Details about Discovered False Alarms

Appendix to the Anti-Virus Comparative No. 23 August 2009

Language: English
August 2009
Last Revision: 2009-09-19

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. 100 FP's and another only 50, it is likely that the first product is more prone to FP's than the other. It doesn't mean the product with 50 FP's doesn't have more than 50 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 questionable applications and tools, as well as FP's distributed by vendors or other non independent sources are not counted here as False Positives.

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.

BitDefender

False alarm found in some parts of	Detected as
HotCorners package	Trojan.Generic.1232219
Notepad2 package	Trojan.Generic.2191426
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve
Z-Cron package	Trojan.Generic.1760814

Bitdefender had 4 false alarms.

eScan

False alarm found in some parts of	Detected as
HotCorners package	Trojan.Generic.1232219
Notepad2 package	Trojan.Generic.2191426
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve
Z-Cron package	Trojan.Generic.1760814

eScan had 4 false alarms.

F-Secure

False alarm found in some parts of	Detected as
HotCorners package	Trojan.Generic.1232219
Notepad2 package	Trojan.Generic.2191426
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve
Z-Cron package	Trojan.Generic.1760814

F-Secure with default settings had 4 false alarms.

Microsoft

False alarm found in some parts of	Detected as
Copernic package	Backdoor:Win32/Harvester.J
MultiSpeak package	TrojanDropper:Win32/SE
PCWizard package	TrojanDownloader:Win32/Agentsmall.H
RunAs package	Trojan:Win32/Killfiles.AG
XPoptimal package	Trojan:Win32/FakeCog

Microsoft OneCare had 5 false alarms.

Avast

False alarm found in some parts of	Detected as
FreeFile package	Win32:Trojan-gen {Other}
QuickID package	Win32:Trojan-gen {Other}
RAMSaverPro package	Win32:Trojan-gen {Other}
SystemSafetyMonitor package	Win32:Trojan-gen {Other}
WeaponQuickSwap package	Win32:Trojan-gen {Other}

Avast had 5 false alarms.

AVG

False alarm found in some parts of	Detected as
Burnintest package	BackDoor.Agent.HH
EasyBurning package	Generic10.AENO
HotCorners package	Dropper.Generic.AOSI
NokiaUnlocker package	Generic13.ACMS
Notepad2 package	Logger.HJF
Spysweeper package	BackDoor.Delf.BVF
VistaBootPro package	Win32/Heur
WISOGeld package	SHeur2.UNK

AVG had 8 false alarms.

Kaspersky

False alarm found in some parts of	Detected as
Browster package	Trojan.Win32.Generic
EasyBurning package	SuspiciousPacker.Multi.Generic
NoURL package	Trojan.Win32.StartPage
PDF555 package	Worm.Win32.Generic
PowerStrip package	Backdoor.Win32.Hupigon.dijh
QDir package	Trojan.Win32.Krament.fn
Quuuiz package	Trojan-Banker.Win32.Banker.afwk
RocketLife package	Trojan-Downloader.Win32.Generic

Kaspersky had 8 false alarms.

G DATA

False alarm found in some parts of	Detected as
FreeFile package	Win32:Trojan-gen {Other}
HotCorners package	Trojan.Generic.1232219
Notepad2 package	Trojan.Generic.2191426
QuickID package	Win32:Trojan-gen {Other}
RAMSaverPro package	Win32:Trojan-gen {Other}
SystemSafetyMonitor package	Win32:Trojan-gen {Other}
TorChat package	Gen:Trojan.Heur.km5@@hk@5Ve
WeaponQuickSwap package	Win32:Trojan-gen {Other}
Z-Cron package	Trojan.Generic.1760814

G DATA had 9 false alarms.

ESET

False alarm found in some parts of	Detected as
Blinkx package	Win32/Genetik
ClockX package	Win32/TrojanDownloader.Esepor
GDSChild package	NewHeur_PE
Gnumeric package	Win32/Oficla.D
iZArc package	Win32/Statik
MWConn package	Win32/Genetik
RestoreIt package	Win32/Genetik
Taskman package	Win32/Spy.Agent
TransMac package	Win32/Agobot
TickerMyMail package	NewHeur_PE
WinPT package	Win32/Genetik
Zoot package	NewHeur_PE

ESET NOD32 had 12 false alarms.

Symantec

False alarm found in some parts of	Detected as
0190warner package	Suspicious.MH690.A
AutoStartAdmin package	Suspicious.MH690.A
Blinkx package	Suspicious.MH690.A
CableMon package	Suspicious.MH690.A
CPUControl package	Downloader
FolderDrive package	Suspicious.MH690.A
HotCorners package	W32.Swich
Iron package	Suspicious.MH690.A
PDFtk package	Suspicious.MH690.A
PopUpBlocker package	Suspicious.MH690.A
SliceAndSave package	Suspicious.MH690.A
TaskMan package	Infostealer.Gampass
UpdateOMatic package	W32.SillyFDC

Symantec Norton Anti-Virus had 13 false alarms.

AVIRA

False alarm found in some parts of	Detected as
AcousticalMP3 package	TR/Downloader.Gen
Amole package	HEUR/Malware
Binary package	TR/Banker.172032.D
CBInk package	HEUR/Crypted
Docserver package	TR/ATRAPS.Gen
EasyBurning package	TR/Spy.345520
EmailArchitect package	HEUR/Malware
Ewido package	TR/Agent.53312
LogAnalysa package	DR/Delphi.Gen
LoginCtrl package	HEUR/Malware
Outlookers package	HEUR/Malware
PerlGnom package	HEUR/HTML.Malware
PreisHai package	TR/Dropper.Gen
ShowShifter package	HEUR/Malware
SpamAware package	TR/Dldr.Delf.idv
SpiceWorks package	HEUR/HTML.Malware
TrojanRemover package	HEUR/Malware
Unyte package	TR/Spy.Gen
VistaBootPro package	PCK/YodaProt
WhatSpeed package	TR/Dropper.Gen
WinPcap package	W32/Tiraz.A

AVIRA had 21 false alarms.

Sophos

False alarm found in some parts of	Detected as
3DScreensaver package	Mal/Generic-A
AcousticalMP3 package	Mal/Generic-A
AdNuke package	Mal/Generic-A
AntiSpamware package	Mal/Behav-034
Anti-Trojan package	Mal/VB-A
Auralog package	Mal/Generic-A
AutoHotKey package	Mal/Generic-A
BMKBuddy package	Mal/Generic-A
CDDVDBurner package	Mal/Generic-A
CL08 package	Mal/Generic-A
CPUControl package	Mal/Generic-A
EasyBurning package	Mal/Generic-A
Ewido package	Mal/Generic-A
GPSPhoto package	Mal/Generic-A
HTMLTranslator package	Mal/HckPk-A
MultiInstall package	Mal/Generic-A
PCWizard package	Mal/Emogen-AA
RAIDE package	Mal/Generic-A
RegCool package	Mal/Generic-A
Skype package	Mal/Packer
SpamAware package	Mal/Generic-A

SpamBully package	Mal/Behav-058
SuperGee package	Mal/Behav-150
TransMac package	Mal/Generic-A
VideoExpress package	Mal/Generic-A
VirusExterminator package	Mal/Behav-053

Sophos had 26 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 very big issue. These files are technically FP’s, but the administrators most likely would like to know about the presence of those applications.

McAfee

False alarm found in some parts of	Detected as
ADO package	W32/Generic.worm!im
AmoKDVDShrinker package	Generic.dx
AutoFeedback package	Artemis!CA53549034FA
BenchEmAll package	W32/Mental
Bestprice package	New Malware.hi
Browster package	Artemis!1D920941DDEC
CopyPod package	Artemis!13AB048544B9
CPUControl package	Artemis!97D34621172D
DPwiper package	Suspect-26!F6918B4678C3
DupFinder package	Artemis!B5B43C0CF59C
EasyBurn package	Generic.dx
EQSecure package	Suspect-02!7CF55681A34E
FBReader package	Artemis!A4EC189CEC9A
FileZilla package	Artemis!A6320A09363B
FreshDow package	New Malware.hi
FZ package	Artemis!C8485B24B775
GetIt package	w32/autorun.worm.ac
HotCorners package	Generic.dx
MyUSB package	New Malware.hi
NetMeter package	Artemis!D46B8D7F38A6
PaperOffice package	W32/Generic.worm!im
PSPVideoExpress package	Artemis!1E207D0A2C1D
RealTimeBrowser package	Artemis!4AA7FF6C7662
RegistrySystemWizards package	Artemis!0BAF3AC9FC5B
RightFTP package	New Malware.hi
RoboFormConverter package	New Malware.bx
Sateirac package	New Malware.hi
SimplyZip package	Generic.dx!bj
SpamAware package	Downloader.gen.a
SpywareRemoval package	Generic PWS.bw
SSC package	W32/Spybot.worm.gen
StickSecurity package	Artemis!5E2E76FF44D6
SysReport package	Suspect-02!8A22063660D5
TaskMan package	PWS-LDPinch
TransMac package	Generic BackDoor
UBCD package	Generic.dx
VideoSplitter package	New Malware.hi

VuPlayer package	Suspect-02!F97A36AC959C
WinAmp package	Artemis!1D20BA239375
WSA package	Artemis!5E804BE94D94
YAW package	Generic Delphi

McAfee with in-the-cloud had 41 false alarms. McAfee without in-the-cloud had 26 false alarms.

TrustPort

False alarm found in some parts of	**Detected as**
ACS package	W32/Hupigon.BQJM
AmericanConquest package	Sohanad.BCW
AmoKDVDShrink package	W32/Packed_Upack.A
Burnintest package	BackDoor.Agent.HH
CDDVDBurning package	W32/Packed_NsPack.I
CFOSSpeed package	W32/PCClient.GCB
CometBrowser package	W32/Delf.AXSP
CPUz package	W32/Malware.GKXE
CreateMovie package	W32/Smalldoor.EQXJ
CyberGhost package	W32/DLoader.OQAA
EasyBurning package	W32/Packed_Upack.A
FolderDrive package	W32/Obfuscated.H3!genr
HotCorners package	Dropper.Generic.AOSI
Kazaa package	W32/Packed_PeX.B
Miranda package	W32/Packed_Upack.H
NetNak package	W32/Crypto.AC
NokiaFree package	Suspicious_F.gen
NoMansLand package	Smalltroj.NBRB
Notepad2 package	Logger.HJF
OpenFiles package	W32/Obfuscated.H11!genr
Outpost package	W32/Smalltroj.EHLA
PowerBullet package	Malware.EVNW
Recolored package	Malware.BHVX
RegCool package	Bifrose.ASTP
RocketLife package	W32/Downloader
RouterSyslog package	W32/Packed_Upack.A
Skype package	W32/Packed_PeX.B
SmartProtectorPro package	W32/Malware.DEKW
SpamAware package	W32/Delf.CEJI
SpamKiller package	W32/Smalltroj.CQYR
SpySweeper package	W32/Delf.BSKH
SSC package	W32/Spybot.AHCY
TransMac package	W32/Madtol.AJ
TurboLister package	W32/Smalltroj.IFPQ
UMRS package	W32/Smalltroj.CFVR
UnBrowster package	W32/Malware
VideoExpress package	W32/Malware.CNJD
WinPcap package	Malware.CZKB
WiNRAR package	DLoader.RZQX
WinTK package	W32/Malware
WISOGeld package	SHeur2.UNK

XPTweaker package	W32/DLoader.CQBK

TrustPort had 42 false alarms.

Norman

False alarm found in some parts of	**Detected as**
ACS package	W32/Hupigon.BQJM
AmericanConquest package	Sohanad.BCW
AmoKDVDShrink package	W32/Packed_Upack.A
CDDVDBurning package	W32/Packed_NsPack.I
CFOSSpeed package	W32/PCClient.GCB
CGWeb package	W32/DLoader.OQAA
CometBrowser package	W32/Delf.AXSP
CPUz package	W32/Malware.GKXE
CreateMovie package	W32/Smalldoor.EQXJ
CyberGhost package	W32/DLoader.OQAA
DVDBurner package	W32/Malware.CNJD
EasyBurning package	W32/Packed_Upack.A
FolderDrive package	W32/Obfuscated.H3!genr
Kazaa package	W32/Packed_PeX.B
Miranda package	W32/Packed_Upack.H
NetNak package	W32/Crypto.AC
NokiaFree package	Suspicious_F.gen
NoMansLand package	Smalltroj.NBRB
OpenFiles package	W32/Obfuscated.H11!genr
Outpost package	W32/Smalltroj.EHLA
PDFtk package	W32/Packed_Upack.A
PowerBullet package	Malware.EVNW
Recolored package	Malware.BHVX
RegCool package	Bifrose.ASTP
RocketLife package	W32/Downloader
RouterSyslog package	W32/Packed_Upack.A
Skype package	W32/Packed_PeX.B
SmartProtectorPro package	W32/Malware.DEKW
SpamAware package	W32/Delf.CEJI
SpamKiller package	W32/Smalltroj.CQYR
SpySweeper package	W32/Delf.BSKH
SSC package	W32/Spybot.AHCY
Towav package	W32/Obfuscated.G!genr
TransMac package	W32/Madtol.AJ
TurboLister package	W32/Smalltroj.IFPQ
UMRS package	W32/Smalltroj.CFVR
UnBrowster package	W32/Malware
VideoExpress package	W32/Malware.CNJD
WinPcap package	Malware.CZKB
WiNRAR package	DLoader.RZQX
WinTK package	W32/Malware
XPTweaker package	W32/DLoader.CQBK

Norman had 42 false alarms.

Kingsoft

False alarm found in some parts of	Detected as
AddZip package	Win32.Troj.Genome.196608
AIM package	Win32.Troj.Taris.135168
ALZZip package	Win32.Hack.PsKill.a.81920
AmoKDVDShrinker package	Win32.Troj.Undef.2498560
AutoHotKey package	Win32.Binder.ac.429653
CFOSSpeed package	Win32.Hack.PcClient.1003520
CoreMediaPlayer package	Win32.TrojDownloader.List.uf.18432
CPUControl package	Win32.TrojDownloader.Small.ei.1086464
DiagramDesigner package	Win32.TrojDownloader.Unknown.zj.97280
EveOfDestruction package	Win32.Troj.Unknown.az.196608
ExPat package	Win32.Troj.VB.22016
FlyingPicture package	Win32.Troj.Agent.za.65261
Gawk package	Win32.Troj.Neshta.284672
GIMP package	Win32.Troj.HexzoneT.xe.221184
ImageAnalyzer package	Win32.TrojDownloader.Unknown.zj.97280
Lektora package	Worm.Skybag.c.974848
MP3Test package	Win32.TrojDownloader.Zlob.2084864
MS Windows 2000 package	Win32.Troj.Aegi.61712
MS Windows 2000 SP2 package	Win32.Troj.IRCBot.54d4.1118208
MS Windows 2000 SP3 package	Win32.Troj.Aegi.186640
MS Windows 2000 SP4 package	Win32.Troj.Aegi.16656
Ms WMDiagnostic package	Heur.Win32.generic.01.h
Nascar package	Win32.Troj.Unknown.az.196608
Nero package	Win32.Troj.Delf.542208
Outpost package	Win32.Troj.Delf.344133
Patchscanner package	Win32.Troj.Genome.516096
Perl package	Win32.Troj.Neshta.117760
Picasa package	Win32.Troj.Agent.4362240
PopimsAnimator package	Win32.Troj.Unknown.zj.97280
Putty package	Worm.Nohoper.a.225280
RAIDE package	Win32.PSWTroj.YBOnline.o.61440
Regmon package	Worm.Beagle.192512
RegSnap package	Win32.Troj.Genome.20992
RoboHelp package	Win32.Troj.Undef.24576
SecurePoint package	Win32.Hack.Ferat.54356
SpamAware package	Win32.TrojDownloader.Delf.126976
SUDG package	Win32.Troj.Agent.b1dae.24516
TaskMan package	Win32.PSWTroj.LdPinch.552960
TransMac package	Win32.Hack.Agobot.376832
Trillian package	Win32.Troj.Agent.za.32768
Uptime package	Win32.TrojDownloader.Small.oj.16384
USBaccess package	Win32.Troj.Spenir.88064
Virtuoza package	Win32.Hack.Delf.dn.884736
VistaExit package	Win32.Troj.mouseoutT.xd.49152
WinAmp package	Win32.Troj.Sality.846848
WinCommander package	Win32.Troj.Taris.84992
WinRAR package	Worm.Ganda.41040.40503

Kingsoft had 47 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 2009)