

## **Details about the discovered False Alarms**



## **Appendix to the Anti-Virus Comparative March 2016**

Language: English

March 2016

Last Revision: 14<sup>th</sup> April 2016

[www.av-comparatives.org](http://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.

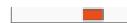
**ESET** and **Trend Micro** had zero false alarms on the used set of clean files.

### McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
TVgenial package	Artemis!E1DB26418B72	

McAfee had 1 false alarm.

### BullGuard

False alarm found in some parts of	Detected as	Supposed prevalence
Granny package	Gen:Variant.Razy.19282	
Runner package	Gen:Variant.Barys.49628	

BullGuard had 2 false alarms.

### eScan

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348 (DB)	 
Runner package	Gen:Variant.Barys.49628 (DB)	

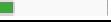
eScan had 2 false alarms.

### Sophos

False alarm found in some parts of	Detected as	Supposed prevalence
BZIP package	Mal/Dorf-D	 
TNI package	Mal/Generic-L	 

Sophos had 2 false alarms.

## Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348	 
Granny package	Gen:Variant.Razy.19282	 
Runner package	Gen:Variant.Barys.49628	 

Bitdefender had 3 false alarms.

## Emsisoft

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348 (B)	 
Granny package	Gen:Variant.Razy.19282 (B)	 
Runner package	Gen:Variant.Barys.49628 (B)	 

Emsisoft had 3 false alarms.

## Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
OnlineEye package	Trojan-Downloader.Win32.Banload.aadbo	 
Puzzle package	Trojan-Spy.Win32.Taopap.phe	 
Radeon package	P2P-Worm.Win32.Palevo.hynv	  

Kaspersky Lab had 3 false alarms.

## ThreatTrack

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348	 
Granny package	Gen:Variant.Razy.19282	 
Runner package	Gen:Variant.Barys.49628	 

ThreatTrack had 3 false alarms.

## F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348	 
FinePrint package	Trojan:W32/Gen4135.1fc23018e8!Online	 
Runner package	Gen:Variant.Barys.49628	 
Xtreme package	Trojan-dropper:W32/Coinminer.99db20ce3c!Online	  

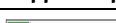
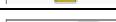
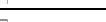
F-Secure had 4 false alarms.

## Lavasoft

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348	 
Granny package	Gen:Variant.Razy.19282	 
Mame package	Gen:Variant.Barys.52421	 
Runner package	Gen:Variant.Barys.49628	 

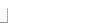
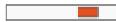
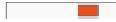
Lavasoft had 4 false alarms.

## Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Corel package	Gen:Variant.Barys.52348	 
Granny package	Gen:Variant.Razy.19282	 
Mame package	Gen:Variant.Barys.52421	 
Runner package	Gen:Variant.Barys.49628	 

Tencent had 4 false alarms.

## Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
Elsword package	Trojanspy.Agent.018127	 
Granny package	EE:Malwr.Heur.Razy.19282	 
IronBrowser package	JS/Agent.KK	 
MakeDisk package	Ransom.Crowti.A4	 
PerfectMenu package	Trojan.Malagent.019169	 
Runner package	EE:Malwr.Heur.Barys.49628	 
Screensaver package	Trojan.Scar.013919	 
WB package	Suspicious	 

Quickheal had 8 false alarms.

## AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
AudaPad package	HEUR/APC	 
Chilkat package	HEUR/APC	 
CreateAMall package	HEUR/APC	 
CueMaker package	HEUR/APC	 
Drei package	HEUR/APC	 
Fujitsu package	HEUR/APC	 
PlantsVSZombies package	HEUR/APC	 
Tiscali package	HEUR/APC	 
WinHotel package	HEUR/APC	 

AVIRA had 9 false alarms.

**AVG**

<b>False alarm found in some parts of</b>	<b>Detected as</b>	<b>Supposed prevalence</b>
Acer package	Zbot.AJKR	
AirSnare package	Collected_c.CGRB	
ArrowSearch package	Win32/DH{d4IRgQw}	
DigitalTheatre package	Win32/DH{cjETMHmBRg?}	
MightyChicken package	Win32/DH{gVGBCoFT?}	
PowerTranslator package	Win32/DH{ZzWCHIEPgRxR?}	
SIW package	Generic36.CGMO	
SysTrayX package	Agent5.AKKG	
VirtualExpander package	Win32/DH{gg92A1g?}	
Zattoo package	Win32/Herz	

AVG had 10 false alarms.

**Fortinet**

<b>False alarm found in some parts of</b>	<b>Detected as</b>	<b>Supposed prevalence</b>
ASUS package	W32/Agent.NESVWS!tr	
CableMon package	W32/Generic.AC.2181457	
ColdFusion package	W32/Generic.AC.2506367	
HWinfo package	W32/Bayrob.AT!tr	
Macromedia package	W32/Generic.AC.2506367	
PageDfrg package	PossibleThreat.SB!tr.rkit	
Pi package	W32/Kryptik.EKOM!tr	
SkinPack package	W32/Sim.SP!tr	
Startupo package	W32/Generic.AC.256673	
SysOpt package	INF/Qhost!tr	
<b>Triton package</b>	<b>W32/Generic.AC.2926293</b>	
WireShark package	W32/Kryptik.EMEK!tr	
WS_FTP package	W32/Kryptik.ELYI!tr	

Fortinet had 13 false alarms.

**Microsoft**

<b>False alarm found in some parts of</b>	<b>Detected as</b>	<b>Supposed prevalence</b>
2H4U package	Trojan:Win32/Varpes.J!plock	
Battlefield package	Trojan:Win32/Skeeyah.A!bit	
ClipInc package	Trojan:Win32/Dorv.C!rfn	
Dbox package	Trojan:Win32/Varpes.J!plock	
DerLauncher package	Trojan:Win32/Varpes.K!plock	
Fotokasten package	Trojan:Win32/Varpes.J!plock	
HiddenFinder package	Trojan:Win32/Varpes.K!plock	
KeriverImage package	Trojan:Win32/Varpes.J!plock	
MediaCenter package	Trojan:Win32/Varpes.J!plock	
MoviePlus package	Trojan:Win32/Varpes.K!plock	
Nero package	Trojan:Win32/Varpes.J!plock	
OrgaMax package	Trojan:Win32/Varpes.J!plock	
Outlookers package	Trojan:Win32/Varpes.J!plock	

Microsoft had 13 false alarms.

## Avast

False alarm found in some parts of	Detected as	Supposed prevalence
Adobe package	Win32:GenMalicious-MUY [Trj]	
BayCheck package	Win32:Evo-gen [Susp]	
DefaultTab package	Win32:Evo-gen [Susp]	
Digistar package	Win32:Evo-gen [Susp]	
FullCircle package	Win32:Malware-gen	
Ikea package	Win32:Evo-gen [Susp]	
Konica package	Win32:Evo-gen [Susp]	
MPlus package	Other:Malware-gen [Trj]	
MusicArena package	Win32:Evo-gen [Susp]	
Nero package	Other:Malware-gen [Trj]	
Nvidia package	Win32:Trojan-gen	
PopUpWasher package	Win32:Evo-gen [Susp]	
RadioTracker package	Win32:Evo-gen [Susp]	
ServersCheck package	Win32:Evo-gen [Susp]	
Sony package	Win32:Evo-gen [Susp]	
SysReport package	Win32:Evo-gen [Susp]	
vSkype package	Win32:Evo-gen [Susp]	

Avast had 17 false alarms.

## Copyright and Disclaimer

This publication is Copyright © 2016 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 2016)