

Details about the discovered False Alarms



Appendix to the Anti-Virus Comparative September 2013

Language: English

September 2013

Last Revision: 8th October 2013

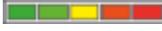
www.av-comparatives.org

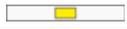
Details about the discovered false alarms

With AV testing it is important to measure not only detection capabilities but also reliability - one of reliability aspects is certainly product's tendency to flag clean files as infected. No product is immune from false positives (FP's) but there are differences among them and the goal is to measure them. Nobody has all legitimate files that exist and so no "ultimate" test of FP's can be done. What can be done and is reasonable, is to create and use a set of clean files which is independent. If on such set one product has e.g. 50 FP's and another only 10, it is likely that the first product is more prone to FP's than the other. It doesn't mean the product with 10 FP's doesn't have more than 10 FP's globally, but important is the relative number.

All listed false alarms were encountered at time of testing and should by now have been fixed. False alarms caused by unencrypted data blocks in Anti-Virus related files were not counted. If a product had several false alarms belonging to the same software, it is counted here as only one false alarm. Cracks, keygens, etc. or other highly questionable tools, including FP's 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 with were digitally signed are considered more important. Due to that, a file with e.g. prevalence "level 1" and a digital signature is upgraded to next level (e.g. prevalence "level 2").

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	Such cases are likely to be seen very less frequently in a false alarm test done at a specific time, as such files are usually either whitelisted or would be noticed and fixed very fast.
5 	Probably several hundred of thousands (or millions) of users	

Most false alarms will probably most of the times fall into the first two levels. In our opinion, Anti-Virus products should not have false alarms on any sort of clean files despite 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 (currently 15 [including low-prevalent FP's]) of false alarms 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 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 QA of signatures before release, etc.

False Positives (FPs) are an important measurement for AV quality. One FP report from a customer can result in large amount of engineering and support work to resolve the issue. Sometimes this can even lead to important data loss or system unavailability.

Even "not significant" FPs (or FP's 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 FP again on a more significant file. Thus, they still deserve mention and still deserve penalty.

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

Microsoft

Microsoft had zero false alarms over our set of clean files.

ESET

False alarm found in some parts of Shanghai package	Detected as Win32/Agent.UWX	Supposed prevalence 
---	---------------------------------------	---

ESET had 1 false alarm.

F-Secure

False alarm found in some parts of GameBox package PerfectFit package	Detected as Gen:Variant.Symmi.18707 Gen:Variant.Symmi.29256	Supposed prevalence  
--	--	--

F-Secure had 2 false alarms.

Fortinet

False alarm found in some parts of GameGuard package InfoPen package KorInstall package	Detected as W32/Packed.2D18!tr W32/LockScreen.LOL!tr W32/FakeAlert.GY!tr	Supposed prevalence   
---	--	---

Fortinet had 3 false alarms. As Fortinet is a product for corporate users, which computers are managed by an administrator, most of the above discovered FP's may not be a big issue.

Kaspersky

False alarm found in some parts of InterVideo package MediaShow package NetTools package Pkv package	Detected as UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Trojan.Win32.Refroso.evle	Supposed prevalence    
---	--	--

UniMed package

Worm.Win32.WBNA.syo



Kaspersky had 5 false alarms.

Emsisoft

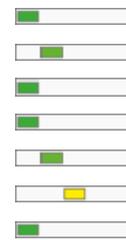
False alarm found in some parts of

- FotoLaborExpress package
- GameBox package
- GhostLadder package
- PerfectFit package
- Pkv package
- SecretZip package
- TotalNetworkInventory package

Detected as

- Trojan.Generic.8491591
- Gen:Variant.Symmi.18707
- Gen:Trojan.Heur.VP.sC0aaK29AeG
- Gen:Variant.Symmi.29256
- Trojan.GenericKDV.1217830
- Trojan.Generic.KDV.380869
- Trojan.Generic.1607609

Supposed prevalence



Emsisoft had 7 false alarms.

BitDefender

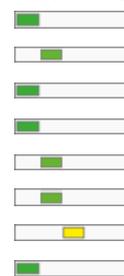
False alarm found in some parts of

- FotoLaborExpress package
- GameBox package
- GhostLadder package
- PerfectFit package
- PKV package
- SafeSystems package
- SecretZip package
- TotalNetworkInventory package

Detected as

- Trojan.Generic.8491591
- Gen:Variant.Symmi.18707
- Gen:Trojan.Heur.VP.sC0aaK29AeG
- Gen:Variant.Symmi.29256
- Trojan.GenericKDV.1217830
- Gen:Trojan.Heur.RP.WAWaayUETIei
- Trojan.Generic.KDV.380869
- Trojan.Generic.1607609

Supposed prevalence



BitDefender had 8 false alarms.

BullGuard

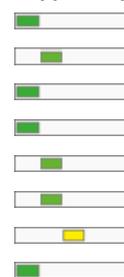
False alarm found in some parts of

- FotoLaborExpress package
- GameBox package
- GhostLadder package
- PerfectFit package
- Pkv package
- SafeSystems package
- SecretZip package
- TotalNetworkInventory package

Detected as

- Trojan.Generic.8491591
- Gen:Variant.Symmi.18707
- Gen:Trojan.Heur.VP.sC0aaK29AeG
- Gen:Variant.Symmi.29256
- Trojan.GenericKDV.1217830
- Gen:Trojan.Heur.RP.WAWaayUETIei
- Trojan.Generic.KDV.380869
- Trojan.Generic.1607609

Supposed prevalence



BullGuard had 8 false alarms.

Sophos

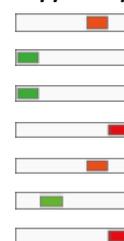
False alarm found in some parts of

- Badgwinner package
- BidFacile package
- FirstAid package
- GamePark package
- JkDefrag package
- Shanghai package
- SoftwareInformer package

Detected as

- Mal/VB-AHO
- Mal/Generic-S
- Troj/Agent-ACSQ
- Mal/Generic-S
- Mal/Generic-L
- Mal/Generic-S
- Mal/Generic-S

Supposed prevalence



UniMed package Mal/Generic-S 

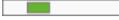
Sophos had 8 false alarms. As Sophos is a product for corporate users, which computers are managed by an administrator, most of the above discovered FP's may not be a big issue.

Avast

False alarm found in some parts of	Detected as	Supposed prevalence
AVG package	Win32:Malware-gen	
ClonyXXL package	Win32:Malware-gen	
HDCleaner package	Win32:Malware-gen	
InterMute package	Win32:Malware-gen	
Kodak package	Win32:Malware-gen	
MyHomeInventory package	Win32:Trojan-gen	
SafeXP package	Win32:Malware-gen	
SunGard package	Win32:FakeAV-BGO	
UniMed package	Win32:Malware-gen	
Zattoo package	Win32:Rebhip-BJ	

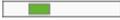
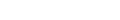
Avast had 10 false alarms.

AhnLab

False alarm found in some parts of	Detected as	Supposed prevalence
ArcSoft package	Trojan/Win32.Koutodoor	
Areaker package	Worm/Win32.Franriv	
ASUSDriver package	Trojan/Win32.Agent	
AVG package	Win-Trojan/Agent.945328	
CDDVDBurner package	Packed/Upack	
EasyBurning package	ASD.Prevention	
L2LC package	Win32/MalPackedB.suspicious	
RaidDriver package	Trojan/Win32.Zbot	
SafeSeven package	ASD.Prevention	
TightVnc package	ASD.Prevention	
Vispa package	Packed/Upack	
WinSetup package	Win-Trojan/Img-wmf.6144.B	
WinWD package	Win-Trojan/Wsnpoem.399872	

AhnLab had 13 false alarms.

Qihoo

False alarm found in some parts of	Detected as	Supposed prevalence
FotoLaborExpress package	Trojan.Generic.8491591	
GameBox package	Gen:Variant.Symmi.18707	
GifAnima package	Trojan.PSW.Win32.Misc.C	
GhostLadder package	Gen:Trojan.Heur.VP.sC0aaK29AeG	
IBM package	Trojan.PSW.Win32.Misc.C	
IconChan package	Trojan.PSW.Win32.Misc.C	
Lenovo package	Trojan.PSW.Win32.Misc.C	
PerfectFit package	Gen:Variant.Symmi.29256	
Pkv package	Trojan.GenericKDV.1217830	
Python package	Trojan.PSW.Win32.Misc.C	
SafeSystems package	Gen:Trojan.Heur.RP.WAWaayUETIei	

SecretZip package	Trojan.Generic.KDV.380869	
TotalNetworkInventory package	Trojan.Generic.1607609	

Qihoo had 13 false alarms.

Trend Micro

False alarm found in some parts of

- Brockhaus package
- ChatZum package
- Direct package
- Emerald package
- Hausdesign package
- Korean package
- ShenZhen package
- SoftDistribution package
- Softtone package
- Tiffanet package
- TuoLang package
- UniMed package
- Video package
- VoiceFuture package

Detected as

- TROJ_GEN.RCBCOE9
- BKDR_BIFROSE.BMC
- TROJ_GEN.FCBCBK9
- Mal_Mlwr-13
- TROJ_AGENT_CA250284.TOMC
- TROJ_GEN.RCBCPCO
- TROJ_GEN.FCBCBKS
- TROJ_GEN.FCBCBKS
- TROJ_GEN.FCBCBLA
- TROJ_GEN.FCBCBKJ
- TROJ_GEN.FCBCBK9
- TROJ_GEN.ROCBCOPGK13
- TROJ_GEN.FCBCBL7
- TROJ_GEN.FCBCBKQ

Supposed prevalence



Trend Micro had 14 false alarms.

AVIRA

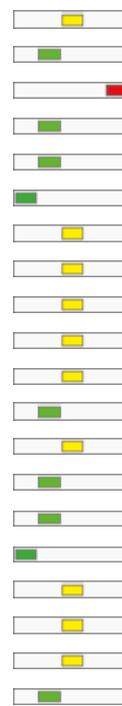
False alarm found in some parts of

- Bins package
- Cargo package
- Chinese package
- DBXExtract package
- DWB package
- Ewido package
- Exent package
- FastRestore package
- GameOtter package
- GameProtect package
- Korean package
- Namtuk package
- NetLeverage package
- RemoteSupport package
- SmartSynch package
- SyncWrangler package
- Toolchain package
- UniMed package
- Xiamen package
- Yascu package

Detected as

- TR/Swisyn.bpmd.1
- TR/ATRAPS.Gen
- TR/Spy.Banker.Gen
- TR/VB.Downloader.Gen8
- TR/Agent.789264
- TR/Agent.cada.3794
- TR/Agent.782704
- JS/Redirector.E.90
- TR/Spy.Gen
- TR/Rootkit.Gen
- TR/Zusy.1104858
- TR/Dropper.MSIL.Gen
- TR/Crypt.ULPM.Gen2
- TR/Barys.1607.13
- TR/Spy.29696.213
- TR/Dropper.Gen8
- TR/Dropper.Gen
- TR/Rogue.kdv.844905
- TR/Kazy.78259.1
- HEUR/Crypted

Supposed prevalence



AVIRA had 20 false alarms.

Kingsoft

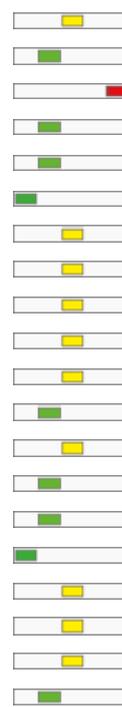
False alarm found in some parts of

- Bins package
- Cargo package
- Chinese package
- DBXExtract package
- DWB package
- Ewido package
- Exent package
- FastRestore package
- GameOtter package
- GameProtect package
- Korean package
- Namtuk package
- NetLeverage package
- RemoteSupport package
- SmartSynch package
- SyncWrangler package
- Toolchain package
- UniMed package
- Xiamen package
- Yascu package

Detected as

- TR/Swisyn.bpmd.1
- TR/ATRAPS.Gen
- TR/Spy.Banker.Gen
- TR/VB.Downloader.Gen8
- TR/Agent.789264
- TR/Agent.cada.3794
- TR/Agent.782704
- JS/Redirector.E.90
- TR/Spy.Gen
- TR/Rootkit.Gen
- TR/Zusy.1104858
- TR/Dropper.MSIL.Gen
- TR/Crypt.ULPM.Gen2
- TR/Barys.1607.13
- TR/Spy.29696.213
- TR/Dropper.Gen8
- TR/Dropper.Gen
- TR/Rogue.kdv.844905
- TR/Kazy.78259.1
- HEUR/Crypted

Supposed prevalence



Kingsoft had 20 false alarms.

McAfee

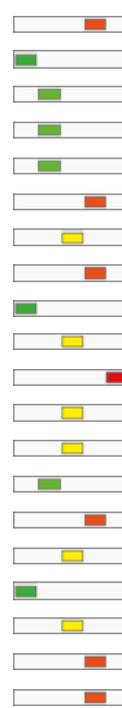
False alarm found in some parts of

- BigKahunaReef package
- Brockhaus package
- CargoAgent package
- ClearProg package
- DWB package
- GameCup package
- Gimas package
- GoogleBAE package
- HitmanPro package
- Iowa package
- IPmessenger package
- Korean package
- Ku6 package
- PKV package
- Rice package
- SecretMaker package
- Snow package
- SoftSecurity package
- Sports package
- Tetrix package

Detected as

- Artemis!714749875DCD
- Artemis!0D5EB245F1F8
- Artemis!44A89F013002
- Artemis!8CED91030DFC
- Artemis!09FF7A6BC767
- Artemis!CA535D4BC22A
- Artemis!0487C8108496
- Artemis!35082C362BE9
- Artemis!75990A8CBE5A
- GenericTRA-BO!D356D0448A69
- Artemis!C7A1D2955161
- Artemis!037F415A7A4F
- Artemis!04AC76D28C36
- Artemis!354013A1AB2F
- Artemis!A16201777ACD
- Artemis!8CED91030DFC
- Artemis!BF50F1E4035B
- Artemis!20110A6CC9A2
- Artemis!89C6A8BAECOD
- Artemis!974A0DF753AF

Supposed prevalence



McAfee had 20 false alarms.

Panda

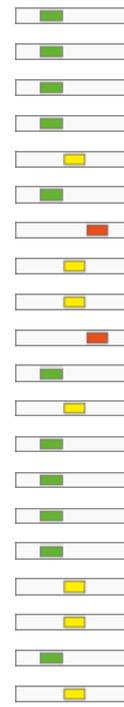
False alarm found in some parts of

360 package
 AvantGard package
 ClientKeeper package
 DWB package
 eCruiser package
 FFDSHOW package
 GameCup package
 Iowa package package
 IPmanager package
 KBC package
 Korean package
 Ku6 package
 LouYue package
 McLeod package
 Qizhi package
 Qplus package
 SoftDistribution package
 SoftSecurity package
 Spamihilator package
 TimeCount package

Detected as

Suspicious file
 Trj/TheD.B
 Trj/CI.A
 Trj/CI.A
 Suspicious file
 Suspicious file

Supposed prevalence



Panda had 20 false alarms.

Tencent

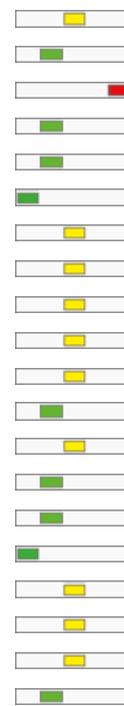
False alarm found in some parts of

Bins package
 Cargo package
 Chinese package
 DBXExtract package
 DWB package
 Ewido package
 Exent package
 FastRestore package
 GameOtter package
 GameProtect package
 Korean package
 Namtuk package
 NetLeverage package
 RemoteSupport package
 SmartSynch package
 SyncWrangler package
 Toolchain package
 UniMed package
 Xiamen package
 Yascu package

Detected as

TR/Swisyn.bpmd.1
 TR/ATRAPS.Gen
 TR/Spy.Banker.Gen
 TR/VB.Downloader.Gen8
 TR/Agent.789264
 TR/Agent.cada.3794
 TR/Agent.782704
 JS/Redirector.E.90
 TR/Spy.Gen
 TR/Rootkit.Gen
 TR/Zusy.1104858
 TR/Dropper.MSIL.Gen
 TR/Crypt.ULPM.Gen2
 TR/Barys.1607.13
 TR/Spy.29696.213
 TR/Dropper.Gen8
 TR/Dropper.Gen
 TR/Rogue.kdv.844905
 TR/Kazy.78259.1
 HEUR/Crypted

Supposed prevalence



Tencent had 20 false alarms.

G DATA

False alarm found in some parts of

AvantGard package

Barrage package

CDDVDBurning package

ClonyXXL package

DateCalc package

DB2EXE package

DesktopIniMaker package

DigitalImaging package

GameBox package

GlaryUtilities package

HWSensors package

MultiInstall package

PerfectFit package

Pkv package

Racing package

SecretZip package

Tools package

TuoLang package

VistaDriveIcon package

VistaMizer package

WinOnCD package

WinsockFix package

Detected as

Win32.Trojan.Agent.KVSRIX

Win32.Trojan-Dropper.Generic.D

Win32.Trojan.Winlock.A

Win32.Trojan.Agent.8Y3L9G

Win32.Trojan.Jorik.F@gen

Win32.Trojan.VB.NT

Win32.Worm.Autorun.A@gen

Win32.Trojan.Agent.QYCENO

Gen:Variant.Symmi.18707

Win32.Worm.Autorun.A@gen

Win32.Trojan.Banload.A

Win32.Trojan.Winlock.A

Gen:Variant.Symmi.29256

Trojan.GenericKDV.1217830

Gen:Trojan.Heur.VP.sC0aaK29AeG

Trojan.Generic.KDV.380869

Win32.Trojan-Dropper.Cloner.C

Win32.Trojan.FlyStudio.F

Win32.Trojan.VB.AIN

Win32.Trojan.VB.AIN

Win32.Worm.Autorun.A@gen

Win32.Trojan.VB.GE

Supposed prevalence



G DATA had 22 false alarms.

AVG

False alarm found in some parts of

3DATlas package

Altiris package

Angelad package

CargoAgent package

CDCop package

Changsha package

ClickExe package

DigiFoto package

Disney package

DrWeb package

DWB package

DY package

Etope package

Fasm package

GameProtect package

GDATA package

Korea package

MaxAs10 package

Mom365 package

Moorhuhn package

OpenOffice package

Pandora package

Detected as

Win32/DH.C943D6CB

PSW.Generic8.BKY0

Win32/DH{QSAiJRMbnkIK}

Downloader.Generic12.AOZB

Win32/DH{Ewx8fQBYNQ}

Win32/DH{QRMgLiILTg}

Dropper.Generic7.CJCT

Generic29.VZH

Win32/Heur

Win32/Heri

SHeur2.BFWH.dropper

Win32/DH{QSAiJQIXTg}

Downloader.Generic8.CAZC

Generic8_c.CIQD

Win32/PolyCrypt

Win32/DH{VUQgZCE}

Dropper.Generic3.AGTH.dropper

Generic8_c.BLJJ

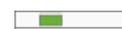
Win32/DH{ADVYQx5Py4S}

Generic24.BDMZ

Generic32.ADG

Generic_r.CK0

Supposed prevalence



DVBViewer package	Suspicious.Cloud.7.F	
Ewido package	Trojan.ADH.2	
Eznix package	Trojan.ADH.2	
Gimas package	WS.Malware.2	
IPmanager package	Suspicious.Cloud.9	
iWin package	Trojan.ADH	
Keyword package	Suspicious.Cloud.9	
Korean package	Suspicious.Cloud.9	
L2LC package	Suspicious.MH690.A	
OEsignup package	Trojan.ADH	
PodCom package	Suspicious.Cloud.9	
Scherba package	Trojan.ADH.2	
ShowSoft package	Suspicious.Cloud.9	
SMP package	Suspicious.Cloud.2	
Snow package	Suspicious.Cloud.9	
SonoControl package	Suspicious.Cloud.9	
SpamBully package	Suspicious.Cloud.5.A	
TabBrowser package	Suspicious.Cloud.2	
TrueCafe package	Suspicious.Cloud.2	
TumTool package	Suspicious.MH690.A	
TuningXP package	Suspicious.Cloud.2	
Tuto package	Suspicious.Cloud.9	
UniversalTranslator package	Suspicious.MH690.A	
Update package	WS.Malware.2	
VirtualBox package	Suspicious.MH690.A	
Vispa package	Suspicious.MH690.A	
XiTao package	Suspicious.Cloud.9	
XPY package	Trojan.ADH	
ZonerPhotoStudio package	Trojan.Dropper	

Symantec had 37 false alarms.

Vipre

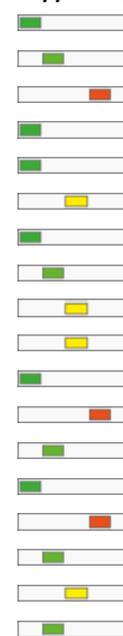
False alarm found in some parts of

- ACLive package
- AdvancedUninstaller package
- AntiCheat package
- Brockhaus package
- Brunhilda package
- ChinaSecurity package
- Chrome package
- DeeEnEs package
- Duomi package
- Evil package
- FishBase package
- Folder2ISO package
- Grub package
- Hauppage package
- HelloKitty package
- iWin package
- Korea package
- Mail package

Detected as

- BehavesLike.Win32.Malware.klt (mx-v)
- Realtime-Spy (fs)
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic!BT
- LooksLike.Win32.Malware.i (v)
- Trojan.Win32.Generic!BT
- Look alike.Win32.Sirefef.p (v)
- Trojan.Win32.Generic!SB.0
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic!BT
- LooksLike.Win32.Sirefef.zc (v)
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic.pak!cobra
- Trojan.Win32.Generic!BT
- Trojan.Win32.Generic.pak!cobra
- Trojan.Win32.Generic.pak!cobra

Supposed prevalence



Mone package	Trojan.Win32.Generic!SB.0	
Need4Speed package	Trojan.Win32.Clicker!BT	
PDF4Free package	Trojan.Win32.Clicker!BT	
PeopleSearch package	Trojan.Win32.Generic.pak!cobra	
Pkv package	Trojan.Win32.Clicker!BT	
Podcom package	Trojan.Win32.Generic.pak!cobra	
ProcessManager package	Trojan.Win32.Generic!BT	
Rice package	Trojan.Win32.Generic.pak!cobra	
Softone package	Trojan.Win32.Generic.pak!cobra	
SoftSecurity package	Trojan.Win32.Generic!SB.0	
Sports package	LooksLike.Win32.InfectedFile!B (v)	
TimeCount package	Trojan.Win32.Generic!BT	
UniMed package	Trojan.Win32.Clicker!BT	
Visualization package	Trojan-Downloader.Win32.Agent	
WiseCommerce package	Trojan.Win32.Generic!SB.0	
Xelerator package	Backdoor.SDBot	
XPY package	Trojan.Win32.Generic!BT	
Zhizhu package	Trojan.Win32.Generic.pak!cobra	
Zylom package	Trojan.Win32.Generic.pak!cobra	

Vipre had 37 false alarms.

Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (October 2013)