

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



## **Appendix to the Anti-Virus Comparative September 2015**

Language: English

September 2015

Last Revision: 10<sup>th</sup> October 2015


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




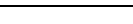

## Details about the discovered false alarms

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	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.
5	 Probably several hundreds of thousands or millions of users	


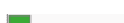
Most false alarms will probably fall into the first two levels most of the time. In our opinion, anti-virus products should not have false alarms on any sort of clean files regardless of how many users are currently affected by them. While some AV vendors may play down the risk of false alarms and play 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, Microsoft** and **Panda** had zero false alarms on the used set of clean files.

### Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
InViewer package	UDS:DangerousObject.Multi.Generic	
WinSweep package	UDS:DangerousObject.Multi.Generic	



Kaspersky Lab had 2 false alarms.

### Lavasoft

False alarm found in some parts of	Detected as	Supposed prevalence
MaxPasswords package	Trojan.Generic.12923569	
SafeNSec package	Trojan.Generic.13008834	



Lavasoft had 2 false alarms.

### Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Cleaner package	TR/Rogue.10439119	
SafeNSec package	TR/Rogue.14336.61	

Tencent had 2 false alarms.

### Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
Mahjongg package	Gen:Variant.Kazy.711143	
ProjectPrivacy package	Gen:Variant.Symmi.51003	

Bitdefender had 2 false alarms.

**Emsisoft**

False alarm found in some parts of	Detected as	Supposed prevalence
Mahjong package	Gen:Variant.Kazy.711143 (B)	
MaxPasswords package	Trojan.Generic.12923569 (B)	
SafeNSec package	Trojan.Generic.13008834 (B)	

Emsisoft had 3 false alarms.

**Trend Micro**

False alarm found in some parts of	Detected as	Supposed prevalence
GameAccelerator package	TROJ_HIDEFIL.BMC	
RadioFree package	Possible_Virus	
SafeNSec package	TROJ_GEN.R015C0EE715	
TempControl package	Cryp_Xed-12	

Trend Micro had 4 false alarms.

**BullGuard**

False alarm found in some parts of	Detected as	Supposed prevalence
Mahjong package	Gen:Variant.Kazy.711143	
MaxPasswords package	Trojan.Generic.12923569	
ProjectPrivacy package	Gen:Variant.Symmi.51003	
SafeNSec package	Trojan.Generic.13008834	

BullGuard had 4 false alarms.

**eScan**

False alarm found in some parts of	Detected as	Supposed prevalence
Mahjong package	Gen:Variant.Kazy.711143 (DB)	
MaxPasswords package	Trojan.Generic.12923569 (DB)	
ProjectPrivacy package	Gen:Variant.Symmi.51003[(DB)	
SafeNSec package	Trojan.Generic.13008834 (DB)	







eScan had 4 false alarms.

**AVIRA**

False alarm found in some parts of	Detected as	Supposed prevalence
Amazon package	HEUR/APC (Cloud)	
Cleaner package	TR/Rogue.10439119	
Presentation package	CLN/NoAutoCRC.Gen.33 (Cloud)	
SafeNSec package	TR/Rogue.14336.61	


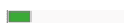





AVIRA had 4 false alarms.

**AVG**

False alarm found in some parts of	Detected as	Supposed prevalence
CrashCheck package	Win32/DH{gRKBE0F3dg}	
eTrust package	Win32/DH{AGFi}	
MDECompiler package	BackDoor.Generic18.CFPU	
MusicMaker package	SHeur4.CIKG	
SafeXP package	Win32/Heur	
Tuner package	Generic36.BTUH	


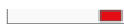





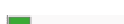
AVG had 6 false alarms.

**McAfee**

False alarm found in some parts of	Detected as	Supposed prevalence
BMKbuddy package	Artemis!91A002BDA561	
Kuebler package	Artemis!FC5059A421A4	
ManualAttaching package	Artemis!67FE7835B937	
Medion package	Artemis!3BFD3CB9537D	
SafeNSec package	Artemis!F55DEDAF88CA	
SmadAV package	Artemis!C515C219CDDA	
Sony package	Artemis!93F30CBB3015	

McAfee had 7 false alarms.

**Sophos**

False alarm found in some parts of	Detected as	Supposed prevalence
Aquadream package	Mal/EncPk-ABF0	
DeadTimeStories package	Mal/Generic-S	
eDataMSNFix package	Mal/Generic-S	
iPodder package	Mal/Generic-S	
PerfMenu package	Mal/Generic-S	
SeaMonkey package	Mal/EncPk-BW	
SimplePaint package	Mal/FakeAV-OZ	
WWFdesktop package	Mal/Packer	

Sophos had 8 false alarms.

## Fortinet

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	W32/Kryptik.DSK0!tr	
Acrobat package	W32/Generic.AC.2505476	
Colours package	W32/Injector.CHUQ!tr	
DigitalMedia package	W32/Waski.A!tr	
Ikarus package	W32/Kryptik.DSK0!tr	
Pause package	PossibleThreat.SB!tr	
PrimeSuspects package	PossibleThreat.SB!tr	
ProclList package	W32/Injector.CFKV!tr	
SwiftButton package	W32/Kryptik.DSK0!tr	
SysReport package	W32/Injector.CFKV!tr	
Valve package	W32/Generic.AC.62635	
WGet package	W32/Agent.MRLO!tr	

Fortinet had 12 false alarms.

## Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
HDDScan package	ExeShield Protector	
Ino package	HLLP.Taras.4423	
Joshua package	eXPressor	
Katalog package	ExeShield Protector	
Mahjong package	EE:Malwr.Heur.Kazy.711143	
MaxPasswords package	EE:Malware.Generic.12923569	
Mimocho package	Trojan.Diple.08520	
Notfall package	File is suspicious	
Passmark package	W32.Vampiro.B	
PowerBatch package	ExeShield Protector	
Registryhealer package	EXECryptor	
SafeNSec package	EE:Malware.Generic.13008834	
SimpleFileShredder package	ExeShield Protector	
StrongSearch package	ExeShield Protector	
TVgenial package	ExeShield Protector	
zWecker package	PC Shrinker	

Quickheal had 16 false alarms.

## F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
Adobe package	W32/Virut.f8539f0198!Online	
BodyPaint package	W32/Shellcode.b345120242!Online	
Cinema package	W32/Shellcode.b345120242!Online	
FinePrint package	W32/Gen4135.1fc23018e8!Online	
Helium package	W32/Malware.e8e7ed8448!Online	
MaxPasswords package	Trojan.Generic.12923569	
PDFserver package	W32/Gen2139.faa49fd666!Online	

SafeNSec package	W32/Malware.aa077bd836!Online	
SmadAV package	W32/Agent.DQ0A	
Synopsis package	W32/Malware.0c8969b4cf!Online	
T2I package	W32/Gen4135.d4b69ee86b!Online	
TempControl package	W32/Malware.afa07e621b!Online	
Time2Backup package	W32/Malware.cf37601bc1!Online	
Tourismus package	W32/Malware.0c8969b4cf!Online	
Trust package	W32/Malware.3a35623f06!Online	
WinOnCD package	W32/Gen1527.3d4465156c!Online	
Xtreme package	W32/Coinminer.99db20ce3c!Online	

F-Secure had 17 false alarms.

### ThreatTrack Vipre

False alarm found in some parts of	Detected as	Supposed prevalence
Audatex package	Trojan.Win32.Generic!BT	
CFOSspeed package	Trojan.Win32.Generic!BT	
Clickr package	Trojan.Win32.Generic!BT	
CrashDown package	Trojan.Win32.Generic!BT	
F-Secure package	BehavesLike.Win32.Malware.bsw	
GenDel package	Trojan.Win32.Generic!BT	
HDDLlife package	Trojan.Win32.Generic!BT	
Heroes package	Trojan.Win32.Generic!BT	
Kodak package	BehavesLike.Win32.Malware.bsw	
Meedio package	Trojan.Win32.Generic!BT	
Olivetti package	Trojan.Win32.Generic!BT	
PodTools package	Trojan.Win32.Generic!BT	
SecretZip package	Trojan.Win32.Generic!BT	
SimplyZip package	Trojan.Win32.Generic!BT	
Symantec package	Trojan.Win32.Generic!BT	
Tiscali package	Trojan.Win32.Generic!BT	
Visualization package	Trojan-Downloader.Win32.Agent	

ThreatTrack Vipre had 17 false alarms.

## Avast

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Win32:Evo-gen [Susp]	
BackupWizard package	Win32:Evo-gen [Susp]	
BCrypt package	Win32:Evo-gen [Susp]	
ByteMobile package	Win32:Evo-gen [Susp]	
Compaq package	Win32:Evo-gen [Susp]	
DeskCalc package	Win32:Evo-gen [Susp]	
<b>DivX package</b>	<b>Win32:Malware-gen</b>	
Druckerei package	Win32:Evo-gen [Susp]	
Eicon package	Win32:Evo-gen [Susp]	
eScan package	Win32:Evo-gen [Susp]	
EuCaSoft package	Win32:Evo-gen [Susp]	
FirstAid package	Win32:Evo-gen [Susp]	
FlashTool package	Win32:Evo-gen [Susp]	
Fujitsu package	Win32:Evo-gen [Susp]	
FurnPlan package	Win32:Evo-gen [Susp]	
Heko package	Win32:Evo-gen [Susp]	
IBM package	Win32:Evo-gen [Susp]	
Inoculate package	Win32:Evo-gen [Susp]	
IntraPact package	Win32:Evo-gen [Susp]	
Kaspersky package	Win32:Evo-gen [Susp]	
LANGuard package	Win32:Evo-gen [Susp]	
MedXpert package	Win32:Evo-gen [Susp]	
Melody package	Win32:Evo-gen [Susp]	
Oobe package	Win32:Agent-AVRG [Trj]	
Pelco package	Win32:Evo-gen [Susp]	
PiratenSchatz package	Win32:Evo-gen [Susp]	
SendToToys package	Win32:Evo-gen [Susp]	
Simon package	Win32:Evo-gen [Susp]	
Suffering package	Win32:Evo-gen [Susp]	
SunnyBall package	Win32:Malware-gen	
<b>Trend Micro package</b>	<b>Win32:Evo-gen [Susp]</b>	
Webbit package	Win32:Evo-gen [Susp]	
WebPlayer package	Win32:Malware-gen	
WhiteOut package	Win32:Evo-gen [Susp]	
Zylom package	Win32:Evo-gen [Susp]	

Avast had 35 false alarms.



**Baidu**

False alarm found in some parts of	Detected as	Supposed prevalence
AbcOE package	Trojan.Crypt.Heur.gen	
Acer package	Trojan.Autorun.Heur.gen	
Adobe package	Trojan.Crypt.Heur.gen	
AIMFix package	Trojan.QQThief.Heur.gen	
Aranea package	Trojan.Adware.Heur.gen	
Assembler package	Trojan.Crypt.Heur.gen	
Automate package	Trojan.Crypt.Heur.gen	
AZN package	Trojan.Crypt.Heur.gen	
BIPA package	Trojan.Crypt.Heur.gen	
Blinkx package	Trojan.Backdoor.Heur.gen	
Brockhaus package	Trojan.Crypt.Heur.gen	
Busch package	Trojan.Crypt.Heur.gen	
CA package	Trojan.Dropper.Heur.gen	
Cabook package	Exploit.CVE-2014-1761	
CaPoS package	Trojan.Crypt.Heur.gen	
CDDruckerei package	Trojan.Crypt.Heur.gen	
CDManager package	Trojan.Autorun.Heur.gen	
Cleaner package	Trojan.Generic.Heur.gen	
ClockCyb package	Trojan.Crypt.Heur.gen	
Cooxie package	Trojan.Dropper.Heur.gen	
CPUcool package	Trojan.Crypt.Heur.gen	
CPUFBS package	Trojan.Crypt.Heur.gen	
CrossFire package	Trojan.Crypt.Heur.gen	
CWShredder package	Trojan.GameThief.Heur.gen	
Cygwin package	Trojan.Crypt.Heur.gen	
DiaShow package	Trojan.Dropper.Heur.gen	
DragZ package	Trojan.Generic.Heur.gen	
Dreikampf package	Trojan.Dropper.Heur.gen	
DrWeb package	Trojan.Downloader.Heur.gen	
Duden package	Trojan.Crypt.Heur.gen	
EA package	Trojan.Crypt.Heur.gen	
EasyBurning package	Trojan.Dropper.Heur.gen	
EasyIndex package	Trojan.Crypt.Heur.gen	
eScan package	Trojan.Generic.Heur.gen	
EuroReisekosten package	Trojan.Crypt.Heur.gen	
Ewido package	Trojan.Downloader.Heur.gen	
ExifTool package	Trojan.Backdoor.Heur.gen	
Fdos package	Trojan.Crypt.Heur.gen	
FileHandler package	Trojan.Crypt.Heur.gen	
FileWorks package	Trojan.Crypt.Heur.gen	
FiZip package	Trojan.Dropper.Heur.gen	
Firefox package	Trojan.Crypt.Heur.gen	
FlexMail package	Trojan.Crypt.Heur.gen	
FotoFit package	Trojan.Crypt.Heur.gen	
Framewood package	Trojan.Autorun.Heur.gen	
FreshUI package	Trojan.Backdoor.Heur.gen	
GameGuard package	Trojan.Crypt.Heur.gen	

GameXP package	Trojan.Crypt.Heur.gen	
GoldRush package	Trojan.Crypt.Heur.gen	
GTA package	Trojan.Backdoor.Heur.gen	
HandyPack package	Trojan.Crypt.Heur.gen	
HardwareSensor package	Trojan.Crypt.Heur.gen	
Hartlauer package	Trojan.Crypt.Heur.gen	
HastaZip package	Trojan.Dropper.Heur.gen	
Heroglyph package	Trojan.Crypt.Heur.gen	
HomeMedia package	Trojan.Crypt.Heur.gen	
HP package	Trojan.Generic.Heur.gen	
IdentityProtection package	Trojan.Crypt.Heur.gen	
Ikaros package package	Trojan.Crypt.Heur.gen	
Installer2Go package	Trojan.Downloader.Heur.gen	
IoWare package	Trojan.GameThief.Heur.gen	
JdTricks package	Trojan.Autorun.Heur.gen	
JumpTo package	Trojan.Crypt.Heur.gen	
Kaspersky package	Trojan.Crypt.Heur.gen	
Kensington package	Trojan.Generic.Heur.gen	
McAfee package	Trojan.Dropper.Heur.gen	
Micrografx package	Trojan.Crypt.Heur.gen	
Mittelerde package	Trojan.GameThief.Heur.gen	
MobileMedia package	Trojan.Crypt.Heur.gen	
MSServer2003 package	Trojan.Downloader.Heur.gen	
MSWindows2000 package	Trojan.Crypt.Heur.gen	
MSWindows98 package	Trojan.Dropper.Heur.gen	
MSWindowsME package	Trojan.Crypt.Heur.gen	
MSWindowsNT package	Trojan.Crypt.Heur.gen	
MSWindowsXP package	Trojan.Downloader.Heur.gen	
Navigon package	Trojan.Downloader.Heur.gen	
Need4Speed package	Trojan.GameThief.Heur.gen	
NewsLeecher package	Trojan.Dropper.Heur.gen	
Obscure package	Trojan.Crypt.Heur.gen	
OnlineEye package	Trojan.Crypt.Heur.gen	
PhotoImpact package	Trojan.Crypt.Heur.gen	
PixPower package	Trojan.Dropper.Heur.gen	
PlantsVsZombies package	Trojan.Crypt.Heur.gen	
PlayMovie package	Trojan.Crypt.Heur.gen	
PowerArchiver package	Trojan.Generic.Heur.gen	
PowerBatch package	Trojan.Crypt.Heur.gen	
PowerStd package	Trojan.Crypt.Heur.gen	
PrimeSuspects package	Trojan.Crypt.Heur.gen	
PunicWar package	Trojan.Crypt.Heur.gen	
Purge package	Trojan.Crypt.Heur.gen	
QuickCliq package	Trojan.Downloader.Heur.gen	
RadioSuite package	Trojan.Crypt.Heur.gen	
Rally package	Trojan.Dropper.Heur.gen	
Redfield package	Trojan.Dropper.Heur.gen	
RegistryHealer package	Trojan.Crypt.Heur.gen	
Rose package	Trojan.Crypt.Heur.gen	
RPMTuning package	Trojan.Crypt.Heur.gen	

RTF2HTML package	Trojan.Crypt.Heur.gen	
SafeNSec package	TR/Rogue.14336.61	
SaferMail package	Trojan.Crypt.Heur.gen	
SafeXP package	Trojan.Crypt.Heur.gen	
SecretMaker package	Trojan.Crypt.Heur.gen	
Sims package	Trojan.Backdoor.Heur.gen	
SIW package	Trojan.GameThief.Heur.gen	
SmartPro package	Trojan.Crypt.Heur.gen	
SmartSuite package	Trojan.Dropper.Heur.gen	
Soccer package	Trojan.Dropper.Heur.gen	
Sony package	Trojan.Crypt.Heur.gen	
Sophos package	Trojan.Win32.Agent.50	
SpamAgent package	Trojan.Crypt.Heur.gen	
SpamFighter package	Trojan.Dropper.Heur.gen	
Stripper package	Trojan.Crypt.Heur.gen	
SuperCollapse package	Trojan.Crypt.Heur.gen	
Sygate package	Trojan.Backdoor.Heur.gen	
Symantec package	Trojan.Backdoor.Heur.gen	
SysBackup package	Trojan.Generic.Heur.gen	
SysRescue package	Trojan.Dropper.Heur.gen	
SystemSafety package	Trojan.Generic.Heur.gen	
Targem package	Trojan.Crypt.Heur.gen	
Thief package	Trojan.Crypt.Heur.gen	
ThumbsPlus package	Trojan.Crypt.Heur.gen	
Tierpension package	Trojan.Crypt.Heur.gen	
TippTop package	Trojan.Crypt.Heur.gen	
Toolbook package	Trojan.Autorun.Heur.gen	
TransXP package	Trojan.Crypt.Heur.gen	
TuneUpUtilities package	Trojan.Generic.Heur.gen	
Tunguska package	Trojan.Crypt.Heur.gen	
TVnoise package	Trojan.Crypt.Heur.gen	
TweakPower package	Trojan.Backdoor.Heur.gen	
Unreal package	Trojan.Crypt.Heur.gen	
Vbox package	Trojan.Crypt.Heur.gen	
VideoDeluxe package	Trojan.Crypt.Heur.gen	
WarCraft package	Trojan.GameThief.Heur.gen	
WhatSpeed package	Trojan.Crypt.Heur.gen	
WildFire package	Trojan.Backdoor.Heur.gen	
WinInBlack package	Trojan.Generic.Heur.gen	
ZipMagic package	Trojan.Generic.Heur.gen	
ZipZag package	Trojan.Backdoor.Heur.gen	
Zylom package	Trojan.Crypt.Heur.gen	

Baidu had 139 false alarms.

## Copyright and Disclaimer

This publication is Copyright © 2015 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 2015)