Details about Discovered False Alarms

Appendix to the Anti-Virus Comparative August 2010

Language: English
August 2010
Last Revision: 19th September 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 noticied 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.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve	🟩⬜⬜⬜⬜
WGet package	Trojan.Generic.3887481	⬜⬜🟨⬜⬜

F-Secure with default settings had 2 false alarms.

Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
Aloha package	TrojanDownloader:Win32/Troxen!rts	🟩⬜⬜⬜⬜
CheopsPyramide package	Trojan:Win32/Meredrop	⬜⬜🟨⬜⬜
SunnyBall package	TrojanDownloader:Win32/Troxen!rts	🟩⬜⬜⬜⬜

Security Essentials had 3 false alarms.

BitDefender

False alarm found in some parts of	Detected as	Supposed prevalence
DZip package	Gen:Trojan.Heur.UT.gmW@bKZeeIei	⬜🟩⬜⬜⬜
Lilypond package	Gen:Trojan.Heur.FU.iCZ@aeqi9dli	🟩⬜⬜⬜⬜
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve	🟩⬜⬜⬜⬜
WGet package	Trojan.Generic.3887481	⬜⬜🟨⬜⬜

Bitdefender had 4 false alarms.

eScan

False alarm found in some parts of	Detected as	Supposed prevalence
DZip package	Gen:Trojan.Heur.UT.gmW@bKZeeIei (DB)	⬜🟩⬜⬜⬜
FolderLock package	Trojan-Dropper (ES)	⬜⬜⬜⬜🟥
Lilypond package	Gen:Trojan.Heur.FU.iCZ@aeqi9dli (DB)	🟩⬜⬜⬜⬜
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve (DB)	🟩⬜⬜⬜⬜
WGet package	Trojan.Generic.3887481 (DB)	⬜⬜🟨⬜⬜

eScan had 5 false alarm.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
GTXTranscoder package	Win32/Genetik	⬜🟩⬜⬜⬜
iTunesGenreManager package	Win32/PSW.LdPinch.ELMNSCM	⬜🟩⬜⬜⬜
PaperOffice package	NewHeur_PE	⬜⬜🟩⬜⬜
StereoscopicPlayer package	Win32/Packed.Themida	⬜🟩⬜⬜⬜
WGet package	Win32/Agent.EWTEPIN	⬜⬜🟩⬜⬜
xCAT package	Win32/Packed.Themida	⬜🟩⬜⬜⬜

ESET NOD32 had 6 false alarms.

PC Tools

False alarm found in some parts of	Detected as	Supposed prevalence
333 package	Trojan.Gen	🟩⬜⬜⬜⬜
GPGKeys package	Trojan.Generic	🟩⬜⬜⬜⬜
Lazarus package	HeurEngine.Vuntid	🟩⬜⬜⬜⬜
SmartNTFSRecovery package	Trojan.FakeAV!rem	⬜🟩⬜⬜⬜
Tiscali package	Trojan.Gen	⬜🟩⬜⬜⬜
vDownloader package	Trojan.ADH	🟩⬜⬜⬜⬜
WGet package	Trojan.Generic	⬜⬜🟩⬜⬜

PC Tools had 7 false alarms.

Avast

False alarm found in some parts of	Detected as	Supposed prevalence
Deluxanoid package	Win32:Malware-gen	🟩⬜⬜⬜⬜
FontTwister package	Win32:Malware-gen	🟩⬜⬜⬜⬜
HP driver package	VBS:Malware-gen	🟩⬜⬜⬜⬜
PacManiac package	Win32:Malware-gen	⬜🟩⬜⬜⬜
Retroremake package	Win32:Malware-gen	⬜🟩⬜⬜⬜
SpamAware package	Win32:Trojan-gen	⬜⬜🟩⬜⬜
SpyDetector package	Win32:Genlot-GO	🟩⬜⬜⬜⬜
Tiscali package	Win32:Malware-gen	⬜🟩⬜⬜⬜
TrendMicro package	Win32:Malware-gen	⬜🟩⬜⬜⬜

Avast had 9 false alarms.

Symantec

False alarm found in some parts of	Detected as	Supposed prevalence
AlienStars package	Suspicious.MH690.A	⬜🟩⬜⬜⬜
CDDVDBurning package	Suspicious.Cloud.AM	⬜🟩⬜⬜⬜
Lazarus package	Packed.Vuntid!gen1	🟩⬜⬜⬜⬜
PhraseExpress package	Suspicious.MH690.A	⬜🟩⬜⬜⬜
SimplyZip package	Infostealer.Gampass	⬜🟩⬜⬜⬜
SmartNTFSRecovery package	Suspicious.Cloud.2	⬜🟩⬜⬜⬜
TeaTimer package	Suspicious.Cloud.2	🟩⬜⬜⬜⬜
Tiscali package	Suspicious.Cloud.2	⬜🟩⬜⬜⬜
WGet package	Trojan Horse	⬜⬜🟩⬜⬜

Symantec Norton Anti-Virus had 9 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
Autorota package	BDS/Delf.uss	⬜⬜🟨⬜⬜
Backtec package	TR/Dropper.Gen	🟩⬜⬜⬜⬜
DiaShowPro package	DR/Agent.7066624	🟩⬜⬜⬜⬜
FrogWares package	TR/PSW.Lmir.1531964	⬜⬜⬜🟧⬜
GPU package	TR/Dldr.Delphi.Gen	🟩⬜⬜⬜⬜
GTRacingOleManager package	TR/Spy.Gen	⬜🟩⬜⬜⬜
PacManiac package	TR/Click.VBiframe.crn	⬜🟩⬜⬜⬜
SymplyZip package	TR/Agent.2274937	⬜🟩⬜⬜⬜
SpamFighter package	TR/Dropper.Gen	🟩⬜⬜⬜⬜
TrendMicro package	HTML/Rce.Gen	⬜🟩⬜⬜⬜

AVIRA had 10 false alarms.

Sophos

False alarm found in some parts of	Detected as	Supposed prevalence
AurTech package	Mal/Generic-A	⬜⬜🟨⬜⬜
Ewido package	Mal/Generic-A	⬜⬜🟨⬜⬜
FireMonitor package	Mal/Generic-A	⬜🟩⬜⬜⬜
InternetExplorer8 package	Mal/Generic-A	⬜⬜⬜🟧⬜
PlainPaste package	Mal/Generic-A	⬜🟩⬜⬜⬜
RegHeal package	Mal/Delf-AR	⬜🟩⬜⬜⬜
Rohos package	Mal/Generic-A	⬜⬜🟨⬜⬜
SuperCopier package	Mal/Generic-A	⬜⬜⬜🟧⬜
TheMusicLoader package	Mal/VBDldr-B	⬜🟩⬜⬜⬜
Toucan package	Mal/Generic-A	⬜🟩⬜⬜⬜
VideoAccelerator package	Mal/Generic-A	⬜⬜⬜⬜🟥
XPizeReloader package	Mal/BredoZp-B	🟩⬜⬜⬜⬜
ZDATABurn package	Mal/Generic-A	⬜🟩⬜⬜⬜

Sophos had 13 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 may not be a big issue.

G DATA

False alarm found in some parts of	Detected as	Supposed prevalence
Deluxanoid package	Win32:Malware-gen	🟩⬜⬜⬜⬜
DiaShowPro package	Win32:Dropper-CMZ	⬜⬜🟨⬜⬜
DrawingHands package	Win32:Trojan-gen	🟩⬜⬜⬜⬜
DZip package	Gen:Trojan.Heur.UT.gmW@bKZeeIei	⬜🟩⬜⬜⬜
FontTwister package	Win32:Malware-gen	🟩⬜⬜⬜⬜
HP driver package	VBS:Malware-gen	🟩⬜⬜⬜⬜
Lilypond package	Gen:Trojan.Heur.FU.iCZ@aeqi9dli	🟩⬜⬜⬜⬜
Pacmaniac package	Win32:Malware-gen	⬜🟩⬜⬜⬜
RetroRemake package	Win32:Malware-gen	⬜🟩⬜⬜⬜
SpamAware package	Win32:Trojan-gen	⬜⬜🟨⬜⬜
SpyDetector package	Win32:Genlot-GO	🟩⬜⬜⬜⬜
Tiscali package	Win32:Malware-gen	⬜🟩⬜⬜⬜
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve	🟩⬜⬜⬜⬜
TrendMicro package	Win32:Malware-gen	⬜🟩⬜⬜⬜
WGet package	Trojan.Generic.3887481	⬜⬜🟨⬜⬜

G DATA had 15 false alarms.

AVG

False alarm found in some parts of	Detected as	Supposed prevalence
Aspell package	Downloader.Obfuskated	🟩⬜⬜⬜⬜
Autorota package	BackDoor.Generic12.CBVX	⬜⬜🟨⬜⬜
CurrentPorts package	Generic18.BOIK	⬜⬜🟨⬜⬜
Dmailer package	SHeur3.BMQ	🟩⬜⬜⬜⬜
EasyBurn package	Generic10.QFQ	⬜🟩⬜⬜⬜
ESET package	Win32/Heur	⬜⬜🟨⬜⬜
FreeProcessManager package	Generic17.ASIR	⬜⬜🟨⬜⬜
HaloThirdFOV package	Generic17.RSG	⬜⬜🟨⬜⬜
InControl package	Generic17.LIY	⬜🟩⬜⬜⬜
InfoCenter package	Script/Exploit	⬜🟩⬜⬜⬜
PlanetMP3 package	IRC/BackDoor.SdBot4.RVB	🟩⬜⬜⬜⬜
PunicWars package	SHeur3.GVT	🟩⬜⬜⬜⬜
TeaTimer package	Win32/Heur	🟩⬜⬜⬜⬜
TrendMicro package	BackDoor.Ircbot.MNQ	⬜⬜🟨⬜⬜
VirtualKeyboard package	Dropper.Generic2.KPZ	⬜🟩⬜⬜⬜
WinRAR package	PSW.Generic8.KYY	⬜⬜🟨⬜⬜
ZDBackup package	Win32/Heur	⬜⬜🟨⬜⬜
ZipGenius package	SHeur3.ACWU	⬜🟩⬜⬜⬜
ZTape package	Win32/Heur	🟩⬜⬜⬜⬜

AVG had 19 false alarms.

TrustPort

False alarm found in some parts of	Detected as	Supposed prevalence
Autorota package	BackDoor.Generic12.CBVX	⬜⬜🟨⬜⬜
DMailer package	SHeur3.BMQ	🟩⬜⬜⬜⬜
DZip package	Gen:Trojan.Heur.UT.gmW@bKZeeIei	⬜🟩⬜⬜⬜
EasyBurn package	Generic10.QFQ	⬜🟩⬜⬜⬜
ESET package	Win32/Heur	⬜⬜🟨⬜⬜
FreeProcessManager package	Generic17.ASIR	⬜⬜🟨⬜⬜
InControl package	Generic17.LIY	⬜🟩⬜⬜⬜
Lilypond package	Gen:Trojan.Heur.FU.iCZ@aeqi9dli	🟩⬜⬜⬜⬜
PlanetMP3 package	IRC/BackDoor.SdBot4.RVB	🟩⬜⬜⬜⬜
PunicWars package	SHeur3.GVT	🟩⬜⬜⬜⬜
TeaTimer package	Win32/Heur	🟩⬜⬜⬜⬜
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve	🟩⬜⬜⬜⬜
TrendMicro package	BackDoor.Ircbot.MNQ	⬜⬜🟨⬜⬜
VirtualKeyboard package	Dropper.Generic2.KPZ	⬜🟩⬜⬜⬜
Wget package	Trojan.Generic.3887481	⬜⬜🟨⬜⬜
WinRAR package	PSW.Generic8.KYY	⬜⬜🟨⬜⬜
ZDBackup package	Win32/Heur	⬜⬜🟨⬜⬜
ZipGenius package	SHeur3.ACWU	⬜🟩⬜⬜⬜
ZTape package	Win32/Heur	🟩⬜⬜⬜⬜

TrustPort had 19 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
A2 package	TROJ_Generic.ADV	⬜⬜🟨⬜⬜
AirSnare package	TROJ_Generic	⬜🟩⬜⬜⬜
ArchiCrypt package	TROJ_Generic.ADV	⬜⬜🟨⬜⬜
BackupSlave package	TROJ_Generic.ADV	⬜⬜🟨⬜⬜
CompuSec package	TROJ_Generic.ADV	🟩⬜⬜⬜⬜
Cubase package	IRC_Generic	⬜⬜🟨⬜⬜
Datawest package	WORM_Generic	🟩⬜⬜⬜⬜
ExeProtect package	TROJ_DELF.PNI	⬜🟩⬜⬜⬜
FBench package	TROJ_Generic.ADV	🟩⬜⬜⬜⬜
FreshDow package	TROJ_Generic.ADV	⬜🟩⬜⬜⬜
GDATA package	TROJ_AGENT.AHDL	⬜🟩⬜⬜⬜
HelloPE package	TROJ_Generic.ADV	🟩⬜⬜⬜⬜
HP package	TROJ_Generic.ADV	🟩⬜⬜⬜⬜
HTTrack package	TROJ_Generic.ADV	⬜⬜🟨⬜⬜
NPP package	TROJ_Generic.ADV	⬜⬜🟨⬜⬜
PeaZip package	TROJ_Generic.ADV	⬜⬜🟨⬜⬜
SpyAgent package	TROJ_Generic.ADV	⬜🟩⬜⬜⬜
SSC package	BKDR_Generic	⬜⬜🟨⬜⬜
TCPFilter package	TROJ_Generic	⬜🟩⬜⬜⬜
TransMac package	BKDR_Generic	⬜🟩⬜⬜⬜
UPACK package	TROJ_Generic.ADV	⬜🟩⬜⬜⬜
VanDerLee package	TROJ_Generic.ADV	🟩⬜⬜⬜⬜
VS2000 package	TROJ_Generic.ADV	🟩⬜⬜⬜⬜

Trend Micro had 23 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
AirSnare package	W32/Sdbot.worm!g	⬜🟩⬜⬜⬜
Alteros3D package	Artemis!6C4512D72D3A	⬜🟩⬜⬜⬜
AppUpdater package	Artemis!D25193E90F3C	⬜🟩⬜⬜⬜
Autorota package	Generic BackDoor!csa	⬜⬜🟨⬜⬜
CCleaner package	Artemis!4408D3463A94	⬜⬜🟨⬜⬜
CrazyWords package	Artemis!A59406647069	⬜⬜🟨⬜⬜
DesktopSafe package	Artemis!EDAA712E946A	⬜🟩⬜⬜⬜
DivX package	Artemis!528974A8525E	⬜⬜⬜⬜🟥
DriveCleaner package	Artemis!C0DE050AF8BA	⬜⬜🟨⬜⬜
HitmanPro package	Artemis!79401AB126D2	⬜⬜🟨⬜⬜
JkDefrag package	Artemis!B3031EFBD8C0	⬜⬜⬜🟧⬜
Kino package	Artemis!517338AD94A0	⬜⬜🟨⬜⬜
maComfort package	Artemis!DEAE123B8282	⬜⬜🟨⬜⬜
MauMau package	Artemis!F5BFA83062ED	⬜⬜⬜🟧⬜
OperaTor package	Artemis!C4B5F5190E26	⬜🟩⬜⬜⬜
PacManiac package	Artemis!0F45B8FB7A16	⬜🟩⬜⬜⬜
PPmateTV package	Generic.dx	⬜⬜⬜🟧⬜
Rahmen package	X97M/Generic	🟩⬜⬜⬜⬜
TeaTimer package	Artemis!D2312566EC20	🟩⬜⬜⬜⬜
Tiscali package	Generic.dx!tdt	⬜🟩⬜⬜⬜
USBDeview package	Artemis!EE5595168557	⬜⬜🟨⬜⬜

WorldOfSoccer package	Puper.gen.ao	□🟩□□□
XenonFilemanager package	Artemis!88645494D347	□□□□🟥
XtremSchwimmen package	Artemis!0C45F6A55EE5	□□□🟧□

McAfee had 24 false alarms.

Kingsoft

False alarm found in some parts of	Detected as	Supposed prevalence
AfrikaKorps package	Win32.Troj.Generic.(kcloud)	□□🟨□□
AutoIt package	Win32.Troj.Agent	□□🟨□□
Autorota package	Win32.Hack.Delf.(kcloud)	□□🟨□□
BartStuff package	Win32.Troj.Generic	□□□□🟥
CPUFSB package	Win32.Troj.Generic	□□🟨□□
DeltaForce package	Win32.DroworT.a	□□□🟧□
DocuMind package	Win32.Troj.EncodeIe.ao.(kcloud)	🟩□□□□
DriveCleaner package	Win32.Troj.Agent.(kcloud)	□□🟨□□
DriveScribe package	Win32.Hack.DTR.14.14336.(kcloud)	□□□🟧□
DVDIdentifier package	Win32.Troj.Generic	□□□□🟥
Ewido package	Win32.Troj.Generic	□□🟨□□
FreeProcessManager package	Win32.Troj.Undef.(kcloud)	🟩□□□□
GifSplitter package	Win32.Troj.Swisyn.(kcloud)	□□🟨□□
HaloThirdFOV package	Win32.Troj.Vilsel.(kcloud)	□□🟨□□
HotPlug package	Win32.Troj.Unknown	□□🟨□□
ImpossibleCreatures package	Worm.Delf.bg	□□□🟧□
Kino package	Win32.Malware.Heur_Generic.A.(kcloud)	□□🟨□□
Min2Tray package	Win32.Troj.Undef	□🟩□□□
MyDriver package	Win32.Troj.Generic	□□□🟧□
MyUSB package	Win32.PSWTroj.GameOLx.cn.(kcloud)	□🟩□□□
No23Recorder package	Win32.RiskWare.PEBundle.49152	□□🟨□□
Pantaray package	Win32.Hack.NsAnti	□□🟨□□
Particles package	Win32.Troj.Depro	□🟩□□□
PEBuilder package	Win32.Troj.Generic.(kcloud)	□□□🟧□
PowerBullet package	Win32.Hack.Bredavi.(kcloud)	□□□🟧□
RegDefrag package	Win32.TrojDownloader.Agent.b.(kcloud)	□🟩□□□
SH package	Win32.Troj.Generic	□□🟨□□
SideBar package	Win32.Malware.Heur_Generic.A.(kcloud)	□□□□🟥
Speakonia package	Win32.PSWTroj.Kuang.k	□🟩□□□
SpeedUp package	Win32.Troj.Unknown	□□□🟧□
SpyAgent package	Win32.Troj.Dialer.61440.(kcloud)	□🟩□□□
SuperCopier package	Win32.Troj.Generic.(kcloud)	□□□🟧□
TeaTimer package	Worm.VB.(kcloud)	🟩□□□□
TubeCatcher package	Win32.Malware.Heur_Generic.A.(kcloud)	□□□🟧□
TweakAll package	Win32.Troj.ADClicker.(kcloud)	□□🟨□□
TweakNow package	Win32.Troj.KillFiles.mn.(kcloud)	□🟩□□□
TweakPower package	Win32.Troj.Agent.(kcloud)	□□🟨□□
UniversalExtractor package	Win32.Troj.Autoit.k.(kcloud)	□🟩□□□
VanDerLee package	Win32.Malware.Heur_Generic.A.(kcloud)	□🟩□□□
VisualStyler package	Win32.PSWTroj.QQPass.(kcloud)	□□🟨□□
Wget package	Win32.Malware.Heur_Generic.A.(kcloud)	□□🟨□□
Widget package	Win32.Troj.Delf.a.(kcloud)	□□🟨□□
WinSEO package	Win32.Malware.Heur_Generic.A.(kcloud)	□🟩□□□

ZipInstaller package	Win32.TrojDownloader.Delf.(kcloud)	⬜🟩⬜⬜⬜
Zuma package	Win32.Troj.Virtumonde.ak.(kcloud)	🟩⬜⬜⬜⬜

Kingsoft had 45 false alarms.

Kaspersky

False alarm found in some parts of	Detected as	Supposed prevalence
AddZip package	Backdoor.Win32.SdBot.tkv	⬜⬜⬜🟧⬜
AlohaTripeaks package	Trojan-Downloader.Win32.Agent.dckk	🟩⬜⬜⬜⬜
Autorota package	Backdoor.Win32.Delf.uss	⬜⬜🟨⬜⬜
BayWatchArchiver package	IM-Worm.Win32.Licat.ev	⬜🟩⬜⬜⬜
BricksOfEgypt package	Trojan-Downloader.Win32.Agent.ebbr	🟩⬜⬜⬜⬜
BrixOut package	Backdoor.Win32.Hupigon.jzlm	⬜🟩⬜⬜⬜
Buchdruck package	Trojan.Win32.Swisyn.ajgb	⬜🟩⬜⬜⬜
CDImage package	Trojan-Banker.Win32.Banker.ayws	⬜⬜🟨⬜⬜
Civilization3 package	Backdoor.Win32.Agent.axsz	⬜🟩⬜⬜⬜
CombineMP3 package	Backdoor.Win32.Bifrose.cuyq	⬜🟩⬜⬜⬜
CrazyWords package	Trojan-Clicker.Win32.VBiframe.ciq	⬜⬜🟨⬜⬜
CUEcards package	Trojan-Spy.Win32.Loxxee.n	⬜⬜🟨⬜⬜
Demolotion package	Trojan.Win32.Agent.evig	⬜⬜🟨⬜⬜
DriveCleaner package	Trojan.Win32.Agent.djoh	⬜⬜🟨⬜⬜
DriverGenius package	Backdoor.Win32.Bifrose.ctzd	⬜⬜🟨⬜⬜
EasyBurning package	SuspiciousPacker.Multi.Generic	⬜⬜🟨⬜⬜
Evolution package	Trojan.Win32.Vapsup.aaeb	🟩⬜⬜⬜⬜
Fabmail package	Email-Flooder.Win32.Agent.p	⬜🟩⬜⬜⬜
FileZilla package	Worm.Win32.Qvod.ark	⬜⬜🟨⬜⬜
FreeTV package	Trojan.Win32.Vilsel.ahqa	⬜⬜🟨⬜⬜
GifSplitter package	Trojan.Win32.Swisyn.afjj	⬜⬜🟨⬜⬜
HaloThirdFOV package	Trojan.Win32.Vilsel.whx	⬜⬜🟨⬜⬜
HiddenFinder package	Trojan-Spy.Win32.Loxxee.g	🟩⬜⬜⬜⬜
IceSword package	HEUR:Trojan.Win32.Generic	⬜⬜🟨⬜⬜
InkLevel package	Trojan.Win32.Inject.anhg	⬜🟩⬜⬜⬜
iTunesGenreManager package	Trojan-PSW.Win32.LdPinch.anpn	⬜🟩⬜⬜⬜
Lilypond package	HEUR:Trojan.Win32.Generic	🟩⬜⬜⬜⬜
Magiskin package	Trojan-Banker.Win32.Banker.atta	🟩⬜⬜⬜⬜
MauMau package	Trojan-Clicker.Win32.VBiframe.ctb	⬜⬜⬜🟧⬜
MobileAssistent package	Trojan.Win32.Delf.fqj	🟩⬜⬜⬜⬜
MultiSync package	Virus.DOS.Eddie	🟩⬜⬜⬜⬜
OperaTor package	Trojan.Win32.Antavmu.ikj	⬜🟩⬜⬜⬜
PacManiac package	Trojan-Clicker.Win32.VBiframe.crn	⬜🟩⬜⬜⬜
PopUpBlocker package	Worm.Win32.VBNA.b	⬜🟩⬜⬜⬜
PowerBullet package	Backdoor.Win32.Bredavi.cci	⬜⬜⬜🟧⬜
Preispiraten package	Trojan-GameThief.Win32.Tibia.gtq	⬜🟩⬜⬜⬜
RootkitUnhooker package	HEUR:Trojan.Win32.Generic	⬜🟩⬜⬜⬜
SH package	Trojan-GameThief.Win32.Lmir.mqw	⬜⬜⬜🟧⬜
Spamihilator package	Trojan-GameThief.Win32.OnLineGames.bnnu	⬜⬜🟨⬜⬜
StickyPassword package	Trojan.Win32.Pincav.ades	⬜🟩⬜⬜⬜
Stranded package	Trojan-Clicker.Win32.VBiframe.cui	⬜⬜🟨⬜⬜
TweakAlVirtualDub package	Trojan-Downloader.Win32.Agent.dunn	⬜⬜🟨⬜⬜
VokalbelMeister package	Backdoor.Win32.VB.lzq	⬜🟩⬜⬜⬜
xCAT package	Trojan-PSW.Win32.LdPinch.anlk	⬜🟩⬜⬜⬜

XtremSchwimmen package	Trojan-Clicker.Win32.VBiframe.coz	⬜⬜⬜🟧⬜
Zuma package	Trojan-Dropper.Win32.Delf.gjg	🟩⬜⬜⬜⬜

Kaspersky had 46 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
AccessCheck package	Riskware (001219651)	⬜⬜⬜🟧⬜
Amazons package	Riskware (fe1fad1e0)	⬜🟩⬜⬜⬜
AmericasArmy package	Riskware (edc396a10)	⬜⬜🟨⬜⬜
Anti-Trojan package	Trojan (786b06920)	🟩⬜⬜⬜⬜
Autorota package	Backdoor (0018f6ee1)	⬜⬜⬜🟧⬜
AVerTV package	Riskware (56e8029f0)	⬜⬜🟨⬜⬜
AZFinder package	Riskware (734f98cb0)	⬜🟩⬜⬜⬜
Backvoll package	Trojan (786b06920)	🟩⬜⬜⬜⬜
BitComet package	Trojan-Downloader (9ed232f20)	⬜⬜⬜⬜🟥
Bitdefender package	Trojan (000200f91)	⬜⬜🟨⬜⬜
BurnInTest package	Backdoor (d48b2eac0)	⬜🟩⬜⬜⬜
Cisco package	Trojan (000149d11)	⬜⬜🟨⬜⬜
Cyberlink package	Trojan (d4cd3f860)	⬜⬜⬜⬜🟥
Decoder package	Riskware (fcf7495a0)	⬜🟩⬜⬜⬜
DeepNet package	Riskware (ec90764d0)	⬜🟩⬜⬜⬜
DiaShowPro package	Trojan (9b83fd0b0)	⬜⬜🟨⬜⬜
DogsAndLights package	Virus (994159940)	⬜🟩⬜⬜⬜
DriveDir package	Riskware (0015e4f11)	⬜⬜⬜⬜🟥
EasyIndex package	Riskware (3c86d9f30)	🟩⬜⬜⬜⬜
eJay package	Trojan (74e546e10)	⬜⬜⬜⬜🟥
FTCheck package	Trojan (dd017b3c0)	⬜🟩⬜⬜⬜
GDATA package	Password-Stealer (a930d7ff0)	⬜🟩⬜⬜⬜
Glasklar package	Riskware (23a4be4c0)	⬜⬜🟨⬜⬜
GMER package	Riskware (eca15ce20)	🟩⬜⬜⬜⬜
Kaspersky package	Trojan (760635d30)	⬜🟩⬜⬜⬜
KLMCodec package	Trojan (0006fe361)	⬜⬜⬜⬜🟥
Lotus package	Unwanted-Program (6a1a0eb80)	🟩⬜⬜⬜⬜
Madden package	Riskware (683697770)	⬜⬜🟨⬜⬜
MatCode package	Trojan (0001140e1)	⬜⬜🟨⬜⬜
MorningsWrath package	Trojan (74e546e10)	⬜🟩⬜⬜⬜
MultiPatcher package	Riskware (0006fb5d1)	⬜🟩⬜⬜⬜
MusicMatch package	Trojan (57109e4b0)	⬜⬜⬜⬜🟥
Namo package	Trojan (d4cd3f860)	⬜🟩⬜⬜⬜
Notepad2 package	Riskware (0009efc41)	⬜🟩⬜⬜⬜
OllyDebug package	Trojan (6adcf5420)	⬜🟩⬜⬜⬜
PeID package	Trojan (a211401c0)	⬜⬜🟨⬜⬜
PowerBullet package	Backdoor (00149dfa1)	⬜⬜⬜🟧⬜
PrcView package	Trojan (0001140e1)	🟩⬜⬜⬜⬜
SafeXP package	Riskware (3c86d9f30)	⬜⬜🟨⬜⬜
SecretMaker package	Riskware (3c86d9f30)	⬜🟩⬜⬜⬜
SimCity package	Riskware (683697770)	⬜⬜⬜⬜🟥
SystemSafety package	Trojan (da2265540)	⬜🟩⬜⬜⬜
TeamViewer package	Trojan (120114b20)	⬜⬜⬜⬜🟥
Tetrix package	Virus (e55847090)	⬜⬜⬜🟧⬜

Thunderbird package	Trojan-Downloader (00117cc51)	□□□□🟥
TimeStampNow package	Trojan (000799ba1)	□□🟨□□
WGet package	Trojan-Downloader (000445931)	□□🟨□□
WinnerTweak package	Trojan (6f1012d10)	□🟩□□□
WinToy package	Trojan (6f93b2610)	□□🟨□□
Zattoo package	Trojan (0005c5d31)	□□□🟧□

K7 had 50 false alarms.

Norman

False alarm found in some parts of	Detected as	Supposed prevalence
AbiWord package	Suspicious_Gen.GPV	□□🟨□□
AddZip package	Agent.UVIQ	□□□🟧□
AIMFix package	W32/Malware	🟩□□□□
Anti-Trojan package	W32/Zbot.PVX	□□🟨□□
Atomaders package	W32/EMailWorm.ELY	□□🟨□□
Auklook package	SuspiciousPE.C.dropper	🟩□□□□
BenQ package	W32/Smalltroj.IKLW	□□□□🟥
BestOfExcel package	W32/Delf.FGMI	□□□🟧□
Bonnie package	ShellCode.M	🟩□□□□
CDDVDBurner package	Suspicious_Gen2.ACSXH	□🟩□□□
Chaser package	Suspicious_Gen2.BTKNN	□🟩□□□
CopyPod package	W32/Obfuscated.VPE	□🟩□□□
CyberLink package	W32/Malware.LOXO	□□□🟧□
Daemon package	W32/Suspicious_Gen2.dam.dropper	□□□🟧□
Darkfox package	W32/Dropper!gens.22139635	□🟩□□□
DeathEcstasy package	W32/Suspicious_Gen2.BSCPS	□🟩□□□
DMailer package	Malware.LNCP	🟩□□□□
DNS package	W32/Malware	□□🟨□□
DupeWipe package	W32/Packed_Upack.I	□□🟨□□
DVDinfo package	Delf.FGCH	🟩□□□□
DVDnextCopy package	Suspicious_Gen2.BQGGO	□□🟨□□
EastTec package	W32/Suspicious_Gen2.Q	□□□□🟥
EasyBurning package	W32/Packed_Upack.A	□□🟨□□
Favoriten package	Smalltroj.OHLB	□🟩□□□
Flux package	W32/Agent.MCVO	□□□□🟥
FolderAccess package	W32/VBTroj.CYAX	□□□🟧□
FreshDevices package	Smalltroj.XPWV	□🟩□□□
FreshDow package	Smalltroj.XPBM	□🟩□□□
GameSpy package	W32/EMailWorm.CML	□🟩□□□
GDATA package	OnLineGames.LSPQ	□🟩□□□
GDSChild package	W32/Obfuscated.F!genr	🟩□□□□
GetIt package	W32/Suspicious_Gen2.AQNHB	🟩□□□□
GliBlock package	W32/Suspicious_Gen2.BRBWN	□🟩□□□
HDDLife package	Malware.CBKD	□□🟨□□
iAlbum package	W32/DLoader.JBYO	□□🟨□□
ICEows package	W32/Suspicious_Gen.GFRR	🟩□□□□
IceSword package	W32/Obfuscated.R	□□🟨□□
ICQ package	W32/SubSeven.ADQ	□□□🟧□
iPing package	W32/Malware	🟩□□□□
IsoBuilder package	Suspicious_Gen2.AGRPB	□🟩□□□

Karafun package	Suspicious_Gen2.AGSWX	⬜⬜🟨⬜⬜
Kaspersky package	W32/Suspicious_Gen2.NMGE	🟩⬜⬜⬜⬜
Launchy package	W32/Obfuscated.Q!genr	⬜⬜🟨⬜⬜
Mandrake package	ShellCode.M	🟩⬜⬜⬜⬜
MediaInfo package	Agent.SDGI.dropper	⬜🟩⬜⬜⬜
MegaTreeSize package	W32/FakeAV.AD!genr	⬜🟩⬜⬜⬜
Min2Tray package	W32/Suspicious_Gen2.LBV	⬜🟩⬜⬜⬜
Mindsoft package	W32/Smalldoor.ECD	⬜🟩⬜⬜⬜
MiniPad package	W32/Obfuscated.AT!genr	⬜🟩⬜⬜⬜
MpegValid package	W32/Obfuscated.L	⬜🟩⬜⬜⬜
MSNMessenger package	W32/Smalltroj.CNYX	⬜⬜⬜🟧⬜
MuzicMan package	W32/Suspicious_Gen2.NIC	🟩⬜⬜⬜⬜
MyGallery package	W32/Agent.SBJQ	🟩⬜⬜⬜⬜
NetMeter package	W32/Delf.EXDN	⬜🟩⬜⬜⬜
NewWorldOrder package	W32/Suspicious_Gen.GYMD	⬜🟩⬜⬜⬜
Norton package	W32/Gamania.RQJ	🟩⬜⬜⬜⬜
OsoTour package	W32/Suspicious_Gen2.AMQIM	⬜🟩⬜⬜⬜
PeaZip package	W32/Suspicious_Gen2.VMUT	⬜⬜🟨⬜⬜
PingPlotter package	SuspiciousPE.C.dropper	⬜⬜🟨⬜⬜
PowerBullet package	Malware.DQBI	⬜⬜⬜🟧⬜
PPMateTV package	Suspicious_Gen2.DIFI	⬜⬜⬜🟧⬜
QText package	ShellCode.M	🟩⬜⬜⬜⬜
Radix package	Malware.KHQW	⬜🟩⬜⬜⬜
RealtimeBrowser package	Suspicious_Gen2.UYN	⬜🟩⬜⬜⬜
Roxio package	W32/Swizzor.KRFL	⬜⬜🟨⬜⬜
Sandboxie package	W32/Obfuscated.CM!genr	⬜⬜🟨⬜⬜
SecuniaPSI package	Suspicious_Gen2.ORWP	🟩⬜⬜⬜⬜
SimplyZip package	Suspicious_Gen3.AUAC	⬜⬜🟨⬜⬜
SmartProtector package	Malware.LQDB	⬜🟩⬜⬜⬜
SpiceWorks package	Suspicious_Gen2.XYNQ	⬜⬜⬜🟧⬜
SpyDetector package	Suspicious_Gen.FIEE	⬜🟩⬜⬜⬜
SpySweeper package	Suspicious_Gen2.NVAR	⬜🟩⬜⬜⬜
Steganos package	W32/Suspicious_Gen2.NMGE	⬜🟩⬜⬜⬜
SystemSafety package	W32/VBWorm.BCGE	⬜🟩⬜⬜⬜
TaskMan package	W32/Suspicious_Gen2.AAXM	⬜🟩⬜⬜⬜
TeaTimer package	Suspicious_Gen2.AGSWX	🟩⬜⬜⬜⬜
TempCleaner package	W32/Suspicious_Gen2.ADZTM	⬜⬜🟨⬜⬜
TheBAT package	W32/Banload.ALTG	⬜⬜🟨⬜⬜
ThunderBird package	Suspicious_Gen.GPV	⬜⬜🟨⬜⬜
Tiscali package	W32/Suspicious_Gen2.UACJ	⬜🟩⬜⬜⬜
TravelMedia package	W32/Suspicious_Gen2.IDLW	🟩⬜⬜⬜⬜
TrendMicro package	W32/Suspicious_Gen2.GJHP	⬜⬜⬜⬜🟥
TrueCrypt package	W32/Malware.LOXN	⬜🟩⬜⬜⬜
TTN package	W32/Obfuscated.L	⬜🟩⬜⬜⬜
TweakMP package	W32/Obfuscated.N!genr	⬜⬜⬜⬜🟥
TweakPower package	W32/Suspicious_Gen2.TRJB	⬜⬜🟨⬜⬜
Unreal package	W32/Suspicious_Gen2.QBUB	⬜⬜⬜⬜🟥
VLite package	Suspicious_Gen2.AAHTG	⬜⬜🟨⬜⬜
WGet package	W32/Suspicious_Gen2.TJIX	⬜⬜🟨⬜⬜
Widget package	W32/NetworkWorm	⬜⬜⬜🟧⬜
WinAudit package	W32/Suspicious_Gen2.RLTO	⬜⬜🟨⬜⬜
WinBuilder package	W32/Suspicious_Gen2.dam	⬜⬜⬜🟧⬜

WinFox package	W32/Tdss.B!genr	□□🟨□□
WinGate package	Suspicious_Gen3.OAH	□🟩□□□
WinnerTweak package	VBFlood.gen1	🟩□□□□
XLdatass package	Suspicious_Gen2.ZKBB	🟩□□□□
Yoono package	ShellCode.M	🟩□□□□
Zattoo package	Suspicious_Gen2.CNXY	□□□□🟥

Norman had 98 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
3DMuehle package	Suspicious file	□□🟨□□
3DScreensaver package	Generic Trojan	🟩□□□□
AddUnzip package	Suspicious file	□🟩□□□
AfrikaKorps package	Trj/CI.A	□□🟨□□
Aida package	Suspicious file	□□🟨□□
AllMyBooks package	Suspicious file	□□□🟧□
Archivarius package	Suspicious file	□🟩□□□
Atomaders package	Suspicious file	□□🟨□□
AutoIt package	Suspicious file	□□🟨□□
Autorota package	Suspicious file	□□🟨□□
AvantBrowser package	Suspicious file	□□🟨□□
Bazooka package	Suspicious file	□□□🟧□
Bemi package	Suspicious file	□🟩□□□
BleachBit package	Suspicious file	□□🟨□□
BMKBuddy package	Suspicious file	□🟩□□□
CDDVDBurning package	Suspicious file	□🟩□□□
CheosPyramide package	Suspicious file	□□🟨□□
Civilization3 package	Suspicious file	□🟩□□□
ClamWin package	Suspicious file	□□🟨□□
CopyPod package	Suspicious file	□🟩□□□
CyberLink package	Suspicious file	□□□🟧□
Datawest package	Suspicious file	🟩□□□□
Diskkeeper package	Suspicious file	□□🟨□□
DontPanic package	Suspicious file	□□🟨□□
DriverCleaner package	Suspicious file	□□🟨□□
DriveScribe package	Suspicious file	□□□🟧□
DupeWipe package	Suspicious file	□□🟨□□
DVDInfo package	Suspicious file	🟩□□□□
EasyBurning package	Suspicious file	□🟩□□□
Enigma package	Suspicious file	□□🟨□□
Ewido package	Suspicious file	□□□🟧□
Fabmail package	Suspicious file	□🟩□□□
Favoriten package	Suspicious file	□🟩□□□
FileWipe package	Suspicious file	🟩□□□□
Flux package	Suspicious file	□□□□🟥
FolderAccess package	Suspicious file	□□□🟧□
F-Secure package	Suspicious file	□□□🟧□
Gettysburg package	Suspicious file	□🟩□□□
Gnumeric package	Suspicious file	□🟩□□□
GTRacing package	Suspicious file	□🟩□□□

GXTrans package	Suspicious file	⬜🟩⬜⬜⬜
HaloThirdFOV package	Suspicious file	⬜⬜🟨⬜⬜
Hauppage package	Suspicious file	⬜⬜🟨⬜⬜
HitmanPro package	Suspicious file	⬜⬜🟨⬜⬜
HotPlug package	Suspicious file	⬜⬜🟨⬜⬜
IconHider package	Trj/Webmoner.O	⬜🟩⬜⬜⬜
iFTP package	Suspicious file	⬜⬜🟨⬜⬜
Kobil package	Suspicious file	🟩⬜⬜⬜⬜
MagiSkin package	Suspicious file	🟩⬜⬜⬜⬜
MP3Test package	Suspicious file	⬜⬜🟨⬜⬜
MP3toWAV package	Suspicious file	⬜⬜⬜🟧⬜
MyDriver package	Suspicious file	⬜⬜⬜🟧⬜
MyUSB package	Suspicious file	⬜🟩⬜⬜⬜
Netio package	W32/Feebs.CN.worm	🟩⬜⬜⬜⬜
NetMeter package	Suspicious file	⬜🟩⬜⬜⬜
Notepad2 package	Suspicious file	⬜🟩⬜⬜⬜
NTFSRRecovery package	Suspicious file	⬜🟩⬜⬜⬜
PCinIE package	Suspicious file	⬜🟩⬜⬜⬜
PDFExplorer package	Suspicious file	⬜🟩⬜⬜⬜
PeBuilder package	Suspicious file	⬜⬜⬜🟧⬜
PointPosition package	Trj/CI.A	⬜🟩⬜⬜⬜
PowerBullet package	Suspicious file	⬜⬜⬜🟧⬜
PowerStrip package	Suspicious file	⬜⬜🟨⬜⬜
Putty package	Suspicious file	🟩⬜⬜⬜⬜
Radix package	Suspicious file	⬜🟩⬜⬜⬜
Rainlendar package	Suspicious file	⬜⬜🟨⬜⬜
RegDefrag package	Suspicious file	⬜🟩⬜⬜⬜
Schriftenpaket package	Suspicious file	⬜⬜⬜🟧⬜
Scite package	Trj/CI.A	⬜⬜🟨⬜⬜
SlipStreamer package	Suspicious file	⬜⬜🟨⬜⬜
Spamihilator package	Suspicious file	⬜🟩⬜⬜⬜
SimplyZip package	Suspicious file	⬜⬜🟨⬜⬜
SpiceWorks package	Suspicious file	⬜⬜⬜🟧⬜
SpyAgent package	Suspicious file	⬜⬜🟨⬜⬜
StartupBooster package	Suspicious file	⬜⬜🟨⬜⬜
Steganos package	Suspicious file	⬜🟩⬜⬜⬜
StyleSelector package	Generic Backdoor	⬜⬜🟨⬜⬜
TransMac package	Generic Backdoor	⬜🟩⬜⬜⬜
TrojanHunter package	Suspicious file	⬜🟩⬜⬜⬜
TubeCatcher package	Suspicious file	⬜⬜⬜🟧⬜
TweakNow package	Suspicious file	⬜🟩⬜⬜⬜
TweakPower package	Suspicious file	⬜⬜🟨⬜⬜
Tworks package	Suspicious file	⬜🟩⬜⬜⬜
UltimateLoader package	Suspicious file	⬜🟩⬜⬜⬜
UniversalExtractor package	Suspicious file	⬜🟩⬜⬜⬜
uTorrent package	Suspicious file	⬜⬜🟨⬜⬜
VirtualKeyboard package	Suspicious file	⬜🟩⬜⬜⬜
VisualStyler package	Suspicious file	⬜⬜🟨⬜⬜
VLCPortable package	Suspicious file	⬜⬜⬜⬜🟥
VS2000 package	Suspicious file	🟩⬜⬜⬜⬜
Wget package	Suspicious file	⬜⬜🟨⬜⬜
WinBoard package	Generic Trojan	⬜🟩⬜⬜⬜

WinSEO package	Suspicious file	□🟩□□□
Winter package	Bck/Nirvana.199	🟩□□□□
xBBrowser package	Trj/StartPage.DIT	□□□🟥□
XmPlay package	Suspicious file	□🟩□□□
XtremSchwimmen package	Suspicious file	□□□🟥□
ZipInstaller package	Trj/CI.A	□🟩□□□

Panda had 98 false alarms.

Copyright and Disclaimer

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. (September 2010)