid package	Gen:Variant.Symmi.64277 (DB)	
Sony package	Gen:Variant.Razy.30991 (DB)	

eScan had 3 false alarms.

Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
A1 package	Trojan.Win32.Llac.lbpa	
AutoIt package	Trojan.Win32.SelfDel.cfzt	
WinTuning package	UDS:DangerousObject.Multi.Generic	

Kaspersky Lab had 3 false alarms.

Sophos

False alarm found in some parts of	Detected as	Supposed prevalence
FreeDM package	Mal/Generic-S	
PersonDJ package	Mal/Zbot-UM	
Profe package	Mal/Generic-S	

Sophos had 3 false alarms.

ThreatTrack

False alarm found in some parts of	Detected as	Supposed prevalence
Herold package	Gen:Variant.Symmi.67713	
Rapid package	Gen:Variant.Symmi.64277	
Sony package	Gen:Variant.Razy.30991	

ThreatTrack had 3 false alarms.

Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Crossfire package	Gen:Variant.Mikey.53043	
Herold package	Gen:Variant.Symmi.67713	
Rapid package	Gen:Variant.Symmi.64277	
Sony package	Gen:Variant.Razy.30991	

Tencent had 4 false alarms.

Emsisoft

False alarm found in some parts of	Detected as	Supposed prevalence
GxTrans package	Trojan.Generic.7464985	
Herold package	Gen:Variant.Symmi.67713	
Orange package	Trojan.Sinowal.Gen.1	
Rapid package	Gen:Variant.Symmi.64277	
Sony package	Gen:Variant.Razy.30991	

Emsisoft had 5 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
BTRV package	RDN/Generic.com	
Pegasys package	Artemis!c5e21bed1b70	
Settlers package	Artemis!32c50b75be89	
TCHunt package	Artemis!5f94359c18d6	
Vuex package	Artemis!94a9fa418324	

McAfee had 5 false alarm.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
FinePrint package	Trojan:W32/Gen4135.1fc23018e8!Online	
GxTrans package	Trojan.Generic.7464985	
Herold package	Gen:Variant.Symmi.67713 (DB)	
InstantPlayer package	Trojan:W32/BitCoinMiner.J	
Orange package	Trojan.Sinowal.Gen.1	
Rapid package	Gen:Variant.Symmi.64277 (DB)	

F-Secure had 6 false alarms.

Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
Crossfire package	EE:Malwr.Heur.Mikey.53043	
GxTrans package	EE:Malware.Generic.7464985	
Herold package	EE:Malwr.Heur.Symmi.67713	
Orange package	EE:Trojan.Sinowal.Gen.1	
Rapid package	EE:Malwr.Heur.Symmi.64277	
Sony package	EE:Malwr.Heur.Razy.30991	

Quickheal had 6 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
Amok package	Trojan:Win32/Rundas!plock	
CDDVDBurner package	Trojan:Win32/Rundas!plock	
eZip package	Trojan:Win32/Rundas!plock	
MinScout package	Trojan:Win32/Dynamer!ac	
PEbuilder package	Trojan:Win32/Dynamer!ac	
SL package	Trojan:Win32/Dynamer!ac	
Snow package	Trojan:Win32/Rundas!plock	
Star package	Trojan:Win32/Dynamer!ac	
SUSD package	Trojan:Win32/Rundas!plock	
Wetterstation package	Trojan:Win32/Dynamer!ac	
WildTangent package	Trojan:Win32/Dorv.D!rfn	
xCAT package	Trojan:Win32/Dynamer!ac	

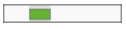
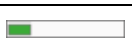
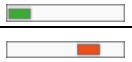
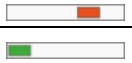
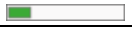
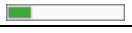
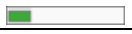
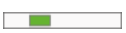
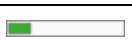
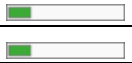
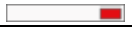
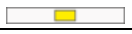
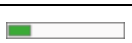
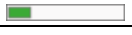
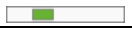
Microsoft had 12 false alarms.

AVG

False alarm found in some parts of	Detected as	Supposed prevalence
ARCAD package	Win32/Herz.A	
Atomic package	Win32/DH{IyQl?}	
Brother package	Generic_s.HNM	
Casino package	Crypt_s.LAG	
Clipsave package	Generic_s.IGI	
CoffeeFTP package	Win32/DH{CA?}	
Delay package	Luhe.Fiha.A	
DigitaleBibliothek package	PSW.Banker7.OSM	
Divx package	BackDoor.Generic19.AIUS	
EOC package	Atros3.AWYT	
HP package	Crypt5.AWRU	
IBM package	Generic_s.HVM	
Kinstone package	Win32/Herz.B	
MyWinLocker package	Generic37.BELF	
Norton package	Generic_r.MFR	
Presto package	Generic_s.HNM	
Roboform package	Generic_s.ILT	
Sygate package	Win32/Herz.B	
WildTangent package	Generic_r.IGQ	

AVG had 19 false alarms.

Avast

False alarm found in some parts of	Detected as	Supposed prevalence
3COM package	FileRepMalware	
Acer package	FileRepMalware	
ActualWindowsManager package	Win32:Evo-gen [Susp]	
Adobe package	Win32:Evo-gen [Susp]	
Cluster package	Win32:Evo-gen [Susp]	
ColorEfex package	Win32:Evo-gen [Susp]	
DateInTray package	Win32:Evo-gen [Susp]	
DirectX package	Win32:Malware-gen	
EuroRoute package	Win32:Evo-gen [Susp]	
FLV package	Win32:Evo-gen [Susp]	
HP package	FileRepMalware	
ISO2USB package	FileRepMetagen [Malware]	
JBTray package	Win32:Evo-gen [Susp]	
LetsTrade package	Win32:Evo-gen [Susp]	
LiteStep package	FileRepMalware	
Logik package	Win32:Evo-gen [Susp]	
Matrox package	Win32:Evo-gen [Susp]	
Money package	Win32:Evo-gen [Susp]	
MP3pooler package	Win32:Evo-gen [Susp]	
MyHints package	Win32:Evo-gen [Susp]	
RibbonCreator package	Win32:Dropper-gen [Drp]	
SafetyBrowser package	Win32:Malware-gen	
StarOffice package	Win32:Evo-gen [Susp]	
TrendMicro package	Win32:Evo-gen [Susp]	
TurboSliders package	Win32:Evo-gen [Susp]	
VOO30C package	Win32:Evo-gen [Susp]	
Vuex package	FileRepMetagen [Malware]	

Avast had 28 false alarms.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (October 2016)