

Details about Discovered False Alarms



Appendix to the Anti-Virus Comparative No. 25 February 2010

Language: English

February 2010

Last Revision: 17th March 2010


www.av-comparatives.org

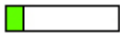




Details about the discovered false alarms

With AV testing it is important to measure not only detection capabilities but also reliability - one of reliability aspects is certainly product's tendency to flag clean files as infected. No product is immune from false positives (FP's) but there are differences among them and the goal is to measure them. Nobody has all legitimate files that exist and so no "ultimate" test of FP's can be done. What can be done and is reasonable, is to create and use a set of clean files which is independent. If on such set one product has e.g. 50 FP's and another only 10, it is likely that the first product is more prone to FP's than the other. It doesn't mean the product with 10 FP's doesn't have more than 10 FP's globally, but important is the relative number.

All listed false alarms were reported and sent to the Anti-Virus vendors for verification and are now already fixed. 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, as well as FP's distributed by vendors or other non independent sources are not counted here as False Positives.

Not all false alarms are equal, so, in order to give even more information to the users about the false alarms, we will try to rate the prevalence of the false alarms. Files with valid digital signatures are considered more important. Due that, a file with e.g. prevalence "level 1" and a valid digital signature gets upgraded to next level (e.g. prevalence "level 2").

The prevalence is given in 5 categories and labeled with the following colors: 

Level	Presumed number of affected users ¹	Comments
1 	Probably fewer than hundred users	Individual cases, old or rarely used files, unknown prevalence
2 	Probably some hundreds of users	Initial distribution of such files was probably higher, but current usage on actual systems is lower (despite its presence), that's why also well-known software may now affect / have only a prevalence of some hundreds or thousands of users.
3 	Probably some thousands of users	
4 	Probably tens of thousands (or more) of users	
5 	Probably hundreds of thousands (or more) of users	Such cases are likely to be seen very 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. We do not even give an own category for cases which affect several millions of users.

Most false alarms will probably most of the times fall into the first two levels. In our opinion Anti-Virus products should not have false alarms on clean files despite how many users are affected by them. While AV vendors 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 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. Also due that, the prevalence data we give about clean files is just for informational purpose. Prevalence data can in some cases be heavily underestimated (like on non-PE files, security software, rarely accessed files, etc.), and the given prevalence is just our rough estimation based on the data (like e.g. from various clouds, download/sales stats, etc.) we could rely on. The listed prevalence can differ inside the report depending on which file / version the false alarm occurred.


¹ If all users would have used the Anti-Virus product causing the false alarm at that time.

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 different internal settings implemented, the additional checks/engines, whitelist databases, time delay between the release of the original signatures and the availability of the signatures for third-party products, additional QA 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 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 FP again on a more significant file. Thus, they still deserve mention and still deserve penalty.



Below you will find the false alarms we observed in our independent set of clean files. Red entries highlight false alarms on files with valid digital signatures.

eScan

False alarm found in some parts of Tiscali package	Detected as Trojan.Generic.1713592	Supposed prevalence 
--	--	---




eScan had 1 false alarm.

F-Secure

False alarm found in some parts of StreamCatcher package Tiscali package	Detected as Gen:Trojan.Heur.GZ.bOW@bWsyLgj Trojan.Generic.1713592	Supposed prevalence  
--	---	--




F-Secure with default settings had 2 false alarms.

BitDefender

False alarm found in some parts of SpamFighter package	Detected as Generic.Malware.E.B1CCD178	Supposed prevalence 
StreamCatcher package	Gen:Trojan.Heur.GZ.bOW@bWsyLgj	
Tiscali package	Trojan.Generic.1713592	

Bitdefender had 3 false alarms.

Microsoft

False alarm found in some parts of MaxAV package	Detected as Trojan:Win32.Bladi!rts	Supposed prevalence 
Tischlampe package	Trojan:Win32/Meredrop	
VisualStyler package	Backdoor:Win32/Pasur!rts	

Security Essentials had 3 false alarms.

ESET

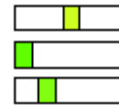
False alarm found in some parts of

PaperOffice package
 PostGuard package
 SonicVisualizer package

Detected as

NewHeur_PE
 Win32/Genetik
 Win32/Statik

Supposed prevalence



ESET NOD32 had 3 false alarms.

Sophos

False alarm found in some parts of

2pic package
 ActivaIP package
 PodTools package
 TCPfilter package

Detected as

Mal/Generic-A
 Mal/Generic-A
 Mal/Packer
 Mal/Generic-A

Supposed prevalence



Sophos had 4 false alarms with default settings. As Sophos is a product for corporate users, which computers are managed by an administrator, the above discovered FP's are not a big issue.

Kaspersky

False alarm found in some parts of

Covermount package
 EastTecEraser package
 EFCommander package
 Kurznachrichten package
 OutlookTuner package

Detected as

HEUR:Trojan.Win32.Generic
 Backdoor.Win32.Hupigon.jjui
 Backdoor.Win32.Agent.anmg
 Trojan-PSW.Win32.LdPinch.bnk
 Packed.Win32.Krap.ae

Supposed prevalence



Kaspersky had 5 false alarms.

G DATA

False alarm found in some parts of

FiberTwig package
 MACperl package
 Tiscali package
 VirtualKeyboard package
 WinOnCD package

Detected as

Win32:Malware-gen
 Win32:Malware-gen
 Trojan.Generic.1713592
 Win32:Malware-gen
 Win32:Malware-gen

Supposed prevalence



G DATA had 5 false alarms.

PC Tools

False alarm found in some parts of

- 3Danalyzer package
- CPUControl package
- Multifunction package
- PhotoMatix package
- PSI package
- TaskManager package
- USBMouseRate package
- VDownloader package

Detected as

- Trojan.Generic
- Downloader.Generic
- Trojan-PWS.Lineage
- Net-Worm.Kolabc!sd6
- Backdoor.Trojan
- Trojan-PSW.Gampass
- Trojan.Generic
- Trojan.Generic

Supposed prevalence



PC Tools had 8 false alarms.

TrustPort

False alarm found in some parts of

- Canna3 package
- ESET package
- FreshDow package
- Kaspersky package
- PlainPaste package
- TheMop package
- TweakXP package
- VistaBootPro package
- YAW package

Detected as

- Downloader.Obfuskated
- Generic.VDY
- SHeur2.BVQO
- SymbOS/Drever.B
- Worm/Autoit.WLJ
- Suspected!yoda
- SHeur2.BRDx
- Win32/Heur
- Generic15.ZQI

Supposed prevalence



TrustPort had 9 false alarms.

AVG

False alarm found in some parts of

- AnimateDesktop package
- Canna3 package
- ESET package
- ExelockExpress package
- FreshDow package
- Kaspersky package
- PlainPaste package
- TweakXP package
- VistaBootPro package
- YAW package

Detected as

- Win32/DH.IA
- Downloader.Obfuskated
- Generic.VDY
- Generic12.AWZM
- SHeur2.BVQO
- SymbOS/Drever.B
- Worm/Autoit.WLJ
- SHeur2.BRDx
- Win32/Heur
- Generic15.ZQI

Supposed prevalence



AVG had 10 false alarms.

Avast

False alarm found in some parts of

CloseIE package
 FiberTwig package
 IrfanView package
 MACperl package
 NortonUtilities package
 RegistryOptimizer package
 VirtualKeyboard package
 WebsiteWatcher package
 WinOnCD package
 YAW package
 zDataburn package

Detected as

Win32:Trojan-gen
 Win32:Malware-gen
 Win32:Trojan-gen
 Win32:Malware-gen
 Win32:Trojan-gen
 Win32:Trojan-gen
 Win32:Malware-gen
 Win32:Trojan-gen
 Win32:Malware-gen
 Win32:Trojan-gen
 Win32:Trojan-gen

Supposed prevalence



Avast had 11 false alarms.

Symantec

False alarm found in some parts of

3Danalyzer package
 AutoStartAdmin package
 Blinkx package
 CableMonitor package
 InternetRadio package
 PDFtk package
 PhotoMatix package
 PSI package
 Slice&Save package
TaskManager package
 USBMouserate package

Detected as

Trojan Horse
 Suspicious.MH690.A
 Suspicious.MH690.A
 Suspicious.MH690.A
 Suspicious.MH690.A
 Suspicious.MH690.A
 Trojan Horse
 Backdoor.Trojan
 Suspicious.MH690.A
Infostealer.Gampass
 Trojan Horse

Supposed prevalence



Symantec Norton Anti-Virus had 11 false alarms.

AVIRA

False alarm found in some parts of

Anti-Trojan package
 Auction package
 BluetoothSender package
 GPGkeys package
 Icon package
 IrfanView package
 Krypter package
 ShowShifter package
 SimplyZIP package
 Telemetry package
 VallenZipper package

Detected as

TR/Agent.263168.1
 BDS/Backdoor.Gen2
 TR/Dropper.Gen
 TR/Downloader.Gen
 TR/ATRAPS.Gen
 TR/Spy.871424.1
 HEUR/Malware
 HEUR/Malware
 TR/Agent.526964
 TR/Spy.Gen
 DR/Delphi.Gen

Supposed prevalence



AVIRA had 11 false alarms.

Trend Micro

False alarm found in some parts of

0190warner package
 3DScreensaver package
 Adward package
 AutostartAdmin package
 BitTorrent package
 CableMon package
 DupeWipe package
eScan package
 FavoriteStartpage package
 FileEncrypter package
 FireMonitor package
 Gothic package
 Gudbrand package
 Hauppauge package
 Ikarus package
 IntelliHyperspeed package
 Miranda package
 OpenOffice package
PaintDotNet package
 PodTools package
 Privacy package
 PSI package
 RegScanner package
 RouterSyslog package
 SimplyZip package
 SpamKiller package
 Splitting package
 StartupBooster package
 Sylpheed package
 TVgenial package
 Unlocker package
 Vanderlee package
 VBA32 package
 ViperRacing package
 W2W package
 WanyWord package
 XpAntispy package
 XpTweaker package

Detected as

PE_Generic.ADV
 TROJ_Generic
 TROJ_GEN.OZ1701
 TROJ_Generic.ADV
 TROJ_NOSHLEX.MCS
 TROJ_Generic.ADV
 PE_Generic
TROJ_Generic.ADV
 TROJ_Generic.ADV
 TROJ_Generic.DIT
 TROJ_Generic.DMS
 TROJ_Generic.ADV
 TROJ_Generic.ADV
 Dialer_PlayGames
 TROJ_Generic.DIT
 TROJ_Generic.ADV
 Cryp_Upack
 Cryp_Upack
TROJ_Generic.ADV
 Cryp_Yodap
 TROJ_FAKEAV.MCS
 Troj_Generic.DIM
 TSPY_Agent
 Cryp_Xed-12
 Cryp_Xed-12
 PE_GENERIC
 Cryp_Yodac
 TROJ_Generic.DIT
 RAP_Generic
 TSPY_Jared
 TROJ_Generic.ADV
 TROJ_Generic.ADV
 TROJ_Generic
 TROJ_Generic.DIT
 TROJ_Gen.6Z0225
 TROJ_Generic.ADV
 TSPY_Agent.OE
 TROJ_Generic

Supposed prevalence



Trend Micro had 38 false alarms. Trend Micro without in-the-cloud had 22 false alarms. Trend Micro is a new entry in our tests – due that, it is to expect that their number of false alarms will be lower next time.

Panda

False alarm found in some parts of

Archivarius package
 AutoHotKey package

Detected as

Trj/CI.A
 Trj/CI.A

Supposed prevalence



CFOSspeed package	Generic Backdoor	
CPUControl package	Generic Trojan	
Cubase package	Generic Malware	
eScan package	Trj/CI.A	
ExcelTools package	W97/NoHate.A	
FastDefrag package	Generic Worm	
FastStone package	Suspicious file	
FileVerifier package	Trj/CI.A	
FotoD3 package	Suspicious file	
FreeNetTV package	Suspicious file	
GDATA package	Generic Trojan	
GetRight package	Generic Malware	
GIMP package	Generic Malware	
GXTranCoder package	Trj/CI.A	
Horallite package	Suspicious file	
HotCorners package	W32/Sohanat.AS.worm	
HyperCam package	W32/Gaobot.OXI.worm	
Konto package	Trj/CI.A	
Lbacache package	W16/Cezar.A	
Lilypond package	Suspicious file	
MaiISync package	Malicious Packer	
MaxAV package	Trj/CI.A	
Mkv2Vob package	Trj/CI.A	
NetInfo package	Suspicious file	
NMAP package	Generic Malware	
No23Recorder package	Malicious Packer	
Pcalc package	Trj/CI.A	
PhotoMatix package	W32/Gaobot.OXI.worm	
PowerStd package	Trj/CI.A	
RealtimeBrowser package	Trj/CI.A	
RegistryScanner package	Trj/CI.A	
rLinux package	Trj/CI.A	
SourceRescue package	Suspicious file	
SSC package	Generic Worm	
Sylpheed package	Trj/CI.A	
TaskManager package	Trj/Lineage.BZE	
Tiscali package	Trj/CI.A	
Translator package	Suspicious file	
UltraDVD package	Suspicious file	
USBdrive package	Dialer.ANF	
VideoExpress package	Bck/Hupigon.AZG	
VideoZilla package	Suspicious file	
Webbit package	Suspicious file	
Wettermelder package	Trj/Downloader.MDW	
WinUPACK package	W32/Spamta.gen.worm	

Panda had 47 false alarms. Panda without in-the-cloud had 32 false alarms. Panda is a new entry in our tests – due that, it is to expect that their number of false alarms will be lower next time.

McAfee

False alarm found in some parts of

3DScreenSaver package
 AudioAnalyzer package
 AVIRA package
 BookmarkBuddy package
 CCleaner package
CFOSSpeed package
 ChoCastl package
 CitySoft package
 CmdlineProcessor package
 CoolMouse package
 CSElite package
 DialerControl package
 DiaShowPro package
 DocServer package
EastTecEraser package
 EmailBackup package
 Ewido package
 FotoBuch package
 FreshDow package
 GameAccelerator package
 GPSPhoto package
 HauppaugeDriver package
 HDVideoConverter package
 Hobby package
 iColorFolder package
 JkDefrag package
 Linkman package
 MakeInstantPlayer package
 Minimize2Tray package
 MKV2VOB package
 MozillaBackup package
 MS IE package
 MS Works package
 MultiInstall package
 Notepad2 package
 NXPowerLite package
PandaCloudAV package
 PlainPaste package
 PortablePGP package
 PSI package
 RegCool package
 RTF2HTML package
Safe'N'Sec package
 Scite package
 SecretMaker package
SpiceWorks package
 StarDownloader package
 StickSecurity package
 StreamRipper package

Detected as

Artemis!72AA666AE5E5
 Artemis!6E0DA4F2E2AB
 Artemis!3C6F97707518
 Artemis!327A598B4AE7
 Generic.dx!mju
Artemis!327B0ED9941F
 Artemis!3D07BC0A0C0E
 Exploit-ZIP.b
 New Malware.bl
 Artemis!E586A090ED45
 Artemis!38E8528588DE
 Artemis!9779B905B021
 Artemis!D8A817D2FDDE
 Artemis!58EFEC13C677
Generic.dx!mvq
 New Malware.bl
 Artemis!88E199CD3A74
 Suspect-02!D65AF320424D
 New Malware.hi
 Kkrunchy Packed
 Artemis!6C292AA6DEDF
 Artemis!AD22112238CA
 New Win32.g4
 FakeAlert-IN!dam
 Artemis!E943ED4E96BA
 Artemis!EAA831008828
 Artemis!9E91F15F9CF4
 Artemis!9D71D26E9C65
 Artemis!354E20997A33
 Artemis!85F6CE295559
 Artemis!6896A03142FD
 Artemis!DA57F048A5A1
 Artemis!88F2E1E04B94
 Artemis!023A8B1266E4
 Artemis!707E6C241CB6
 Artemis!EB9F505A37D3
Artemis!EA0442DA060E
 Generic.dx
 Artemis!4660AE8AB28E
 Artemis!12BAC5724865
 Artemis!3B5E8139B2E5
 New Malware.l
Artemis!0BBA61663EE6
 Artemis!E161732AF9D3
 Artemis!FCA232D44FC6
Artemis!674DBE3541FF
 Artemis!AADB88A53BE6
 New Malware.d
 Artemis!CB9EA5B3587D

Supposed prevalence



TyperShark package	Generic PUP.l	
Video2iPod package	Artemis!B02B2D1BBBCB	
VLCPortable package	Artemis!7505C2724E3B	
VPELoader package	Artemis!5228C788C83C	
VUI package	Artemis!3FBFC4610C8A	
WhatSpeed package	Artemis!AB5AF80131F5	
WinampLyrics package	Keylog.gen	
WMIenable package	New Malware.ai	
xBrowser package	Artemis!5F4F6C44F0AC	
XFire package	Artemis!2124D346DE1E	
Xilisoft DVD2iPhone package	New Win32.g4	
YAW package	Artemis!C35A0E239EC6	
ZonerPhotostudio package	Generic PWS.y!bwv	

McAfee with in-the-cloud (default) had 61 false alarms. McAfee without in-the-cloud had 19 false alarms.

Norman

False alarm found in some parts of

- AcrobatReader package
- AscGen package
- Asghan package
- ATASec package
- Atomaders package
- BenQ driver package
- BestBuyFinder package
- BLZ package
- Bullguard package
- Calcy package
- ClickEXE package
- ClipInc package
- Cloxc package
- CopyPod package
- CPUz package
- CrashLogCollector package
- Deeenes package
- DownloadTimer package
- DrawingHands package
- EastTec package
- EasyBurning package
- eJay package
- Euromat package
- EVTerminate package
- Ewido package
- FileZilla package
- GetIt package
- GoldWave package
- Harrys package
- HotKeys package
- IETweaker package

Detected as

- W32/Smalltroj.Q00E
- Suspicious_Gen.AUQA
- W32/Suspicious_Gen2.LOXX
- W32/Obfuscated.FA
- W32/EMailWorm
- W32/Smalltroj.IKLW
- SuspiciousPE.C.dropper
- W32/Suspicious_Gen2.AICD
- W32/Swizzor.GTJF
- W32/Obfuscated.Q!genr
- W32/Suspicious_Gen2.RON
- W32/Suspicious_Gen.EAPJ
- W32/Suspicious_Gen2.dam
- W32/Obfuscated.VPE
- W32/Malware
- W32/Malware
- W32/Malware
- SuspiciousPE.C.dropper
- W32/Bifrose.BKYF
- W32/Suspicious_Gen2.Q
- W32/Packed_Upack.A
- Malware.IQH0
- W32/Suspicious_Gen2.AICD
- W32/Obfuscated.CD!genr
- W32/Suspicious_Gen2.LEL
- Agent.SDGI
- W32/AutoRun.ACKY
- W32/Agent.SPEG
- SuspiciousPE.C.dropper
- W32/DLoader.ABFOS
- W32/Obfuscated.F!genr

Supposed prevalence



JkDefrag package	Autoit.SQ	
K-Meleon package	W32/Suspicious_Gen.EQBJ	
kAmel package	SuspiciousPE.C.dropper	
Medion driver package	W32/Obfuscated.AT!genr	
MegaTR package	W32/FakeAV.AD!genr	
Min2Tray package	W32/Suspicious_Gen2.LBV	
MS Frontpage package	W32/Suspicious_Gen.FPMK	
MusicMan package	W32/Suspicious_Gen2.NIC	
MyBook package	W32/Suspicious_Gen.FNQP	
MyGallery package	W32/Agent.SBJQ	
OpenOffice package	W32/Suspicious_Gen2.AIR	
PaperOffice package	W32/FakeAV.X!genr	
PhotoMatix package	W32/Akbot.HE	
PNGPLT package	SuspiciousPE.C.dropper	
PowerBullet package	Malware.DQBI	
PSP package	W32/Suspicious_Gen2.LKEW	
RealtimeBrowser package	Suspicious_Gen2.UYN	
ReiseBoerse package	W32/Suspicious_Gen2.IDLW	
RipCast package	Spyware.CZM	
Sandboxie package	W32/Obfuscated.CM!genr	
ShareAza package	W32/Obfuscated.B!genr	
SimplyZip package	Suspicious_Gen2.AAED	
SL package	Suspicious_Gen2.KXJH	
TaskManager package	W32/Suspicious_Gen2.AAXM	
TinyPerf package	W32/FakeAV.AD!genr	
TrendMicro package	W32/Suspicious_Gen2.GJHP	
Tribes package	W32/Zlob.gen17	
TrueCrypt package	W32/Malware	
VCC package	W32/Malware.BHJA	
VirtualDrive package	W32/Malware	
WinConsole package	W32/Malware	
WinTK package	W32/Malware.INXK	
ZipInstaller package	W32/VBDoor.UIR	

Norman had 64 false alarms.

Kingsoft

False alarm found in some parts of

- AllWaterfall package
- Anti-Trojan package
- ATI driver package
- AttachmentExtractor package
- AudioTagging package
- Avast package
- AVIRA package
- Besieger package
- BloodMoon package
- CFOSSpeed package
- Chars package
- ClipInc package

Detected as

- Win32.Troj.Delsha.c.844380
- Win32.Troj.Undef.622592
- Heur.Win32.Generic.an
- Heur.Win32.Generic.an
- Win32.Hack.VB.91136
- Worm.WhiteIce.d.232960
- Win32.Adware.Vundoa.98344
- Heur.Win32.Generic.an
- Heur.Win32.Generic.an
- Heur.Win32.Generic.an
- Win32.Troj.Undef.684740

Supposed prevalence



ColinMcRae package	Heur.Win32.Generic.an	
CorelDraw package	Win32.Troj.Undef.48128	
CreativeLabs driver package	Heur.Win32.Generic.an	
CyclingManager package	Heur.Win32.Generic.an	
Cywin package	Win32.Troj.Undef.35840	
Digibin package	Win32.Troj.Delsha.c.844380	
DirectX package	Win32.Troj.Undef.299520	
DiskFront package	Win32.Troj.Undef.795136	
DraculaTwins package	Heur.Win32.Generic.an	
DriveScribe package	Win32.Hack.DTR.14.14336	
DRU package	Win32.Troj.Delf.311988	
ExpPrint package	Heur.Win32.Generic.an	
ExtraTool package	JS.Agent.oj.9650	
FileZilla package	Heur.Win32.Generic.an	
FolderLock package	Win32.Hack.Final.a.4042752	
GDATA package	Win32.Troj.Undef.231248	
GPSPPhoto package	Heur.Win32.Generic.an	
Haushaltsbuch package	Heur.Win32.Generic.an	
HeatMapper package	Heur.Win32.Generic.an	
HP driver package	Heur.Win32.Generic.an	
IELinker package	JS.Downloader.xo.791	
Launcher package	BAT.AutorunT.vs	
MS Windows 2000 package	Win32.Troj.Aegi.12048	
Norman package	Win32.Troj.Swisyn.446000	
NVIDIA driver package	Heur.Win32.Generic.an	
ODFplugin package	Heur.Win32.Generic.an	
OilTycoon package	Heur.Win32.Generic.an	
OpenOffice package	Heur.Win32.Generic.an	
Outpost package	Win32.Troj.Delf.73793	
PanoramaStudio package	Heur.Win32.Generic.an	
Particles package	Win32.Troj.Depro.265366	
PeToUSB package	Heur.Win32.Generic.an	
PhotoMatix package	Worm.Kolabc.51156	
ProcessManager package	Win32.Troj.FraudPack.180224	
Quicken package	Win32.Troj.Undef.196608	
RealNetworks package	Heur.Win32.Generic.an	
RegistryMonitor package	Worm.Beagle.192512	
Replication package	Heur.Win32.Generic.an	
SafeNSec package	Heur.Win32.Generic.an	
SciTe package	Heur.Win32.Generic.an	
SD package	Win32.Hack.Huigezi.85736	
Shutdown package	Heur.Win32.Generic.an	
SmartCap package	Heur.Win32.Generic.an	
SSM package	Win32.Troj.Delf.54514	
Sync package	Heur.Win32.Generic.an	
TimeBoxManager package	Heur.Win32.Generic.an	
TransMute package	Heur.Win32.Generic.an	
TrueCrypt package	Heur.Win32.Generic.an	
TubeBox package	Heur.Win32.Generic.an	
URE package	Heur.Win32.Generic.an	
VUIS package	Heur.Win32.Generic.an	
WDM driver package	Win32.Troj.Obfuscated.ap.958464	

WinUpack package	Win32.Troj.Undef.143360	
WS FTP package	Heur.Win32.Generic.an	
zDataBurn package	Win32.Troj.Generic.811008	

Kingsoft had 67 false alarms.

K7

False alarm found in some parts of

- ACDSee package
- AcousticalMP3 package
- AcrobatReader package
- ActiveSpeed package
- AdminStick package
- ADSL package
- AlarmI package
- Anmanie package
- Aut2Exe package
- AutoHotKey package
- Autoruns package
- AVIRA package
- AZN package
- BabelMap package
- BarNone package
- Battlefield package
- BearShare package
- BitComet package
- BitTorrent package
- BootSpeed package
- Borg package
- BrotherDriver package
- CDCreator package
- CDex package
- CDProtect package
- CFOSSpeed package
- CharsetFilter package
- CineBench package
- Clavier package
- ClearProg package
- CommTest package
- CopyPod package
- CPUcontrol package
- CPUz package
- DailyDiary package
- DBFunktionen package
- DCU package
- Decoder package
- DeskTask package
- DigiPhoto package
- Dnet package
- DriveImage package

Detected as

- Trojan (0001140e1)
- Trojan (0001140e1)
- Riskware (a8f280a10)
- Backdoor (d0f92e5e0)
- Backdoor (f9252b040)
- Trojan (0006f5451)
- Adware (000414251)
- Trojan (0006f5451)
- Adware (0006fbd91)
- Trojan (0001e2d91)
- Backdoor (00059be31)
- Trojan (0006f5451)
- Riskware (734f98cb0)
- Trojan (0006f5451)
- Virus (994159940)
- Exploit (dc80ca2b0)
- Trojan (0001140e1)
- Riskware (abfae70b0)
- Trojan (7bca017b0)
- Trojan (f31bd6760)
- Trojan (0006f5451)
- Trojan (0006f2c01)
- Backdoor (484780d50)
- Trojan (0006f5451)
- Backdoor (0b733f880)
- Exploit (dc80ca2b0)
- Backdoor (00059be31)
- Trojan (0006f5451)
- Trojan (0006f5451)
- Riskware (3c86d9f30)
- Backdoor (a3adc1400)
- Riskware (3c86d9f30)
- Trojan (0001140e1)
- Trojan-Downloader (0006f2b71)
- Trojan (808726980)
- Backdoor (00059be31)
- Backdoor (f85e35660)
- Riskware (fcf7495a0)
- Trojan (0006f5451)
- Spyware (0006f8c41)
- Trojan (00071a9a1)
- Backdoor (00059be31)

Supposed prevalence



DupeWipe package	Riskware (3c86d9f30)	
DVBViewer package	EmailWorm (00091f9b1)	
DVDPlayer package	Riskware (bcb638e90)	
EasyHDR package	Trojan (0003445f1)	
EFcommander package	Backdoor (0011f83a1)	
EMIS package	Backdoor (bee5801a0)	
eMusic package	Trojan-Downloader (0006f2b71)	
eScan package	Riskware (df9b14ef0)	
ESET package	EmailWorm (0001cb3b1)	
Eulalyzer package	Backdoor (000405371)	
EvilLyrics package	Trojan (0001140e1)	
Ewido package	Trojan (00071a9b1)	
FastDefrag package	Trojan (0001140e1)	
FileMonitor package	Trojan (0007176c1)	
FloppyOffice package	Trojan (0006f5451)	
FolderLock package	Trojan (0001140e1)	
FreeRAM package	Trojan (0006f5451)	
FreshDow package	Trojan (10ea3e230)	
FTcheck package	Trojan (dd017b3c0)	
GameAccelerator package	Trojan (0001140e1)	
GDATA package	Password-Stealer (00090f7e1)	
GetWIM package	Trojan (dd017b3c0)	
GPGkeys package	Trojan (0001140e1)	
GPSPhoto package	Trojan (0001140e1)	
GrammatikTrainer package	Trojan (bcc72b9c0)	
GridMove package	Backdoor (0006f2d51)	
HauppaugeDriver package	Riskware (fcf7495a0)	
HiSpot package	Trojan (0006f5451)	
HotCorners package	Trojan (0001140e1)	
HotKeys package	Trojan-Downloader (8bf671b80)	
ImageForge package	Trojan (0006f5451)	
Incredimail package	Riskware (324353060)	
Inspiration package	Riskware (6e83b1080)	
IntegratedDriver package	Virus (94dad6410)	
Isobuster package	Trojan (000b5a321)	
ITpro package	Backdoor (00059be31)	
JkDefrag package	Trojan (0006f8aa1)	
Joshua package	Riskware (3c86d9f30)	
Kalender package	Trojan (0006f5451)	
KartenSpiele package	Backdoor (00059be31)	
Kaspersky package	EmailWorm (0c1872450)	
Kassenbuch package	Trojan (e13cd27f0)	
KeyboardLink package	Backdoor (00032e6e1)	
KostenRechner package	Trojan (0006f5451)	
Krieger package	Trojan (0001140e1)	
MalwareDestroyer package	Unwanted-Program (ec3a9a6d0)	
MapCreator package	Backdoor (0006fb2c1)	
MapleXP package	Trojan (67ba8f5b0)	
MaxiVista package	Trojan (0006f5451)	
MaxPasswords package	Riskware (fbeedfb00)	
MemoryZip package	Trojan-Downloader (000078731)	
MemTest package	Spyware (0006f8c41)	

MgTweak package	Backdoor (713fd5670)	
MineSweeper package	Trojan (bcc72b9c0)	
MP3Test package	Trojan (0001140e1)	
MSIwlan package	Adware (000695041)	
MSOffice2001 package	Trojan (00071a9a1)	
MSWorks package	Trojan (0001140e1)	
MS IE package	Spyware (0000fee01)	
MS WindowsXP package	Trojan (0001a9451)	
MultiStageRecovery package	Trojan (1401fe750)	
nDroid package	Spyware (000288871)	
Nero package	Trojan (ebf64a000)	
NetMonitor package	Trojan (1ab053f80)	
No23Recorder package	Riskware (3c86d9f30)	
NokiaFreeCalc package	Trojan (0001140e1)	
Notepad++ package	Adware (47d574fe0)	
Notepad2 package	Riskware (0009efc41)	
NoURL package	Trojan (0006f5451)	
OleManager package	Trojan (d46bbeb80)	
Outpost package	Trojan (0001140e1)	
PaperOffice package	Trojan (45ec77210)	
PatchScanner package	Spyware (0006fd511)	
PE2USB package	Spyware (0006f8c41)	
PlainPaste package	Trojan (0001140e1)	
PodTools package	Riskware (3c86d9f30)	
Posterazor package	Trojan (0006f5451)	
ProcessExplorer package	Spyware (0006f8c41)	
ProcMan package	Trojan (0006f5451)	
ProgramStopper package	Spyware (0006f8c41)	
Putty package	Trojan (0001140e1)	
RadioSuite package	Riskware (3c86d9f30)	
RCS package	Trojan (d0f63bc60)	
Recolored package	Spyware (0006f8b41)	
RegRun package	Trojan (0001140e1)	
RegSeeker package	Trojan (0006f5451)	
RegShot package	Trojan (0001140e1)	
RegSnap package	Spyware (0006f8c41)	
Reiseboerse package	Trojan (00071a9a1)	
RTF2HTML package	Riskware (eca15ce20)	
SafeXP package	Riskware (3c86d9f30)	
Salive package	Trojan (d0f63bc60)	
Samurize package	Trojan (10ea3e230)	
San package	Spyware (0006f8c41)	
Schwimmen package	Trojan (241d818c0)	
SearchMyDiscs package	Backdoor (0b733f880)	
SecretMaker package	Riskware (3c86d9f30)	
SFLZ package	Trojan (0006f5451)	
SFTM package	Password-Stealer (b304c75c0)	
SimplyZip package	Backdoor (0006f2b91)	
Skype package	Riskware (3c86d9f30)	
SoftCam package	EmailWorm (00091f981)	
SopCast package	Adware (0006f6e41)	
SpamAI package	Trojan (ee87ea920)	

SpamAware package	Trojan-Downloader (00044b411)	
SparkleXP package	Backdoor (0004cbf11)	
SplitF package	Trojan (ce706ba90)	
SpySweeper package	Backdoor (000143381)	
SSC package	Virus (1c4403fc0)	
StartupBooster package	Trojan (0001140e1)	
Steeper package	Backdoor (8ba6f2c00)	
Strokes package	Trojan (0006f5451)	
Super package	Adware (c3e349630)	
Suse package	Virus (ed85809a0)	
Symantec package	Riskware (a8f280a10)	
SystemLupe package	Spyware (0006f8c41)	
SystMech package	Backdoor (6f9982670)	
TagesAnzeiger package	Trojan (0006f5451)	
TaskManager package	Trojan (00071a9b1)	
TechnoTrend package	Riskware (fcf7495a0)	
TeechArt package	Trojan (0006f5451)	
Tetrix package	Virus (e55847090)	
ThumbHTML package	Trojan (000b5a321)	
TIN package	Riskware (4af336af0)	
Tiscali package	Trojan (0001140e1)	
TopDesk package	Trojan (00014a681)	
ToWav package	Trojan (cb0e187d0)	
TrafficMonitor package	Backdoor (000461131)	
TrendMicro package	Riskware (3280796a0)	
TrueCrypt package	Backdoor (00059be31)	
Twibble package	Backdoor (00059be31)	
UltraStar package	Riskware (db04faa20)	
UniExtract package	EmailWorm (000130f61)	
USBagent package	Trojan (dd017b3c0)	
VistaDriveIcon package	Trojan (0001140e1)	
Weihnachtsgruss package	Backdoor (00059be31)	
WEKAvorlagen package	Backdoor (00059be31)	
Wettermelder package	Adware (2a3dac7b0)	
WF package	Trojan (bd500b400)	
WinBoard package	Trojan (dd017b3c0)	
WinPooch package	Backdoor (00059be31)	
WinRAR package	Trojan (0006f5aa1)	
Wisterer package	Trojan (0006f5451)	
WordPro package	Unwanted-Program (6a1a0eb80)	
Wos package	Trojan (000720041)	
WW2 package	Trojan (241d818c0)	
Xampp package	EmailWorm (73df9d620)	
Xmoto package	Backdoor (0006f5871)	
XPclean package	Trojan (0006f5451)	
ZMatrix package	Trojan (0001140e1)	
ZonerPhotoStudio package	Spyware (651178b70)	

K7 had 193 false alarms. K7 is a new entry in our tests – due that, it is to expect that their number of false alarms will be lower next time.

Copyright and Disclaimer

This publication is Copyright © 2010 by AV-Comparatives e.V. ®. 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 e.V., prior to any publication. AV-Comparatives e.V. 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 e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (March 2010)