

Details about the discovered False Alarms



Appendix to the Anti-Virus Comparative March 2015

Language: English

March 2015

Last Revision: 30th April 2015


www.av-comparatives.org

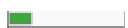



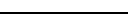
Details about the discovered false alarms

With AV testing it is important to measure not only detection capabilities but also reliability. One aspect of reliability is the ability to recognize clean files as such, and not produce false alarms (false positives). No product is immune from false positives (FPs), but some produce more than others, and the our goal is to find out which programs do best in this respect. There is no complete collection of all legitimate files that exist, and so no "ultimate" test of FPs can be done. What can be done, and is reasonable, is to create and use a set of clean files which is independently collected. If with such a set one product has e.g. 30 FPs and another only 5, it is likely that the first product is more prone to FP's than the other. It doesn't mean the product with 5 FPs doesn't have more than 5 FPs globally, but it is the relative number that is important.

All listed false alarms were encountered at the time of testing. False alarms caused by unencrypted data blocks in anti-virus related files were not counted. If a product had several false alarms belonging to the same software, it is counted here as only one false alarm. Cracks, keygens, etc. or other highly questionable tools, including FPs distributed/shared primarily by vendors (which may be in the several thousands) or other non-independent sources are not counted here as false positives.

In order to give more information to the users about the false alarms, we try to rate the prevalence of the false alarms. Files which were digitally signed are considered more important. Due to that, a file with e.g. prevalence "level 1" and a valid digital signature is upgraded to the next level (e.g. prevalence "level 2"). Files which according to several telemetry sources had zero prevalence have been provided to the vendors in order to fix them, but have also been removed from the set and were not counted as false alarms.

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

Level	Presumed number of affected users	Comments
1 	Probably fewer than hundred users	Individual cases, old or rarely used files, unknown prevalence
2 	Probably several hundreds of users	Initial distribution of such files was probably much higher, but current usage on actual systems is lower (despite its presence), that is why also well-known software may now affect / have only a prevalence of some hundreds or thousands of users.
3 	Probably several thousands of users	
4 	Probably several tens of thousands (or more) of users	
5 	Probably several hundreds of thousands or millions of users	Such cases are likely to be seen much less frequently in a false alarm test done at a specific time, as such files are usually either whitelisted or would be noticed and fixed very fast.

Most false alarms will probably fall into the first two levels most of the time. In our opinion, anti-virus products should not have false alarms on any sort of clean files regardless of how many users are currently affected by them. While some AV vendors may play down the risk of false alarms and play up the risk of malware, we are not going to rate products based on what the supposed prevalence of false alarms is. We already allow a certain amount of false alarms (currently 10) inside our clean set before we start penalizing scores, and in our opinion products which produce a higher amount of false alarms are also more likely to produce false alarms on more prevalent files (or in other sets of clean files). The prevalence data we give about clean files is just for informational purpose. The listed prevalence can differ inside the report, depending on which file/version the false alarm occurred, and/or how many files of the same kind were affected.


Some products using third-party engines/signatures may have fewer or more false alarms than the licensed engine has by its own, e.g. due to different internal settings implemented, the additional checks/engines/clouds/signatures, whitelist databases, time delay between the release of the original signatures and the availability of the signatures for third-party products, additional quality assurance of signatures before release, etc.

False Positives (FPs) are an important measurement for AV quality. One FP report from a customer can result in large amount of engineering and support work to resolve the issue. Sometimes this can even lead to important data loss or system unavailability. Even “not significant” FPs (or FPs on old applications) deserve mention and attention because FPs are likely to be a result of principled rule detections. It just happened that the FP was on an insignificant file. The FP possibility is probably still in the product and could cause an FP again on a more significant file. Thus, they still deserve mention and still deserve to be penalised. Below you will find the false alarms we observed in our independent set of clean files. Red entries highlight false alarms on files that were digitally signed.

Microsoft


Microsoft had zero false alarms on the used set of clean files.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
XPwinExit package	a variant of Win32/Injector.BTTD trojan	




ESET had 1 false alarm.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
XEmacs package	Mal_DRPR-3	







Trend Micro had 1 false alarm.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
AmericanConquest package	Unknown name	
MedBild package	Unknown name	
MonkeyPhoto package	Unknown name	

Panda had 3 false alarms.

Fortinet

False alarm found in some parts of	Detected as	Supposed prevalence
Audatex package	W32/Injector.ADYQ!tr	
BPMMSec package	W32/Generic.AC.1159	
CleanRegistry package	W32/Banker.QY!tr.spy	
FLVConverter package	W32/Spy.BANCOS.OKV!tr	
Frisk package	W32/Swizzor.fam!tr	
Incomedia package	PossibleThreat.SB!tr.dldr	

Fortinet had 6 false alarms.

Sophos

False alarm found in some parts of	Detected as	Supposed prevalence
Brockhaus package	Mal/Generic-S	
Deadtimestories package	Mal/Generic-S	
MSIDriver package	Mal/Generic-S	
OneScreensaver package	Mal/EncPk-ABFO	
SeaMonkey package	Mal/EncPk-BW	
SimplePaint package	Mal/FakeAV-OZ	
WWFdesktop package	Mal/Packer	
Youngsoft package	Mal/Generic-S	

Sophos had 8 false alarms.

Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Adobe package	HEUR/Malware	
Avast package	WORM/Agent.CT	
BricksOfEgypt package	TR/Agent.155648.405	
ClientSlave package	TR/Dropper.Gen	
HighwayNights package	TR/Crypt.ZPACK.95941	
ImperialGlory package	TR/Dropper.A.33996	
NXsetup package	HEUR/Crypted	
OpenOffice package	HEUR/Malware	

Tencent had 8 false alarms.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
CrazyTaxi package	Gen:Variant.Strictor.77227	
CrystalCave package	Backdoor.Generic.714455	
FotoOrganizer package	Gen:Variant.Symmi1.228	
GKAS package	Gen:Variant.Symmi.47767	
Google package	Trojan.Generic.12790599	
LegoStarWars package	Gen:Variant.Symmi.47430	
Poker package	Gen:Variant.Kazy.536383	
Ringtone package	Gen:Variant.Kazy.502936	
XPauto package	Gen:Variant.Kazy.142120	

Bitdefender had 9 false alarms.

Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
CircleDock package	UDS:DangerousPattern.Multi.Generic	
Epson package	HEUR:Trojan.Win32.Generic	
HTTPsync package	HEUR:Trojan.Win32.Generic	
MeteoCom package	HEUR:Trojan.Win32.Generic	
PostInstall package	UDS:DangerousObject.Multi.Generic	
RC4 package	HEUR:Trojan.Win32.Generic	
Snare package	HEUR:Trojan.Win32.Generic	
YAW package	UDS:DangerousObject.Multi.Generic	
ZDBackup package	HEUR:Trojan.Win32.Generic	

Kaspersky Lab had 9 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
AutoHotKey package	Artemis!83FB8A32927A	
GTRacing package	Artemis!31B5EBDA2AAD	
HP package	Trojan-FBOH!6FB3AEEB38F4	
Mohrhuhn package	Artemis!767E5F253F06	
OneScreensaver package	Artemis!DEE40159D0EC	
Photoshop package	Artemis!3B23F0BD6FCD	
Portraiture package	Artemis!273DE16FDE7B	
Tetrix package	Artemis!E476082178DE	
WinAmpPlugins package	Artemis!4FD7D505937F	
WWFdesktop package	Artemis!31D52F2B65FF	

McAfee had 10 false alarms.

AVG

False alarm found in some parts of	Detected as	Supposed prevalence
ApplicationService package	Generic11_c.AZXT	
DSLspeed package	Win32/Heur	
GTRacing package	Generic11_c.BTKZ	
HandyPack package	SHeur4.CFIO	
IcyTower package	Worm/Pakes.BXJ	
Kleptomania package	PSW.Generic12.BA0B	
MacType package	Downloader.Banload2.WCS	
NXsetup package	Win32/Heur	
Rechnungsdruckerei package	SHeur4.CBOR	
TeraCopy package	Agent4.AVA0	
Thinkpad package	ScreenLocker_s.ARO	
VirtualCD package	ScreenLocker_s.ARO	
Wingate package	BackDoor.Generic18.BCSP	
Xplosiv package	PSW.Agent.BHHR	

AVG had 14 false alarms.

Emsisoft

False alarm found in some parts of	Detected as	Supposed prevalence
ATI package	Trojan.Generic.12750903	
Casino package	Trojan.GenericKD.2082750	
CrazyTaxi package	Gen:Variant.Strictor.77227	
CrystalCave package	Backdoor.Generic.714455	
Driver package	Trojan.Generic.11905838	
eHome package	Trojan.Generic.12555279	
GotoOrganizer package	Gen:Variant.Symmi1.228	
GKAS package	Gen:Variant.Symmi.47767	
Google package	Trojan.Generic.12790599	
InstantOnUtilities package	Trojan.Generic.12376189	
LegoStarWars package	Gen:Variant.Symmi.47430	
Leitz package	Trojan.Generic.12315026	
Poker package	Gen:Variant.Kazy.536383	
Ringtone package	Gen:Variant.Kazy.502936	
Translator package	Trojan.Generic.12322173	

XPauto package	Gen:Variant.Kazy.142120	
----------------	-------------------------	--

Emsisoft had 16 false alarms.

BullGuard

False alarm found in some parts of	Detected as	Supposed prevalence
ATI package	Variant.Kazy.142120	
Casino package	Trojan.GenericKD.2082750	
CrazyTaxi package	Variant.Strictor.77227	
CrystalCave package	Backdoor.Generic.714455	
Driver package	Trojan.Generic.11905838	
eHome package	Trojan.Generic.12555279	
FotoOrganizer package	Gen:Variant.Symmi1.228	
GKAS package	Gen:Variant.Symmi.47767	
Google package	Trojan.Generic.12790599	
GTRacing package	Trojan.Generic.12221544	
InstantOnUtilities package	Trojan.Generic.12376189	
LegoStarWars package	Gen:Variant.Symmi.47430	
Leitz package	Trojan.Generic.12315026	
MSI package	Trojan.Generic.12742304	
MyPhoneExplorer package	Android.Trojan.SMSSend.AAH	
Poker package	Gen:Variant.Kazy.536383	
Ringtone package	Gen:Variant.Kazy.502936	
Translator package	Trojan.Generic.12322173	
XPauto package	Variant.Kazy.142120	

BullGuard had 19 false alarms.

eScan

False alarm found in some parts of	Detected as	Supposed prevalence
ATI package	Trojan.Generic.12750903 (DB)	
Casino package	Trojan.GenericKD.2082750 (DB)	
CrazyTaxi package	Gen:Variant.Strictor.77227 (DB)	
CrystalCave package	Backdoor.Generic.714455[ZP] (DB)	
Driver package	Trojan.Generic.11905838 (DB)	
eHome package	Trojan.Generic.12555279 (DB)	
FotoOrganizer package	Gen:Variant.Symmi1.228 (DB)	
GKAS package	Gen:Variant.Symmi.47767[ZP] (DB)	
Google package	Trojan.Generic.12790599 (DB)	
GTRacing package	Trojan.Generic.12221544[ZP] (DB)	
InkScape package	eScan.Cloud.Suspicious.2817 (ES)	
InstantOnUtilities package	Trojan.Generic.12376189 (DB)	
LegoStarWars package	Gen:Variant.Symmi.47430 (DB)	
Leitz package	Trojan.Generic.12315026 (DB)	
MSI package	Trojan.Generic.12742304[ZP] (DB)	
Poker package	Gen:Variant.Kazy.536383 (DB)	
Ringtone package	Gen:Variant.Kazy.502936[ZP] (DB)	
Translator package	Trojan.Generic.12322173[ZP] (DB)	
XPauto package	Gen:Variant.Kazy.142120 (DB)	

eScan had 19 false alarms.

F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
BestPractice package	Suspicious:W32/Malware.dfd5128b8e!Online	
CrazyTaxi package	Gen:Variant.Strictor.77227	
CrystalCave package	Backdoor.Generic.714455	
DigiFoto package	Suspicious:W32/Malware.4c6d06c8eb!Online	
Driver package	Trojan.Generic.11905838	
eHome package	Trojan.Generic.12555279	
FotoOrganizer package	Suspicious:W32/Malware.8f1f259c57!Online	
GKAS package	Gen:Variant.Symmi.47767	
Helium package	Suspicious:W32/Malware.e8e7ed8448!Online	
InstantOnUtilities package	Suspicious:W32/Malware.9fdecadaf6!Online	
InterVideo package	Backdoor:W32/Gen2365.69f76a6dbe!Online	
iTunesExport package	Suspicious:W32/Malware.0debee829b!Online	
LegoStarWars package	Gen:Variant.Symmi.47430	
MyPhoneExplorer package	Android.Trojan.SMSSend.AAH	
PDFserver package	Trojan:W32/Gen2139.faa49fd666!Online	
Poker package	Gen:Variant.Kazy.536383	
SpySweep package	Suspicious:W32/Malware.6e362a455c!Online	
TempControl package	Suspicious:W32/Malware.afa07e621b!Online	
XPauto package	Gen:Variant.Kazy.142120	

F-Secure had 19 false alarms.

Lavasoft

False alarm found in some parts of	Detected as	Supposed prevalence
ATI package	Variant.Kazy.142120	
Casino package	Trojan.GenericKD.2082750	
CrazyTaxi package	Variant.Strictor.77227	
CrystalCave package	Backdoor.Generic.714455	
Driver package	Trojan.Generic.11905838	
eHome package	Trojan.Generic.12555279	
FotoOrganizer package	Gen:Variant.Symmi1.228	
GKAS package	Gen:Variant.Symmi.47767	
Google package	Trojan.Generic.12790599	
GTRacing package	Trojan.Generic.12221544	
InstantOnUtilities package	Trojan.Generic.12376189	
LegoStarWars package	Gen:Variant.Symmi.47430	
Leitz package	Trojan.Generic.12315026	
MSI package	Trojan.Generic.12742304	
MyPhoneExplorer package	Android.Trojan.SMSSend.AAH	
Poker package	Gen:Variant.Kazy.536383	
Ringtone package	Gen:Variant.Kazy.502936	
Translator package	Trojan.Generic.12322173	
XPauto package	Variant.Kazy.142120	

Lavasoft had 19 false alarms.

Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
ATI package	EE:Malware.Generic.12750903	

Casino package	EE:Malware.GenericKD.2082750	
CrazyTaxi package	EE:Malwr.Heur.Strictor.77227	
CrystalCave package	EE:Malware.Generic.714455	
Ctnot package	File is suspicious	
DocServer package	EE:Malware.Generic.12338489	
Driver package	EE:Malware.Generic.11905838	
eHome package	EE:Malware.Generic.12555279	
FotoOrganizator package	EE:Malwr.Heur.Symmi1.228	
GenHTML package	W97M.Dropper.D	
GKAS package	EE:Malwr.Heur.Symmi.47767	
Google package	EE:Malware.Generic.12790599	
InfinityTexturs package	EE:Malware.Generic.12489781	
InstantOnUtilities package	EE:Malware.Generic.12376189	
LegoStarWars package	EE:Malwr.Heur.Symmi.47430	
Leitz package	EE:Malware.Generic.12315026	
MyPhoneExplorer package	EE:Android.Trojan.SMSSend.AAH	
OpenIn package	VBS.SsiWg	
Poker package	EE:Malwr.Heur.Kazy.536383	
PortableApps package	W32.HLLW.Plea.A	
Replacer package	File is suspicious	
Ringtone package	EE:Malwr.Heur.Kazy.502936	
Stuffpad package	File is suspicious	
Translator package	EE:Malware.Generic.12322173	
WinRAR package	TrojanSpy.Bancos.B	
WinSolution package	VBS.SsiWg	
WINtory package	EE:Malwr.Heur.Barys.2984	
XPauto package	EE:Malwr.Heur.Kazy.142120	

Quickheal had 28 false alarms.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
3DAlbum package	TR/Agent.2872320.2	
Acer package	HEUR/APC (Cloud)	
ACR package	HEUR/APC (Cloud)	
AntiKeylogger package	HEUR/APC (Cloud)	
BreakQuest package	TR/Agent.21170214	
BricksOfEgypt package	TR/Agent.155648.405	
Bulents package	HEUR/APC (Cloud)	
ClientSlave package	TR/Dropper.Gen	
Ctrl package	HEUR/APC (Cloud)	
Dir2Text package	HEUR/APC (Cloud)	
DVDplay package	HEUR/APC (Cloud)	
EasyLog package	HEUR/APC (Cloud)	
FireWire package	HEUR/APC (Cloud)	
Fujitsu package	HEUR/APC (Cloud)	
GameAccelerator package	HEUR/APC (Cloud)	
GiBlock package	HEUR/APC (Cloud)	
Grammiweb package	HEUR/APC (Cloud)	
HeroesOfHellas package	HEUR/APC (Cloud)	

HighwayNights package	HEUR/APC (Cloud)	
HP package	HEUR/APC (Cloud)	
ImperialGlory package	TR/Dropper.A.33996	
Iuspawn package	HEUR/APC (Cloud)	
Kreed package	HEUR/APC (Cloud)	
Macromedia package	HEUR/APC (Cloud)	
MaxPasswords package	TR/Agent.320000.34	
MultiSpeak package	HEUR/APC (Cloud)	
NTR package	HEUR/APC (Cloud)	
OneClickStarter package	HEUR/APC (Cloud)	
Prey package	HEUR/APC (Cloud)	
PWL package	HEUR/APC (Cloud)	
Recompress package	HEUR/APC (Cloud)	
RegistryFirstAid package	HEUR/APC (Cloud)	
Renamer package	HEUR/APC (Cloud)	
SlipStreamer package	HEUR/APC (Cloud)	
Sony package	HEUR/APC (Cloud)	
Sound2Vision package	HEUR/APC (Cloud)	
StarCraft package	HEUR/APC (Cloud)	
Titlebar package	HEUR/APC (Cloud)	
VirtualBox package	HEUR/APC (Cloud)	
WildTangent package	TR/Agent.48685.1 (Cloud)	
WinPatrol package	HEUR/APC (Cloud)	
WinRAR package	HEUR/APC (Cloud)	
WOB package	HEUR/APC (Cloud)	
XPwinExit package	HEUR/APC.Griffin (Cloud)	

AVIRA had 44 false alarms.

Vipre

False alarm found in some parts of	Detected as	Supposed prevalence
ABCadressen package	Trojan.Win32.Zbot.pj (v)	
ActiveSoftware package	Trojan.Win32.Generic!BT	
AmericanConquest package	Trojan.Win32.Generic!BT	
Archicrypt package	BehavesLike.Win32.Malware.klt (mx-v)	
Avira package	Trojan.Win32.Generic!BT	
Backspin package	Trojan.Win32.Generic!BT	
BigFoot package	LooksLike.Win32.InfectedFile!B (v)	
Boxoft package	Trojan.Win32.Generic!BT	
BuddyIcons package	Trojan.Win32.Generic!BT	
CoolButton package	Trojan.Win32.Generic!BT	
Cryppie package	Trojan.Win32.Generic!BT	
DeDupler package	Trojan.Win32.Generic!BT	
DemoMaker package	Trojan.Win32.Generic!BT	
DesktopBackground package	Trojan.Win32.Generic!SB.0	
DialRight package	Trojan.Win32.Generic.pak!cobra	
DriverPacks package	Trojan.Win32.Generic!BT	
EasyDivx package	Trojan.Win32.Generic!BT	
eKonnekt package	Trojan.Win32.Generic!SB.0	
ESET package	Trojan.Win32.Generic!BT	

EuroPlus package	BehavesLike.Win32.Malware.wsc (mx-v)	
FontTwister package	Trojan.Win32.Generic.pak!cobra	
GhostRider package	Trojan.Win32.Generic!SB.0	
Gimp package	Trojan.Win32.Generic!BT	
IcyTower package	Trojan.Win32.Generic!BT	
InternetMeter package	Trojan.Win32.Generic!BT	
iScsiCake package	Trojan.Win32.Generic!BT	
KrutiDev package	Trojan.Win32.Generic!BT	
LinkValidator package	Trojan.Win32.Generic!BT	
ListSP package	Trojan.Win32.Generic!BT	
Mailru package	Trojan.Win32.Generic!SB.0	
MSI package	Trojan.Win32.Buzus	
NewFolderExplorer package	Trojan.Win32.Generic!BT	
NXPlite package	Trojan.Win32.Generic!BT	
Open package	Trojan.Win32.Generic!BT	
PEbuilder package	Trojan.Win32.Generic!BT	
Photoshop package	Trojan.Win32.Generic!BT	
QuickTime package	Trojan.Win32.Generic!BT	
RegistryCleanExpert package	Trojan.Win32.Generic!BT	
SB package	Trojan.Win32.Generic!SB.0	
SecureIt package	Trojan.Win32.Generic!BT	
StarCraft package	Trojan.Win32.Generic!BT	
StartTime package	Trojan.Win32.Generic!BT	
Tetrix package	Trojan.Win32.Generic!BT	
TweakLite package	Trojan.Win32.Generic!BT	
UFOattack package	Trojan.Win32.Generic!BT	
Unet package	Trojan.Win32.Generic!BT	
Ustri package	Back Orifice (B02K)	
WinAmpPlugins package	Trojan-Downloader.Win32.Agent	
WWFdesktop package	Trojan.Win32.Generic!BT	
XPI package	Trojan.Win32.Generic!BT	

Vipre had 50 false alarms.

Avast

False alarm found in some parts of	Detected as	Supposed prevalence
AbsoluteBlue package	Win32:Malware-gen	
Acer package	Win32:GenMalicious-GJQ [Trj]	
ActiveState package	Win32:Evo-gen [Susp]	
Aedix package	Win32:Evo-gen	
Antiwins package	Win32:Evo-gen [Susp]	
ATI package	Win32:Malware-gen	
Backoffice package	Win32:Evo-gen [Susp]	
BananaPC package	Win32:Malware-gen	
Baukosten package	Win32:Evo-gen [Susp]	
BigKahunaReef package	Win32:Malware-gen	
BricksOfEgypt package	Win32:Malware-gen	
ComTest package	Win32:Evo-gen [Susp]	
ContactGrabber package	Win32:Evo-gen [Susp]	
DigitalMedia package	Win32:Dropper-gen [Drp]	

DriveManager package	Win32:Malware-gen	
DropUpload package	Win32:Evo-gen [Susp]	
DVDVideosoft package	Win32:Malware-gen	
EasyDriver package	Win32:Malware-gen	
Epson package	Win32:Malware-gen	
F-Secure package	Win32:Evo-gen [Susp]	
FastStone package	Win32:Trojan-gen	
FileSplitter package	Win32:Evo-gen [Susp]	
FileZilla package	Win32:Dropper-gen [Drp]	
Forte package	Win32:Malware-gen	
FotoKasten package	Win32:Malware-gen	
FriendFactory package	Win32:Evo-gen [Susp]	
FunctionGrapher package	Win32:Evo-gen [Susp]	
Guenstig package	Win32:Evo-gen [Susp]	
GXTranscoder package	Win32:Malware-gen	
HDCleaner package	Win32:Malware-gen	
Hexen package	Win32:Malware-gen	
HotKey package	Win32:Malware-gen	
HP package	Win32:Malware-gen	
Inkscape package	Win32:Evo-gen [Susp]	
iPower package	Win32:Evo-gen [Susp]	
Joshua package	Win32:Malware-gen	
JoWood package	Win32:Trojan-gen	
KeePass package	Win32:Dropper-gen [Drp]	
Lidl package	Win32:Malware-gen	
LiteOn package	Win32:Evo-gen [Susp]	
Lotus package	Win32:Malware-gen	
Mausii package	Win32:Evo-gen [Susp]	
MaximumCopy package	Win32:Evo-gen [Susp]	
MaxPasswords package	Win32:Malware-gen	
MediaConverter package	Win32:Malware-gen	
MediaGallery package	Win32:Malware-gen	
MediaMaker package	Win32:Evo-gen [Susp]	
MegaCubo package	Win32:Malware-gen	
MiniSudoku package	Win32:Evo-gen [Susp]	
MoreTunes package	Win32:Malware-gen	
Mozilla package	Win32:Evo-gen [Susp]	
NPE package	Win32:Malware-gen	
OpenOffice package	Win32:Evo-gen [Susp]	
Pauker package	Win32:Malware-gen	
Pnotes package	Win32:Malware-gen	
ProcX package	Win32:Malware-gen	
PsiPhon package	Win32:Malware-gen	
RelaxIt package	Win32:Malware-gen	
RemoteKeys package	Win32:Evo-gen [Susp]	
Reorganize package	Win32:Evo-gen [Susp]	
Settler package	Win32:Malware-gen	
Shanghai package	Win32:Agent-AVJC [Trj]	
Simplyzip package	Win32:Malware-gen	
SpamControl package	Win32:Evo-gen [Susp]	





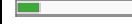







StarBrite package	Win32:WrongInf-D [Susp]	
Symantec package	Win32:GenMaliciousA-ACZ [Trj]	
SystemSecurity package	Win32:Evo-gen [Susp]	
Translator package	Win32:Evo-gen [Susp]	
Tria package	Win32:Malware-gen	
TVnoise package	Win32:Malware-gen	
VistaTweaker package	AutoIt:Agent-AHT [Trj]	
VisualGSM package	Win32:GenMalicious-HYA [Trj]	
Warner package	Win32:Malware-gen	
WinAmp package	Win32:Rootkit-gen [Rtk]	
WinPulse package	Win32:Evo-gen [Susp]	
WxMusic package	Win32:Malware-gen	
zVolumne package	Win32:Malware-gen	

Avast had 77 false alarms.

Baidu

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Trojan.Win32.Downloader.asVj	
AscGen package	Backdoor.Win32.Bifrose.al	
Avanquest package	Worm.Win32.Viking.pf	
Avira package	Trojan.Win32.Lmir.gen	
Babylon package	Worm.Win32.Runouce.aOu	
Backoffice package	Trojan.Win32.Virtumonde.ASkO	
BackupManager package	Trojan.Win32.Patched.AGNh	
Bananarama package	Trojan.Win32.Agent.cku	
Barracuda package	Backdoor.IRC.Flood.mk	
BartePE package	Trojan.Win32.Agent.aIfH	
Blowfish package	Trojan.Win32.Zlob.jbp	
BoostSpeed package	Trojan.Win32.Agent.gen	
BricksOfEgypt package	TR/Agent.155648.405	
BriskAlbum package	Trojan.Win32.StartPage.puj	
Broker package	Trojan.Win32.Flg.gen	
Casino package	Trojan.Win32.Generic.aR	
Casio package	Worm.Win32.Neeris.gen	
Citrix package	Trojan.Win32.FakeAV.am	
ClamWin package	Worm.Win32.Runouce.ac	
Clickster package	Trojan.Win32.Delf.gen	
ClientSlave package	TR/Dropper.Gen	
CloneyXXL package	Trojan.Win32.GhostKeyLogger.Amd	
CNOserver package	Trojan.Win32.Generic.aJa	
CopyToFloppy package	Backdoor.Win32.Final.ao	
Cywin package	Backdoor.Win32.Iroffer.aZ	
Dnet package	Trojan.Win32.Agent.aIfH	
DreiKampf package	Trojan.Win32.PossibleMalware.ca	
DungeonSiege package	Trojan.Win32.Zlob.gen	
eMerge package	Backdoor.Win32.Final.ao	
Eumex package	Trojan.Win32.Agent.Aep	
F-Secure package	Trojan.Win32.Agent.ADF	
FlashJester package	Trojan.Win32.Pincav.AV	

FlightSimulator package	Trojan.Win32.Zlob.gen	
Galton package	Trojan.Win32.Flg.gen	
GDATA package	Worm.Win32.AutoIt.akZ	
GIMP package	Trojan.Win32.Kryptik.bKGY	
GoodMem package	Trojan.Win32.InfoStealer.AF	
Googles package	Trojan.Win32.Ponmocup.a	
HDCopy package	Trojan.Win32.Banload.ha	
HotPlug package	Trojan.Win32.Undef.cll	
IcyTower package	Trojan.Win32.Kryptik.BVVE	
Idman package	Trojan.Win32.InfoStealer.aEAd	
IfoEdit package	Trojan.Win32.GhostKeyLogger.Amd	
ImperialGlory package	TR/Dropper.A.33996	
InterAct package	Trojan.Win32.Ursnif.a	
iPhone package	Hacktool.Win32.PsKill.AaR	
ISDM package	Virus.Win32.Alman.72	
iTimeSync package	Trojan.Win32.Kryptik.m	
IyName package	Trojan.Win32.Pincav.AeQ	
Java package	Backdoor.Win32.Final.ao	
Kleptomania package	Trojan.Win32.Small.Ax0	
Krlite package	Trojan.Win32.Bumat.CGen	
Linksys package	Virus.Win32.Nimnul.gen	
Logik package	Backdoor.Win32.Final.ao	
MachPE package	Backdoor.Win32.Iroffer.aZ	
McAfee package	Worm.Win32.LovGate.Aq	
Menue package	Trojan.Win32.Pincav.AV	
Min2Tray package	Trojan.Win32.Agent.APp	
Miranda package	Trojan.Win32.Kryptik.VW	
Monkey package	Trojan.Win32.Generik.MQZWPMV	
MSI package	Trojan.Win32.Inject.aIxs	
MSWindows2000 package	Backdoor.Win32.Netbus.AA	
MSWorks package	Trojan.Win32.Generic.aqK	
NETLan package	Trojan.Win32.Agent.am	
NovaPDF package	Trojan.Win32.Bumat.gen	
PanoramaStudio package	Worm.Win32.FakeFolder.gen	
Photoshop package	Trojan.Win32.Trabin.aGB	
PlainPaste package	Worm.Win32.Agent.Aw	
PowerArc package	Trojan.Win32.Kryptik.BAGN	
Printy package	Trojan.Win32.EmailFlooder.AM	
Regens package	Trojan.Win32.Ursnif.a	
RegistryCleanExpert package	Trojan.Win32.Drob.AgI	
SageTV package	Trojan.Win32.VBKrypt.AKsi	
Sandboxie package	Trojan.Win32.Agent.40	
SBook package	Trojan.HTML.Clicker.AIrT	
SealOfEvil package	Worm.Win32.Runouce.ay	
Silicon package	Trojan.Win32.Agent.AKn	
Skype package	Trojan.Win32.Kryptik.m	
Splinter package	Trojan.Win32.Flg.gen	
Spryjinx package	Trojan.Win32.Flg.gen	
StartupBooster package	Trojan.Win32.Tibs.gen	
Texter package	Trojan.Win32.Antavmu.aWad	

TheDebugger package	Backdoor.Win32.Final.ao	
Tiscali package	Trojan.Win32.Orsam.gen	
TrafficMonitor package	Trojan.Win32.Kryptik.m	
Trust package	Trojan.Win32.Agent.aD	
VirtualLibraries package	Trojan.Win32.Mafod.CGen	
WinAce package	Trojan.Win32.Sasfis.AMM	
WinRar package	Trojan.MSIL.Agent.AbW	
WinRun package	Trojan.Win32.Flg.gen	
XPwinExit package	Trojan.Win32.Injector.BTTD	
XPY package	Trojan.Win32.Downloader.AOB	
ZDbackup package	Trojan.Win32.VBKrypt.APa	
Zzzap package	Trojan.Win32.Flood.n	

Baidu had 94 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 (April 2015)