

Details of False Alarms



Appendix to the Anti-Virus Comparative March 2018

Language: English

March 2018

Last Revision: 12th April 2018


www.av-comparatives.org

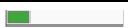




Details of false alarms

In 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 to produce false alarms (false positives). No product is immune from false positives (FPs), but some produce more than others. False Positives Tests measure which programs do best in this respect, i.e. distinguish clean files from malicious files, despite their context. 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, when using 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 FPs 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 application, it is counted here as only one false alarm. Cracks, keygens, 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 user 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 the lowest prevalence level (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 a hundred users	Individual cases, old or rarely used files, very low 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 number of false alarms (currently 10) inside our clean set before we start penalizing scores, and in our opinion products which produce a higher number of false alarms are also more likely to produce false alarms with more prevalent files (or in other sets of clean files). The prevalence data we give for 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.

There may be a variation in the number of false positives produced by two different programs that use the same engine (principal detection component). For example, Vendor A may license its detection engine to Vendor B, but Vendor A's product may have more or fewer false positives than Vendor B's product. This can be due to factors such as different internal settings being implemented, differences in other components and services such as additional or differing secondary engines/signatures/whitelist databases/cloud services/quality assurance, and possible time delay between the release of the original signatures and the availability of the signatures for third-party products.

False Positives (FPs) are an important measurement for AV quality. Furthermore, the test is useful and needed to avoid that vendors optimize products to score good in tests by looking at the context – this is why false alarms are being mixed and tested the same way as tests with malware are done. 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 older 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 potentially cause an FP again on a more significant file. Thus, they still deserve mention and still deserve to be penalised.


Below you will find some info about the false alarms we observed in our independent set of clean files. Red entries highlight false alarms on files that were digitally signed.

AVIRA

False alarm found in some parts of	Detected as	Supposed prevalence
NetClientManager package	TR/Kryptik.ewexv	


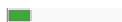
AVIRA had 1 false alarm.

ESET

False alarm found in some parts of	Detected as	Supposed prevalence
NetClientManager package	MSIL/Kryptik.LHT	



ESET had 1 false alarm.

Bitdefender

False alarm found in some parts of	Detected as	Supposed prevalence
CorelVentura package	Gen:Variant.Barys.57935	
NetClientManager package	Trojan.GenericKD.40105859	

Bitdefender had 2 false alarms.

BullGuard

False alarm found in some parts of	Detected as	Supposed prevalence
CorelVentura package	Gen:Variant.Barys.57935	
DigitalTheatre package	Gen:Variant.Symmi.70545	

NetClientManager package	Trojan.GenericKD.40105859	
PESetEnv package	Gen:Trojan.Heur.JP.am0@aead5lo	
Redstreak package	Gen:Variant.Ursu.115789	

BullGuard had 5 false alarms.

VIPRE

False alarm found in some parts of	Detected as	Supposed prevalence
CorelVentura package	Gen:Variant.Barys.57935	
DigitalTheatre package	Gen:Variant.Symmi.70545	
NetClientManager package	Trojan.GenericKD.40105859	
PESetEnv package	Gen:Trojan.Heur.JP.am0@aead5lo	
RedStreak package	Gen:Variant.Ursu.115789	

VIPRE had 5 false alarms.

Emsisoft

False alarm found in some parts of	Detected as	Supposed prevalence
CorelVentura package	Gen:Variant.Barys.57935	
DigitalTheatre package	Gen:Variant.Symmi.70545	
LotRIcon package	Trojan.Agent	
NetClientManager package	Trojan.GenericKD.40105859	
OrangeGem package	Trojan.Sinowal.Gen.1	
PESetEnv package	Gen:Trojan.Heur.JP.am0@aead5lo	
RedStreak package	Gen:Variant.Ursu.115789	

Emsisoft had 7 false alarms.







Quick Heal

False alarm found in some parts of	Detected as	Supposed prevalence
CDDCDBurner package	Trojan.Generic	
CorelVentura package	EE:Malwr.Heur.Barys.57935	
DigitalTheatre package	EE:Malwr.Heur.Symmi.70545	
jNetTool package	Trojan.UGeneric	
NetClientManager package	EE:Malware.GenericKD.40105859	
PESetEnv package	EE:Malwr.Heur.JP.am0	
Webshop package	EE:Malwr.Heur.Ursu.111593	
WT package	Trojan.IGENERIC	

Quick Heal had 8 false alarms.





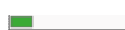


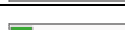

Avast

False alarm found in some parts of	Detected as	Supposed prevalence
AutoHotKey package	Win32:Malware-gen	
BMKBuddy package	Win32:Malware-gen	
Deskline package	Win32:Malware-gen	

LapTimer package	FileRepMalware	
NetClientManager package	Win32:Malware-gen	
Photomatix package	Win32:Kraton-A [Trj]	
PowerArc package	FileRepMetagen	
TakeABreak package	Win32:Malware-gen	
UPXshell package	FileRepMalware	







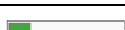


Avast had 9 false alarms.

AVG

False alarm found in some parts of	Detected as	Supposed prevalence
AutoHotKey package	Win32:Malware-gen	
BMKBuddy package	Win32:Malware-gen	
Deskline package	Win32:Malware-gen	
LapTimer package	FileRepMetagen	
NetClientManager package	Win32:Malware-gen	
Photomatix package	Win32:Kraton-A	
PowerArc package	FileRepMetagen	
TakeABreak package	Win32:Malware-gen	
UPXshell package	FileRepMalware	







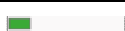
AVG had 9 false alarms.




Kaspersky Lab

False alarm found in some parts of	Detected as	Supposed prevalence
ARCpeek package	Packed.Win32.Dico.gen	
Finalhit package	Trojan.Win32.Scar.qoqc	
FreeOCR package	UDS:Trojan.Win32.Schoolboy.bdb	
Nullable package	HEUR:Trojan.Win32.Generic	
ScreenTime package	Trojan.Win32.Scar.qohc	
Steganos package	Trojan-Spy.Win32.Keylogger.bfco	
WinShake package	Trojan.Win32.Agent.newzhl	
WinTBS package	UDS:Trojan.Win32.Generic	
Wisdom package	Trojan.Win32.Scar.qoqx	

Kaspersky Lab had 9 false alarms.











F-Secure

False alarm found in some parts of	Detected as	Supposed prevalence
CorelVentura package	Gen:Variant.Barys.57935	
Defcon package	Trojan:W32/Generic.0d91a53930!Online	
DigitalTheatre package	Gen:Variant.Symmi.70545	
NetClientManager package	Trojan.GenericKD.40105859	
Path2Copy package	Trojan:W32/Generic.06b6bb60fd!Online	
PESetEnv package	Gen:Trojan.Heur.JP.am0@aead5lo	
RedStreak package	Gen:Variant.Ursu.115789	

TheMovies package	Trojan:W32/Generic.8029382fde!Online	
USBsuite package	Trojan:W32/Generic.aeffce8a92!Online	
WinRepair package	Trojan:W32/Generic.e410232d50!Online	

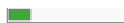




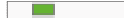








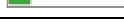



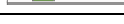


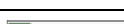
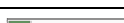

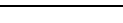
F-Secure had 10 false alarms.

McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
AtomTech package	JTI/Suspect.131076!d3db2c159a34	
DrDivx package	JTI/Suspect.131076!d9daf3110473	
NetXfer package	GenericRXDX-WB!B0ACE52CD4F9	
PassPack package	GenericRXCD-LK!383B25C93DC4	
Pause package	JTI/Suspect.131076!14bbca68f85c	
Reime package	Suspect!bb67f76f9434	
Screensaver package	JTI/Suspect.196665!d5e67dcf17bc	
Synopsis package	Suspect!24239384a75e	
YTdownload package	Suspect!10246cbd0ef1	
ZyloM package	GenericRXCA-JD!0AF7674D33F0	

McAfee had 10 false alarms.

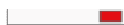




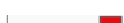


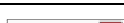

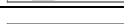
















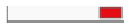




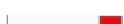
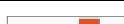






Microsoft

False alarm found in some parts of	Detected as	Supposed prevalence
Abolimba package	Blocked	
Adobe package	Blocked	
Baywatch package	Blocked	
Butterflies package	Blocked	
Caillou package	Blocked	
CompuTec package	Blocked	
Core2Max package	Blocked	
CorelVentura package	Blocked	
CPUcool package	Blocked	
Dallas package	Blocked	
Deeenes package	Blocked	
DieSiedler package	Blocked	
DropUpload package	Blocked	
Duden package	Blocked	
EFcommander package	Blocked	
eRightSoft package	Trojan:Win32/Dynamer!ac	
Execute package	Blocked	
Falcson package	Blocked	
FEAR package	Blocked	
FolderMarker package	Blocked	
FreshUI package	Blocked	
GMER package	Blocked	
HandySoftware package	Blocked	
HexEdit package	Blocked	
HurtWorld package	Blocked	

ImagePrint package	Blocked	
iMeter package	Blocked	
InterVideo package	Blocked	
IPCheck package	Blocked	
IrfanView package	Blocked	
ISPwizard package	Blocked	
ITpro package	Blocked	
LG package	Blocked	
Mages package	Blocked	
Mash package	Blocked	
MaxPayne package	Blocked	
Moorhuhn package	Blocked	
MultiLauncher package	Blocked	
Musicbase package	Blocked	
MusicMaker package	Blocked	
NetClientManager package	Blocked	
NetInfo package	Blocked	
Nolia package	Blocked	
OfView package	Blocked	
OnlineOptimizer package	Blocked	
Pause package	Blocked	
RegBench package	Blocked	
RestoreNatur package	Blocked	
RollerCoaster package	Blocked	
SafeNSec package	Blocked	
Screensaver package	Blocked	
SeekFreak package	Blocked	
StartTime package	Blocked	
SysInfo package	Blocked	
Terminator package	Blocked	
Thundersave package	Blocked	
TraxTime package	Blocked	
Tris package	Blocked	
UniMed package	Blocked	
UOM package	Blocked	
Vanderlee package	Blocked	
Vuex package	Blocked	
Warner package	Blocked	
WhatInStartup package	Blocked	
Windows package	Blocked	
Xmplay package	Blocked	
xStarter package	Blocked	
Youtubedown package	Blocked	
ZTape package	Blocked	
ZyloM package	Blocked	

Microsoft had 70 false alarms.

K7

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Trojan 7000000f1	
Adobe package	Riskware 0040eff71	
Ahnenforscher package	NetWorm 700000151	
ArcSoft package	Trojan f10005021	
Ascii package	Trojan 004def811	
Audatex package	NetWorm 700000151	
AutoCAD package	Riskware 0040eff71	
AutoDesk package	Riskware 0049f6ae1	
Avira package	Riskware 0040eff71	
Beatunes package	Trojan 0050f28e1	
CameraMonitor package	Riskware 0040eff71	
CleverCleaner package	Trojan 004def811	
ColorPicker package	Trojan f1000f011	
ConsoleHoster package	Trojan 004def811	
CounterStrike package	Riskware 0040eff71	
CrazyTaxi package	Riskware 0040eff71	
Creative package	Riskware 0040eff71	
Databecker package	Trojan 005257651	
Datacard package	Riskware 0040eff71	
Deskline package	Riskware 0040eff71	
DiffPDF package	Trojan 004def811	
DisableWinTracking package	Trojan 004ccb1e1	
Driver package	Riskware 0040eff71	
DumpIt package	Riskware 0040eff71	
EA package	Trojan 7000000f1	
Eieruhr package	Password-Stealer 004fb7421	
FileRally package	Trojan 004def811	
FTPUploader package	Riskware f15000051	
Fuhu package	Trojan 700000121	
GIMP package	Unwanted-Program 004bc56d1	
GMER package	Riskware 0040eff71	
Google package	Riskware 0040eff71	
Grub package	Trojan 700000111	
HappyFoto package	Riskware 0040eff71	
HP package	P2PWorm 004c69cd1	
IBM package	Riskware 0040eff71	
iLivid package	Riskware 0040eff71	
ImageMixer package	Trojan 0047dc6e1	
InfoCentre package	Trojan 004bf4781	
InterVideo package	Trojan 0034218c1	
Keynote package	Trojan 004def811	
Lernassistent package	Trojan f10005021	
ListSp package	Trojan 004def811	
LockNote package	Trojan 004def811	
Logitech package	Trojan f10005021	
LucasChess package	Riskware 0040eff71	
MacType package	Trojan 004def811	


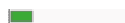

Magix package	Trojan 005257651	
MakePDF package	Unwanted-Program 004f7b361	
Maturafoto package	Trojan 7000000f1	
Medusa package	Riskware 0040eff71	
MSOffice package	Trojan 004d89db1	
MyChars package	Trojan 004def811	
NEC package	Trojan 7000000f1	
NetClientManager package	Trojan 00519c0e1	
Nokia package	Unwanted-Program 004e0f4d1	
Norton package	Riskware 0040eff71	
Nvidia package	Riskware 0040eff71	
OpenHardwareMonitor package	Trojan 004def811	
OpenSource package	Riskware 0040eff71	
OutlookBackup package	Trojan 7000000f1	
PCconnectivity package	Riskware 0040eff71	
Pipedown package	Riskware 0040eff71	
PushOver package	Trojan 004def811	
QuickWay package	Trojan 004def811	
RawWrite package	Trojan 004def811	
RollerCoaster package	Trojan 004def811	
SAM package	Riskware 0040eff71	
Scan2PC package	Riskware 0040eff71	
Scancode package	Trojan 004def811	
Screensaver package	Riskware 0040eff71	
Seagate package	Riskware 0040eff71	
Skype package	Trojan 004d65011	
StarCraft package	Trojan 004c82931	
TCPoptimizer package	Riskware 0040eff71	
TestDisk package	Trojan 004def811	
TheDebugger package	Riskware 0040eff71	
Tmobile package	Riskware 0040eff71	
TomTom package	Adware 004f2edc1	
TouchTyping package	Trojan 000141f61	
TowerToppler package	Trojan 004def811	
TXTBST package	Password-Stealer 004fb7421	
Umrechner package	Riskware 0040eff71	
Updater package	Unwanted-Program 700000121	
Vimicro package	Riskware 0040eff71	
VirtualBox package	Trojan 0051ad611	
Vuex package	Riskware 0040eff71	
Wavosaur package	Trojan f1000f011	

K7 had 88 false alarms. K7 is a new re-entry in our tests – it is to be expected that their number of false alarms will be much lower next time.

Symantec Norton











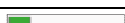
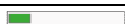


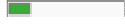






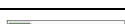


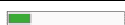











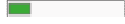



False alarm found in some parts of	Detected as	Supposed prevalence
AmericanConquest package	Trojan Horse	
AnalogX package	Trojan.Gen.8!cloud	
AntiTrojan package	Trojan.Gen.2	
AnyDVD package	Trojan.Gen.8!cloud	
ASMlessons package	Heur.AdvML.B	
Avi2Dvd package	Trojan.Gen.8!cloud	
AZN package	Packed.Cupx!gen2	
Backspin package	Trojan Horse	
Beispieldateien package	Trojan.Gen.2	
BlueSquirrel package	Heur.AdvML.B	
BmkBuddy package	Trojan.Gen.2	
BrockhausF package	Trojan Horse	
Burn package	Trojan.Gen.2	
CDDVDburner package	Heur.AdvML.B	
CDML package	Heur.AdvML.C	
Cfminibar package	Heur.AdvML.B	
CineMac package	Trojan.Gen.8!cloud	
ClearProg package	Trojan.Gen.8!cloud	
Corel package	Heur.AdvML.B	
CorelVentura package	Heur.AdvML.B	
CreativeLabs package	Heur.AdvML.C	
Dap package	Trojan.Gen.8!cloud	
Databecker package	Heur.AdvML.B	
Debugger package	Trojan.Gen.8!cloud	
Decryptor package	Heur.AdvML.B	
DrDivx package	Backdoor.Graybird	
Duden package	Trojan.Gen.8!cloud	
DVBviewer package	Heur.AdvML.A	
EKalkulator package	Heur.AdvML.A	
eRightSoft package	Trojan.Gen.2	
ESET package	Trojan.Gen.8!cloud	
Female package	Heur.AdvML.B	
Finanz package	Trojan.Gen.8!cloud	
FlashJester package	Trojan.Gen.8!cloud	
Fotograf package	Heur.AdvML.A	
FreeCrypt package	Heur.AdvML.A	
Fujitsu package	Trojan.Gen.8!cloud	
GEMER package	Trojan.Gen.8!cloud	
GPU package	Heur.AdvML.B	
GTL package	Heur.AdvML.C	
GuiPDF package	Trojan.Gen.8!cloud	
Halflife package	Trojan.Gen.2	

HashTab package	Trojan.Gen.8!cloud	
Hitman package	Trojan.Gen.8!cloud	
HyperMak package	Trojan.Gen.8!cloud	
Insaniquarium package	Trojan.Gen.8!cloud	
IrfanView package	Trojan.Gen.2	
K3D package	Heur.AdvML.C	
LANtool package	Heur.AdvML.C	
LinkMan package	Heur.AdvML.C	
Mailbox package	Heur.AdvML.C	
Miui package	Heur.AdvML.C	
Mozilla package	Trojan.Gen.8!cloud	
MyBoot package	Trojan.Gen.2	
MyCarPC package	Heur.AdvML.A	
No23recorder package	Heur.AdvML.A	
Opera package	Trojan.Gen.8!cloud	
PacManiac package	Trojan.Gen.2	
PCW package	Heur.AdvML.B	
PCwizard package	Trojan.Gen.8!cloud	
PEbuilder package	Trojan.Gen.2	
PerfMenu package	Trojan.Gen.8!cloud	
Picasa package	Heur.AdvML.A	
PodTools package	Trojan.Gen.2	
Preispiraten package	Heur.AdvML.C	
RAS package	Trojan.Gen.2	
RegCool package	Trojan.Gen.8!cloud	
RootkitShark package	Heur.AdvML.B	
SimplyZip package	Trojan.Gen.2	
Skype package	Trojan.Gen.2	
StartMeta package	Trojan.Gen.8!cloud	
SuperPower package	Trojan.Gen.8!cloud	
SweetDreams package	Trojan.Gen.2	
TerminPlaner package	Heur.AdvML.C	
Tzwei package	Heur.AdvML.C	
URLsnopper package	Backdoor.Graybird	
Vallen package	Trojan.Gen.2	
WebsiteArchive package	Trojan.Gen.2	
Wesnoth package	Trojan.Gen.2	
WinAmp package	Trojan.Gen.2	
WinHotel package	Trojan.Gen.2	
Word2PDF package	Trojan.Gen.8!cloud	
Workshop package	Trojan.Gen.2	
WTM package	Trojan.Gen.2	
XBlock package	Trojan.Gen.2	
XMplay package	Trojan.Gen.8!cloud	
Zdbackup package	Trojan.Gen.2	




ZFTP package	Heur.AdvML.A	
ZonerDraw package	Trojan.Dropper	
Zylom package	Heur.AdvML.A	

Symantec Norton had 90 false alarms.

Tencent

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Dangerous activity	
Adwcleaner package	Dangerous activity	
AgendaAtOnce package	Dangerous activity	
Alpenverein package	Dangerous activity	
Amok package	Dangerous activity	
AntiSpam package	Dangerous activity	
AnwaltOnline package	Dangerous activity	
Assi package	Dangerous activity	
Aston package	Dangerous activity	
AudioDVD package	Dangerous activity	
Ausfuellen package	Dangerous activity	
AVIjoiner package	Dangerous activity	
Avira package	Dangerous activity	
AVM package	Dangerous activity	
Baltic package	Dangerous activity	
Baywatch package	Dangerous activity	
Bluefish package	Dangerous activity	
Burn4Free package	Dangerous activity	
Chaos package	Dangerous activity	
CheckAndGet package	Dangerous activity	
Comfort package	Dangerous activity	
Comtest package	Dangerous activity	
Corel package	Dangerous activity	
Corel Ventura package	Gen:Variant.Barys.57935	
Databecker package	Dangerous activity	
DB2PDF package	Dangerous activity	
Deeenes package	Dangerous activity	
DesperateHousewives package	Dangerous activity	
DigitalTheatre package	Gen:Variant.Symmi.70545	
DUNbackup package	Dangerous activity	
DVBviewer package	Dangerous activity	
EnhanceMovie package	Dangerous activity	
eRight package	Dangerous activity	
ESET package	Dangerous activity	
ESreg package	Dangerous activity	
Execute package	Dangerous activity	
Factory package	Dangerous activity	
FileShredder package	Dangerous activity	
Freshdow package	Dangerous activity	
FTcheck package	Dangerous activity	






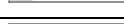
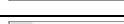





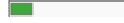



HP package	Dangerous activity	
iNetFormFiller package	Dangerous activity	
JustZipIt package	Dangerous activity	
Kao package	Dangerous activity	
KonfKit package	Dangerous activity	
L2LC package	Dangerous activity	
Leserbefragung package	Dangerous activity	
LG package	Dangerous activity	
Loop package	Dangerous activity	
MagixDVD package	Dangerous activity	
Maxres package	Dangerous activity	
Menue package	Dangerous activity	
MSOffice package	Dangerous activity	
MSWindows package	Dangerous activity	
MSWorks package	Dangerous activity	
NetClientManager package	Trojan.GenericKD.40105859	
NetTools package	Dangerous activity	
NetworkConnect package	Dangerous activity	
NetXfer package	Dangerous activity	
NewsLeecher package	Dangerous activity	
Nolia package	Dangerous activity	
OOBE package	Dangerous activity	
Pdesk package	Dangerous activity	
PDFcreate package	Dangerous activity	
PDFcreator package	Dangerous activity	
PESetEnv package	Gen:Trojan.Heur.JP.am0@aead5lo	
Pfymenu package	Dangerous activity	
PhotoEditor package	Dangerous activity	
Pia package	Dangerous activity	
PLX package	Dangerous activity	
Podifier package	Dangerous activity	
PowerArc package	Dangerous activity	
Purge package	Dangerous activity	
RedStreak package	Gen:Variant.Ursu.115789	
SefeNSec package	Dangerous activity	
Screensaver package	Dangerous activity	
SilentStorm package	Dangerous activity	
SkiRacing package	Dangerous activity	
SoftCAT package	Dangerous activity	
Solitaire package	Dangerous activity	
SteigEin package	Dangerous activity	
SuperOffice package	Dangerous activity	
Terminator package	Dangerous activity	
Texiterator package	Dangerous activity	
TNI package	Dangerous activity	
Traxtime package	Dangerous activity	
Ultrasave package	Dangerous activity	
Unreal package	Dangerous activity	
USBfix package	Dangerous activity	
VisualCD package	Dangerous activity	

WinScheduler package	Dangerous activity	
WinTBS package	Dangerous activity	
Zylom package	Dangerous activity	









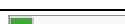








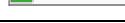

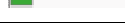


Tencent had 94 false alarms.

Trend Micro

False alarm found in some parts of	Detected as	Supposed prevalence
A43 package	Suspicious File	
Activaip package	Suspicious File	
ActualWindows package	Suspicious File	
Addition package	Suspicious File	
Adwcleaner package	Suspicious File	
AEP package	Suspicious File	
Aevita package	Suspicious File	
Alpenland package	Suspicious File	
Amok package	Suspicious File	
Aol package	Suspicious File	
Apfelmann package	Suspicious File	
ArchiCrypt package	Suspicious File	
AudioDVD package	Suspicious File	
AutoInstallation package	Suspicious File	
Azip package	Suspicious File	
Backup package	Suspicious File	
Baltic package	Suspicious File	
Bayorganizer package	Suspicious File	
Baywatcher package	Suspicious File	
Bildverkleinerer package	Suspicious File	
BIOS package	Suspicious File	
BlueOffice package	Suspicious File	
Book2Print package	Suspicious File	
Brass package	Suspicious File	
Brother package	Suspicious File	
BrowserChoice package	Suspicious File	
Capture package	Suspicious File	
CheckAndGet package	Suspicious File	
CleanDisk package	Suspicious File	
ClickMedia package	Suspicious File	
Clickris package	Suspicious File	
Corel package	Suspicious File	
Corretora package	Suspicious File	
Dallas package	Suspicious File	
Databecker package	Suspicious File	
Deeenes package	Suspicious File	
Dreikampf package	Suspicious File	
DUNbackup package	Suspicious File	
DVDIdentifier package	Suspicious File	
E2S40 package	Suspicious File	
EA package	Suspicious File	








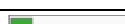


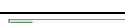


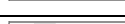


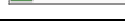


eMerge package	Suspicious File	
EuCaSoft package	Suspicious File	
EventMeister package	Suspicious File	
Fantamorph package	Suspicious File	
Fibu package	Suspicious File	
FileShredder package	Suspicious File	
FinalHit package	Suspicious File	
FireTune package	Suspicious File	
FlashJester package	Suspicious File	
FolderMarker package	Suspicious File	
Forensic package	Suspicious File	
FreeCrypt package	Suspicious File	
Freshdownload package	Suspicious File	
FreshUI package	Suspicious File	
GDATA package	Suspicious File	
Girokonto package	Suspicious File	
HandySoftware package	Suspicious File	
HDCopy package	Suspicious File	
HistoryEraser package	Suspicious File	
HotKeyz package	Suspicious File	
HPV package	Suspicious File	
IceAge package	Suspicious File	
IconXtractor package	Suspicious File	
ImageEditor package	Suspicious File	
iMeter package	Suspicious File	
iNetAdviser package	Suspicious File	
IntelliTab package	Suspicious File	
iPodBook package	Suspicious File	
ISPwizard package	Suspicious File	
Itpro package	Suspicious File	
JPEGimager package	Suspicious File	
Kalenderpack package	Suspicious File	
Kastanie package	Suspicious File	
Kicker package	Suspicious File	
Kostenkalkulator package	Suspicious File	
Kreed package	Suspicious File	
Krypter package	Suspicious File	
Lexikon package	Suspicious File	
LG package	Suspicious File	
MagicDVD package	Suspicious File	
Mash package	Suspicious File	
MaxTray package	Suspicious File	
MetaEditor package	Suspicious File	
MinGW package	Suspicious File	
MobileAssistent package	Suspicious File	
MPBrowser package	Suspicious File	
MSWindows package	Suspicious File	
Musicnet package	Suspicious File	
MyPC package	Suspicious File	
NetClientManager package	TROJ_GEN.R011C00B818	

Netlink package	Suspicious File	
NetXfer package	Suspicious File	
NextSoft package	Suspicious File	
Nfind package	Suspicious File	
nLite package	Suspicious File	
OnTime package	Suspicious File	
ORF package	TROJ_GEN.R00AC00J517	
OTP package	Suspicious File	
OxygenBag package	Suspicious File	
PaquetBuilder package	Suspicious File	
PassKeep package	Suspicious File	
Pause package	Suspicious File	
Pcanalyzer package	Suspicious File	
PDFcompressor package	Suspicious File	
Pdfkonvert package	Suspicious File	
PowerText package	Suspicious File	
Printy package	Suspicious File	
ProjectTimer package	Suspicious File	
Puzzle package	Suspicious File	
RegBench package	Suspicious File	
RegCool package	Suspicious File	
RegToy package	Suspicious File	
Reminder package	Suspicious File	
RestoreNatur package	Suspicious File	
RouterControl package	Suspicious File	
Sateirac package	Suspicious File	
Screensaver package	Suspicious File	
SeekFreak package	Suspicious File	
Ship package	Suspicious File	
SKS package	Suspicious File	
SpeedCommander package	Suspicious File	
Spline package	Suspicious File	
SpyBlocker package	Suspicious File	
Spybot package	Suspicious File	
StartDelay package	Suspicious File	
StartTime package	Suspicious File	
Startuplite package	Suspicious File	
StartupStar package	Suspicious File	
SteigEin package	Suspicious File	
SuperUser package	Suspicious File	
SynchExp package	Suspicious File	
Syslog package	Suspicious File	
Targem package	Suspicious File	
TaxiRaser package	Suspicious File	
TelefonInfo package	Suspicious File	
TraceMap package	Suspicious File	
TrafficMonitor package	Suspicious File	
Tris package	Suspicious File	
TrueCrypt package	Suspicious File	
TweakNow package	Suspicious File	

Unreal package	Suspicious File	
UOM package	Suspicious File	
VideoLogic package	Suspicious File	
VideoWave package	Suspicious File	
VOVSOFY package	Suspicious File	
Washer package	Suspicious File	
Watermill package	Suspicious File	
WebDe package	Suspicious File	
Webdesign package	Suspicious File	
WebORama package	Suspicious File	
Webvideo package	Suspicious File	
WinControl package	Suspicious File	
WinHotel package	Suspicious File	
WinSecurityGate package	Suspicious File	
WinTools package	Suspicious File	
Wizard package	Suspicious File	
WriteCD package	Suspicious File	
Wtrate package	Suspicious File	
XMLplay package	Suspicious File	
Xpired package	Suspicious File	
xStarter package	Suspicious File	
Zdefrag package	Suspicious File	
ZFTPcopy package	Suspicious File	
Zwitter package	Suspicious File	
Zylom package	Suspicious File	

Trend Micro had 166 false alarms.

Panda

False alarm found in some parts of	Detected as	Supposed prevalence
Acer package	Suspicious	
Acquire package	Suspicious	
Activa package	Suspicious	
ActualWindows package	Suspicious	
Addition package	Suspicious	
Adobe package	Suspicious	
AdvancedPDF package	Suspicious	
AdwCleaner package	Suspicious	
AEP package	Suspicious	
AgendaAtOnce package	Suspicious	
Aidsoid package	Suspicious	
Amok package	Suspicious	
Apache package	Suspicious	
Aquareal package	Suspicious	
ASDlite package	Suspicious	
Assi package	Suspicious	
Aston package	Suspicious	
Atmaxtra package	Suspicious	
AtomTech package	Suspicious	

AudioTags package	Suspicious	
Ausfuellen package	Suspicious	
AutoInstallation package	Suspicious	
AutoZip package	Suspicious	
AVG package	Trojan Trj/Genetic.gen	
Backtec package	Suspicious	
Backtozip package	Suspicious	
BackupSlave package	Suspicious	
Baltic package	Suspicious	
Baraha package	Suspicious	
Baywatch package	Suspicious	
BeClean package	Suspicious	
BibFacil package	Suspicious	
BigFish package	Suspicious	
BIMexplorer package	Suspicious	
BIOS package	Suspicious	
Bistone package	Suspicious	
BlackJack package	Suspicious	
BlueOffice package	Suspicious	
BookPrint package	Suspicious	
Brass package	Suspicious	
Brockhaus package	Suspicious	
BroLink package	Suspicious	
Brother package	Suspicious	
BrowserChoice package	Suspicious	
Busch package	Suspicious	
BusinessFlow package	Suspicious	
Caillou package	Suspicious	
Calculator package	Suspicious	
Canon package	Suspicious	
Cerberus package	Suspicious	
Cetus package	Suspicious	
CheckAndGet package	Suspicious	
CheckQuota package	Suspicious	
Cineast package	Suspicious	
Cint package	Suspicious	
CleanDisk package	Suspicious	
ClickMedia package	Suspicious	
Clickris package	Suspicious	
CloneCD package	Suspicious	
CodecPack package	Suspicious	
Comfort package	Suspicious	
CommandAndConquer package	Suspicious	
Comtest package	Suspicious	
Corel package	Suspicious	
CorelVentura package	Suspicious	
CPUFix package	Suspicious	
CreateMovie package	Suspicious	
Dallas package	Suspicious	
Databecker package	Suspicious	



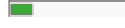
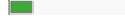




Deadlink package	Suspicious	
DebutVideo package	Suspicious	
Defrag package	Suspicious	
DeltaForce package	Suspicious	
Deskline package	Suspicious	
DesktopOK package	Suspicious	
DisableWinTracking package	Suspicious	
DiskChart package	Suspicious	
DiskSpace package	Suspicious	
Djjukebox package	Suspicious	
Doom package	Suspicious	
DoubleDriver package	Suspicious	
DrHobby package	Suspicious	
DriveIcons package	Suspicious	
DSL package	Suspicious	
DunBackup package	Suspicious	
DVBviewer package	Suspicious	
DVDregion package	Suspicious	
EasyDVD package	Suspicious	
eBook package	Suspicious	
EEP package	Suspicious	
Electra package	Suspicious	
ELWA package	Suspicious	
Emco package	Suspicious	
eMedia package	Suspicious	
eMerge package	Suspicious	
EnhancedMovie package	Suspicious	
Erotik package	Suspicious	
ESreg package	Suspicious	
EuCaSoft package	Suspicious	
EuroRechner package	Suspicious	
EventMeister package	Suspicious	
Execute package	Suspicious	
ExperienceIndex package	Suspicious	
Exportgenerator package	Suspicious	
F1 package	Suspicious	
Factory package	Suspicious	
Falcson package	Suspicious	
FastCard package	Suspicious	
FastWebs package	Suspicious	
FEAR package	Suspicious	
FIFA package	Suspicious	
FileShredder package	Suspicious	
FileWorks package	Suspicious	
FinalHit package	Suspicious	
FireTune package	Suspicious	
FiveWin package	Suspicious	
FlashJester package	Suspicious	
Floppy package	Suspicious	
FocusMagic package	Suspicious	

FolderMarker package	Suspicious	
FolderPrint package	Suspicious	
FotoFit package	Suspicious	
Fotograf package	Suspicious	
Fotokasten package	Suspicious	
Fractalus package	Suspicious	
FreshDownload package	Suspicious	
FreshUI package	Suspicious	
FTCheck package	Suspicious	
GIF2PNG package	Suspicious	
Girokonto package	Suspicious	
GliBlock package	Suspicious	
GMER package	Suspicious	
GoldenSection package	Suspicious	
Grundlagenquiz package	Suspicious	
HandySoftware package	Suspicious	
Haushalt package	Suspicious	
Helper package	Suspicious	
HideFolders package	Suspicious	
Hitrecorder package	Suspicious	
HotKeyz package	Suspicious	
HP package	Suspicious	
HurtWorld package	Trojan Trj/GdSda.A	
IBM package	Suspicious	
IceAge package	Suspicious	
Idealgewicht package	Suspicious	
IESecPro package	Suspicious	
ImagePrint package	Suspicious	
IMG package	Suspicious	
iNetAdviser package	Suspicious	
iNetFormFiller package	Suspicious	
Inifnity package	Suspicious	
InstantGalleryMaker package	Suspicious	
IPCheck package	Suspicious	
IrfanView package	Suspicious	
ITpro package	Suspicious	
Jose package	Suspicious	
JumpTo package	Suspicious	
JustZipIt package	Suspicious	
Kaffeepause package	Suspicious	
Kakuro package	Suspicious	
Kaleido package	Suspicious	
Kalenderpack package	Suspicious	
Kao package	Suspicious	
Kastanie package	Suspicious	
Keller package	Suspicious	
Knoppix package	Suspicious	
Komfort package	Suspicious	
Kreed package	Suspicious	
Laptimer package	Suspicious	

Lazarus package	Trojan Trj/GdSda.A	
LG package	Suspicious	
LinkValidator package	Suspicious	
Lohninfo package	Suspicious	
MailView package	Suspicious	
ManualAttaching package	Suspicious	
Mash package	Suspicious	
Math package	Suspicious	
Maxx package	Suspicious	
Mdaemon package	Suspicious	
MediaPlayer package	Suspicious	
Mediator package	Suspicious	
medXpert package	Suspicious	
MenuApp package	Suspicious	
Menue package	Suspicious	
Microsoft package	Suspicious	
Miller package	Suspicious	
MillionenShow package	Suspicious	
MindExplosion package	Suspicious	
MinGW package	Suspicious	
Miui package	Suspicious	
Moorhuhn package	Suspicious	
MovieJack package	Suspicious	
MP3Total package	Suspicious	
MPBrowser package	Suspicious	
MPEG2AVI package	Suspicious	
MSWindows package	Suspicious	
MSWorks package	Suspicious	
MultipleCamera package	Suspicious	
MusicNet package	Suspicious	
NachtStation package	Suspicious	
NetClientManager package	Suspicious	
NetGear package	Suspicious	
NetLink package	Suspicious	
NetTools package	Suspicious	
NewsLeecher package	Suspicious	
NextSoft package	Suspicious	
Nfind package	Suspicious	
Nlite package	Suspicious	
Nokia package	Suspicious	
NotesBrowser package	Suspicious	
OEMFirstRun package	Suspicious	
Olivetti package	Suspicious	
OnlineOptimizer package	Suspicious	
OnlineTV package	Suspicious	
OnTime package	Suspicious	
OpenOffice package	Suspicious	
Opera package	Suspicious	
Orcame package	Suspicious	
OutlookTuner package	Suspicious	

OxygenBag package	Suspicious	
Ozi package	Suspicious	
PartitionDoctor package	Suspicious	
PasswordSafe package	Suspicious	
PatchIt package	Suspicious	
Pause package	Suspicious	
PDFcompressor package	Suspicious	
PDFcreator package	Suspicious	
Peload package	Suspicious	
PersonalDesktop package	Suspicious	
PhotoBC package	Suspicious	
PhotoWizard package	Suspicious	
Preishai package	Suspicious	
Pristine package	Suspicious	
ProList package	Suspicious	
Provisionsrechner package	Suspicious	
PSZip package	Suspicious	
Purge package	Suspicious	
Puzzle package	Suspicious	
RecoveryTool package	Suspicious	
RegBench package	Suspicious	
RegEditor package	Suspicious	
RegToy package	Suspicious	
Reminder package	Suspicious	
RemoveFromRegistry package	Suspicious	
ResetWueng package	Suspicious	
RestoreNatur package	Suspicious	
SafeNSec package	Trojan Trj/CI.A	
Sateirac package	Suspicious	
ScanSoft package	Suspicious	
Screensaver package	Suspicious	
SearchMyDiscs package	Suspicious	
SecureNotes package	Suspicious	
SiGuardian package	Suspicious	
SilentDrive package	Suspicious	
SimplyZip package	Suspicious	
SkiRacing package	Suspicious	
SL package	Suspicious	
SlipStreamer package	Suspicious	
SoftCAT package	Suspicious	
Solitaire package	Suspicious	
SpeedCommander package	Suspicious	
Spline package	Suspicious	
SSC package	Suspicious	
StartDelay package	Suspicious	
StartTime package	Suspicious	
Startupstar package	Suspicious	
StarWars package	Suspicious	
SteigEin package	Suspicious	
SuperOffice package	Suspicious	

SuperUser package	Suspicious	
SysReport package	Suspicious	
SysTray package	Suspicious	
Tage package	Suspicious	
TagesAnzeiger package	Suspicious	
TakeABreak package	Suspicious	
Tankwart package	Suspicious	
TelefonCD package	Suspicious	
TelefonInfo package	Suspicious	
Terzio package	Suspicious	
Texefex package	Suspicious	
Thundersave package	Suspicious	
TippTop package	Suspicious	
Tiscali package	Backdoor Trojan Unknown name	
TNI package	Suspicious	
ToolLoader package	Suspicious	
TraceMap package	Suspicious	
Traduzioni package	Suspicious	
Traxtime package	Suspicious	
TributeToMagic package	Suspicious	
Tris package	Suspicious	
Truckers package	Suspicious	
TrueCrypt package	Suspicious	
TweakNow package	Suspicious	
UBCD package	Suspicious	
Ultrasave package	Suspicious	
Unidream package	Suspicious	
Unreal package	Suspicious	
UOM package	Suspicious	
UpdateBackup package	Suspicious	
Updater package	Suspicious	
USBaccess package	Suspicious	
USBagent package	Suspicious	
VideoWave package	Suspicious	
VisualCD package	Suspicious	
vLite package	Suspicious	
VorlagenExplorer package	Suspicious	
VOVSOFTE package	Suspicious	
Vuex package	Trojan Trj/Zbot.M	
Wanyword package	Suspicious	
Washer package	Suspicious	
Watermill package	Suspicious	
WebvideoAuthor package	Suspicious	
WesternDigital package	Suspicious	
WhatInStartup package	Suspicious	
Wifi package	Suspicious	
WinHotel package	Trojan Trj/CI.A	
WinPower package	Suspicious	
WinSecurityGate package	Suspicious	
Wisini package	Trojan Trj/Genetic.gen	

WriteCD package	Suspicious	
Xint package	Suspicious	
xStarter package	Suspicious	
Zdefrag package	Suspicious	
ZFTPcopy package	Suspicious	
ZipPlus package	Suspicious	
ZTape package	Suspicious	
ZyloM package	Suspicious	

Panda had 327 false alarms.

Copyright and Disclaimer

This publication is Copyright © 2018 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 2018)