

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

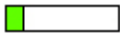




Details about the discovered false alarms

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 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.

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

- GTXTranscoder package
- iTunesGenreManager package
- PaperOffice package
- StereoscopicPlayer package
- WGet package
- xCAT package

Detected as

- Win32/Genetik
- Win32/PSW.LdPinch.ELMNSCM
- NewHeur_PE
- Win32/Packed.Themida
- Win32/Agent.EWTEPIN
- Win32/Packed.Themida

Supposed prevalence



ESET NOD32 had 6 false alarms.

PC Tools

False alarm found in some parts of

- 333 package
- GPGKeys package
- Lazarus package
- SmartNTFSRecovery package
- Tiscali package
- vDownloader package
- WGet package

Detected as

- Trojan.Gen
- Trojan.Generic
- HeurEngine.Vuntid
- Trojan.FakeAV!rem
- Trojan.Gen
- Trojan.ADH
- Trojan.Generic

Supposed prevalence



PC Tools had 7 false alarms.

Avast

False alarm found in some parts of

- Deluxanoid package
- FontTwister package
- HP driver package
- PacManiac package
- Retroremake package
- SpamAware package
- SpyDetector package
- Tiscali package
- TrendMicro package

Detected as

- Win32:Malware-gen
- Win32:Malware-gen
- VBS:Malware-gen
- Win32:Malware-gen
- Win32:Malware-gen
- Win32:Trojan-gen
- Win32:Genlot-GO
- Win32:Malware-gen
- Win32:Malware-gen

Supposed prevalence



Avast had 9 false alarms.

Symantec

False alarm found in some parts of

- AlienStars package
- CDDVDBurning package
- Lazarus package
- PhraseExpress package
- SimplyZip package
- SmartNTFSRecovery package
- TeaTimer package
- Tiscali package
- WGet package

Detected as

- Suspicious.MH690.A
- Suspicious.Cloud.AM
- Packed.Vuntid!gen1
- Suspicious.MH690.A
- Infostealer.Gampass
- Suspicious.Cloud.2
- Suspicious.Cloud.2
- Suspicious.Cloud.2
- Trojan Horse

Supposed prevalence



Symantec Norton Anti-Virus had 9 false alarms.

AVIRA

False alarm found in some parts of

Autorota package
 Backtec package
 DiaShowPro package
 FrogWares package
 GPU package
 GTRacingOleManager package
 PacManiac package
 SymplyZip package
 SpamFighter package
 TrendMicro package

Detected as

BDS/Delf.uss
 TR/Dropper.Gen
 DR/Agent.7066624
 TR/PSW.Lmir.1531964
 TR/Dldr.Delphi.Gen
 TR/Spy.Gen
 TR/Click.VBiframe.crn
 TR/Agent.2274937
 TR/Dropper.Gen
 HTML/Rce.Gen

Supposed prevalence



AVIRA had 10 false alarms.

Sophos

False alarm found in some parts of

AurTech package
 Ewido package
 FireMonitor package
 InternetExplorer8 package
 PlainPaste package
 RegHeal package
 Rohos package
 SuperCopier package
 TheMusicLoader package
 Toucan package
 VideoAccelerator package
 XPizeReloader package
 ZDATABurn package

Detected as

Mal/Generic-A
 Mal/Generic-A
 Mal/Generic-A
 Mal/Generic-A
 Mal/Generic-A
 Mal/Delf-AR
 Mal/Generic-A
 Mal/VBDldr-B
 Mal/Generic-A
 Mal/Generic-A
 Mal/BredoZp-B
 Mal/Generic-A

Supposed prevalence



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

Deluxanoid package
 DiaShowPro package
 DrawingHands package
 DZip package
 FontTwister package
 HP driver package
 Lilypond package
 Pacmaniac package
 RetroRemake package
 SpamAware package
 SpyDetector package
 Tiscali package
 TorChat package
 TrendMicro package
 WGet package

Detected as

Win32:Malware-gen
 Win32:Dropper-CMZ
 Win32:Trojan-gen
 Gen:Trojan.Heur.UT.gmW@bKZeeIei
 Win32:Malware-gen
 VBS:Malware-gen
 Gen:Trojan.Heur.FU.iCZ@aeqi9dli
 Win32:Malware-gen
 Win32:Malware-gen
 Win32:Trojan-gen
 Win32:Genlot-GO
 Win32:Malware-gen
 Gen:Trojan.Heur.km5@@hk@5Ve
 Win32:Malware-gen
 Trojan.Generic.3887481

Supposed prevalence



G DATA had 15 false alarms.

AVG

False alarm found in some parts of

Aspell package
 Autorota package
 CurrentPorts package
 Dmailer package
 EasyBurn package
 ESET package
 FreeProcessManager package
 HaloThirdFOV package
 InControl package
 InfoCenter package
 PlanetMP3 package
 PunicWars package
 TeaTimer package
TrendMicro package
 VirtualKeyboard package
 WinRAR package
 ZDBackup package
 ZipGenius package
 ZTape package

Detected as

Downloader.Obfuskated
 BackDoor.Generic12.CBVX
 Generic18.BOIK
 SHeur3.BMQ
 Generic10.QFQ
 Win32/Heur
 Generic17.ASIR
 Generic17.RSG
 Generic17.LIY
 Script/Exploit
 IRC/BackDoor.SdBot4.RVB
 SHeur3.GVT
 Win32/Heur
BackDoor.Ircbot.MNQ
 Dropper.Generic2.KPZ
 PSW.Generic8.KYY
 Win32/Heur
 SHeur3.ACWU
 Win32/Heur

Supposed prevalence



AVG had 19 false alarms.

TrustPort

False alarm found in some parts of

Autorota package
 DMailer package
 DZip package
 EasyBurn package
 ESET package
 FreeProcessManager package
 InControl package
 Lilypond package
 PlanetMP3 package
 PunicWars package
 TeaTimer package
 TorChat package
TrendMicro package
 VirtualKeyboard package
 Wget package
 WinRAR package
 ZDBackup package
 ZipGenius package
 ZTape package

Detected as

BackDoor.Generic12.CBVX
 SHeur3.BMQ
 Gen:Trojan.Heur.UT.gmW@bKZeeIei
 Generic10.QFQ
 Win32/Heur
 Generic17.ASIR
 Generic17.LIY
 Gen:Trojan.Heur.FU.iCZ@aeqi9dli
 IRC/BackDoor.SdBot4.RVB
 SHeur3.GVT
 Win32/Heur
 Gen:Trojan.Heur.km5@@hk@5Ve
BackDoor.Ircbot.MNQ
 Dropper.Generic2.KPZ
 Trojan.Generic.3887481
 PSW.Generic8.KYY
 Win32/Heur
 SHeur3.ACWU
 Win32/Heur

Supposed prevalence



TrustPort had 19 false alarms.

Trend Micro

False alarm found in some parts of

- A2 package
- AirSnare package
- ArchiCrypt package
- BackupSlave package
- CompuSec package
- Cubase package
- Datawest package
- ExeProtect package
- FBench package
- FreshDow package
- GDATA package
- HelloPE package
- HP package
- HTTrack package
- NPP package
- PeaZip package
- SpyAgent package
- SSC package
- TCPFilter package
- TransMac package
- UPACK package
- VanDerLee package
- VS2000 package

Detected as

- TROJ_Generic.ADV
- TROJ_Generic
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- IRC_Generic
- WORM_Generic
- TROJ_DELF.PNI
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_AGENT.AHDL
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- BKDR_Generic
- TROJ_Generic
- BKDR_Generic
- TROJ_Generic.ADV
- TROJ_Generic.ADV
- TROJ_Generic.ADV

Supposed prevalence



Trend Micro had 23 false alarms.

McAfee

False alarm found in some parts of

- AirSnare package
- Alteros3D package
- AppUpdater package
- Autorota package
- CCleaner package
- CrazyWords package
- DesktopSafe package
- DivX package
- DriveCleaner package
- HitmanPro package
- JkDefrag package
- Kino package
- maComfort package
- MauMau package
- OperaTor package
- PacManiac package
- PPmateTV package
- Rahmen package
- TeaTimer package
- Tiscali package
- USBDeview package

Detected as

- W32/Sdbot.worm!g
- Artemis!6C4512D72D3A
- Artemis!D25193E90F3C
- Generic BackDoor!csa
- Artemis!4408D3463A94
- Artemis!A59406647069
- Artemis!EDAA712E946A
- Artemis!528974A8525E
- Artemis!CODE050AF8BA
- Artemis!79401AB126D2
- Artemis!B3031EFBD8C0
- Artemis!517338AD94A0
- Artemis!DEAE123B8282
- Artemis!F5BFA83062ED
- Artemis!C4B5F5190E26
- Artemis!0F45B8FB7A16
- Generic.dx
- X97M/Generic
- Artemis!D2312566EC20
- Generic.dx!tdt
- Artemis!EE5595168557

Supposed prevalence



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

- AfrikaKorps package
- AutoIt package
- Autorota package
- BartStuff package
- CPUFSB package
- DeltaForce package
- DocuMind package
- DriveCleaner package
- DriveScribe package
- DVDIdentifier package
- Ewido package
- FreeProcessManager package
- GifSplitter package
- HaloThirdFOV package
- HotPlug package
- ImpossibleCreatures package
- Kino package
- Min2Tray package
- MyDriver package
- MyUSB package
- No23Recorder package
- Pantaray package
- Particles package
- PEBuilder package
- PowerBullet package
- RegDefrag package
- SH package
- SideBar package
- Speakonia package
- SpeedUp package
- SpyAgent package
- SuperCopier package
- TeaTimer package
- TubeCatcher package
- TweakAll package
- TweakNow package
- TweakPower package
- UniversalExtractor package
- VanDerLee package
- VisualStyler package
- Wget package
- Widget package
- WinSEO package

Detected as

- Win32.Troj.Generic.(kcloud)
- Win32.Troj.Agent
- Win32.Hack.Delf.(kcloud)
- Win32.Troj.Generic
- Win32.Troj.Generic
- Win32.DroworT.a
- Win32.Troj.EncodeIe.ao.(kcloud)
- Win32.Troj.Agent.(kcloud)
- Win32.Hack.DTR.14.14336.(kcloud)
- Win32.Troj.Generic
- Win32.Troj.Generic
- Win32.Troj.Undef.(kcloud)
- Win32.Troj.Swisyn.(kcloud)
- Win32.Troj.VilSel.(kcloud)
- Win32.Troj.Unknown
- Worm.Delf.bg
- Win32.Malware.Heur_Generic.A.(kcloud)
- Win32.Troj.Undef
- Win32.Troj.Generic
- Win32.PSWTroj.GameOLx.cn.(kcloud)
- Win32.RiskWare.PEBundle.49152
- Win32.Hack.NsAnti
- Win32.Troj.Depro
- Win32.Troj.Generic.(kcloud)
- Win32.Hack.Bredavi.(kcloud)
- Win32.TrojDownloader.Agent.b.(kcloud)
- Win32.Troj.Generic
- Win32.Malware.Heur_Generic.A.(kcloud)
- Win32.PSWTroj.Kuang.k
- Win32.Troj.Unknown
- Win32.Troj.Dialer.61440.(kcloud)
- Win32.Troj.Generic.(kcloud)
- Worm.VB.(kcloud)
- Win32.Malware.Heur_Generic.A.(kcloud)
- Win32.Troj.ADClicker.(kcloud)
- Win32.Troj.KillFiles.mn.(kcloud)
- Win32.Troj.Agent.(kcloud)
- Win32.Troj.Autoit.k.(kcloud)
- Win32.Malware.Heur_Generic.A.(kcloud)
- Win32.PSWTroj.QQPass.(kcloud)
- Win32.Malware.Heur_Generic.A.(kcloud)
- Win32.Troj.Delf.a.(kcloud)
- Win32.Malware.Heur_Generic.A.(kcloud)

Supposed prevalence



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

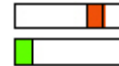
Detected as

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.aueb	
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
Zuma package

Trojan-Clicker.Win32.VBiframe.coz
Trojan-Dropper.Win32.Delf.gjj



Kaspersky had 46 false alarms.

K7

False alarm found in some parts of

AccessCheck package

Amazons package

AmericasArmy package

Anti-Trojan package

Autorota package

AVerTV package

AZFinder package

Backvoll package

BitComet package

Bitdefender package

BurnInTest package

Cisco package

Cyberlink package

Decoder package

DeepNet package

DiaShowPro package

DogsAndLights package

DriveDir package

EasyIndex package

eJay package

FTCheck package

GDATA package

Glasklar package

GMER package

Kaspersky package

KLMCodec package

Lotus package

Madden package

MatCode package

MorningsWrath package

MultiPatcher package

MusicMatch package

Namo package

Notepad2 package

OllyDebug package

PeID package

PowerBullet package

PrcView package

SafeXP package

SecretMaker package

SimCity package

SystemSafety package

TeamViewer package

Tetrix package

Detected as

Riskware (001219651)

Riskware (fe1fad1e0)

Riskware (edc396a10)

Trojan (786b06920)

Backdoor (0018f6ee1)

Riskware (56e8029f0)

Riskware (734f98cb0)

Trojan (786b06920)

Trojan-Downloader (9ed232f20)

Trojan (000200f91)

Backdoor (d48b2eac0)

Trojan (000149d11)

Trojan (d4cd3f860)

Riskware (fcf7495a0)

Riskware (ec90764d0)

Trojan (9b83fd0b0)

Virus (994159940)

Riskware (0015e4f11)

Riskware (3c86d9f30)

Trojan (74e546e10)

Trojan (dd017b3c0)

Password-Stealer (a930d7ff0)

Riskware (23a4be4c0)

Riskware (eca15ce20)

Trojan (760635d30)

Trojan (0006fe361)

Unwanted-Program (6a1a0eb80)

Riskware (683697770)

Trojan (0001140e1)

Trojan (74e546e10)

Riskware (0006fb5d1)

Trojan (57109e4b0)

Trojan (d4cd3f860)

Riskware (0009efc41)

Trojan (6adcf5420)

Trojan (a211401c0)

Backdoor (00149dfa1)

Trojan (0001140e1)

Riskware (3c86d9f30)

Riskware (3c86d9f30)

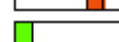
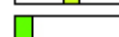
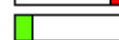
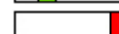
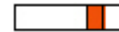
Riskware (683697770)

Trojan (da2265540)

Trojan (120114b20)

Virus (e55847090)

Supposed prevalence



Thunderbird package
 TimeStampNow package
 WGet package
 WinnerTweak package
 WinToy package
 Zattoo package

Trojan-Downloader (00117cc51)
 Trojan (000799ba1)
 Trojan-Downloader (000445931)
 Trojan (6f1012d10)
 Trojan (6f93b2610)
 Trojan (0005c5d31)



K7 had 50 false alarms.

Norman

False alarm found in some parts of

AbiWord package
 AddZip package
 AIMFix package
 Anti-Trojan package
 Atomaders package
 Auklook package
 BenQ package
 BestOfExcel package
 Bonnie package
 CDDVDBurner package
 Chaser package
 CopyPod package
 CyberLink package
 Daemon package
 Darkfox package
 DeathEcstasy package
 DMailer package
 DNS package
 DupeWipe package
 DVDinfo package
 DVDnextCopy package
 EastTec package
 EasyBurning package
 Favoriten package
 Flux package
 FolderAccess package
 FreshDevices package
 FreshDow package
 GameSpy package
 GDATA package
 GDSchild package
 GetIt package
 GliBlock package
 HDDLife package
 iAlbum package
 ICEows package
 IceSword package
 ICQ package
 iPing package
 IsoBuilder package

Detected as

Suspicious_Gen.GPV
 Agent.UVIQ
 W32/Malware
 W32/Zbot.PVX
 W32/EMailWorm.ELY
 SuspiciousPE.C.dropper
 W32/Smalltroj.IKLW
 W32/Delf.FGMI
 ShellCode.M
 Suspicious_Gen2.ACSXH
 Suspicious_Gen2.BTKNN
 W32/Obfuscated.VPE
 W32/Malware.LOXO
 W32/Suspicious_Gen2.dam.dropper
 W32/Dropper!gens.22139635
 W32/Suspicious_Gen2.BSCPS
 Malware.LNCP
 W32/Malware
 W32/Packed_Upack.I
 Delf.FGCH
 Suspicious_Gen2.BQGGO
 W32/Suspicious_Gen2.Q
 W32/Packed_Upack.A
 Smalltroj.OHLB
 W32/Agent.MCVO
 W32/VBTroj.CYAX
 Smalltroj.XPWV
 Smalltroj.XPBM
 W32/EMailWorm.CML
 OnLineGames.LSPQ
 W32/Obfuscated.F!genr
 W32/Suspicious_Gen2.AQNHB
 W32/Suspicious_Gen2.BRBWN
 Malware.CBKD
 W32/DLoader.JBYO
 W32/Suspicious_Gen.GFRR
 W32/Obfuscated.R
 W32/SubSeven.ADQ
 W32/Malware
 Suspicious_Gen2.AGRP

Supposed prevalence



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	

GXTrans package	Suspicious file	
HaloThirdFOV package	Suspicious file	
Hauppage package	Suspicious file	
HitmanPro package	Suspicious file	
HotPlug package	Suspicious file	
IconHider package	Trj/Webmoner.0	
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/Feeps.CN.worm	
NetMeter package	Suspicious file	
Notepad2 package	Suspicious file	
NTFSRRRecovery 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	
Works 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
Winter package
xBrowser package
XmPlay package
XtremSchwimmen package
ZipInstaller package

Suspicious file
Bck/Nirvana.199
Trj/StartPage.DIT
Suspicious file
Suspicious file
Trj/CI.A



Panda had 98 false alarms.

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. (September 2010)