# Details of False Alarms

## Appendix to the Anti-Virus Comparative September 2018

Language: English

September 2018
Last Revision: 11th October 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”). Extinct 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.

### ESET

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| Dashnite package | a variant of Win32/Injector.DWIM trojan | 🟩 |

ESET had 1 false alarm.

### AVIRA

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| ComfortUpdater package | TR/Dropper.MSIL.owqsp | 🟩 |
| Tickmeter package | HEUR/APC (Cloud) | 🟩 |

AVIRA had 2 false alarms.

### Avast

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| BMKbuddy package | Win32:Malware-gen | 🟩 |
| Lockbox package | Win32:Malware-gen | 🟨 |
| Photomatix package | Win32:Kraton-A [Trj] | 🟩 |
| Spryzip package | Win32:Malware-gen | 🟩 |
| TakeABreak package | Win32:Malware-gen | 🟩 |

Avast had 5 false alarms.

## AVG

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| BMKbuddy package | Win32:Malware-gen | 🟩 |
| Lockbox package | Win32:Malware-gen | 🟨 |
| Photomatix package | Win32:Kraton-A [Trj] | 🟩 |
| Spryzip package | Win32:Malware-gen | 🟩 |
| TakeABreak package | Win32:Malware-gen | 🟩 |

AVG had 5 false alarms.

## Kaspersky Lab

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| Doppeldecker package | HEUR:Trojan.Win32.Agent.gen | 🟨 |
| Melody package | UDS:Trojan-Banker.Win32.ClipBanker.sb | 🟩 |
| NetClientManager package | HEUR:RiskTool.Win32.Generic | 🟩 |
| Sony package | Trojan-Ransom.Win32.Foreign.nzdy | 🟧 |
| SubmitTwo package | UDS:Trojan.Win32.Agent.a | 🟩 |

Kaspersky Lab had 5 false alarms.

## Bitdefender

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| ComfortUpdater package | Gen:Variant.Ursu.220013 | 🟩 |
| E-Calc package | Gen:Variant.Symmi.61975 | 🟩 |
| FileWorks package | Gen:Variant.Jacard.128910 | 🟩 |
| Gero package | Advanced Threat Defense | 🟩 |
| Herold package | Gen:Variant.Ursu.147178 | 🟩 |
| MaceGriffin package | Gen:Suspicious.Cloud.8.kqW@auZOhyni | 🟩 |
| MyPhoneExplorer package | Gen:Variant.Ursu.281421 | 🟨 |
| Qualimail package | Generic.Malware.SMH@mmg.0B88689C | 🟩 |
| TextScan package | Advanced Threat Defense | 🟩 |

Bitdefender had 9 false alarms.

## Emsisoft

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| AntiDuplicate package | Blocked | 🟩 |
| BlueTooth package | Blocked | 🟥 |
| ComfortUpdater package | Gen:Variant.Ursu.220013 (B) | 🟩 |
| FileWorks package | Gen:Variant.Jacard.128910 (B) | 🟩 |
| Herold package | Gen:Variant.Ursu.147178 (B) | 🟩 |
| MyPhoneExplorer package | Gen:Variant.Ursu.281421 (B) | 🟨 |
| Qualimail package | Generic.Malware.SMH@mmg.0B88689C (B) | 🟩 |
| Restore package | Blocked | 🟩 |
| StartTime package | Blocked | 🟩 |

| | | |
|---|---|---|
| Yabe package | DeepScan:Generic.MSIL.DownloaderB.420228B4 (B) | 🟩 |

Emsisoft had 10 false alarms.

## BullGuard

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| ComfortUpdater package | Gen:Variant.Ursu.220013 | 🟩 |
| ConnectionManager package | Suspicious | 🟨 |
| E-Calc package | Gen:Variant.Symmi.61975 | 🟩 |
| FileWorks package | Gen:Variant.Jacard.128910 | 🟩 |
| GranParadiso package | Suspicious | 🟩 |
| Herold package | Gen:Variant.Ursu.147178 | 🟩 |
| Magix package | Suspicious | 🟨 |
| MyPhoneExplorer package | Gen:Variant.Ursu.281421 | 🟨 |
| NetClientManager package | Suspicious | 🟩 |
| Qualimail package | Generic.Malware.SMH@mmg.0B88689C | 🟩 |
| Rainmeter package | Suspicious | 🟨 |
| TakeABreak package | Suspicious | 🟩 |
| TKKG package | Suspicious | 🟨 |

BullGuard had 13 false alarms.

## Tencent

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| ComfortUpdater package | Gen:Variant.Ursu.220013 | 🟩 |
| E-Calc package | Gen:Variant.Symmi.61975 | 🟩 |
| FileWorks package | Gen:Variant.Jacard.128910 | 🟩 |
| Gero package | Dangerous | 🟩 |
| Herold package | Gen:Variant.Ursu.147178 | 🟩 |
| IeTester package | Gen:Variant.Ursu.231296 | 🟩 |
| MyPhoneExplorer package | Gen:Variant.Ursu.281421 | 🟨 |
| Qualimail package | Generic.Malware.SMH@mmg.0B88689C | 🟩 |
| SemSim package | Dangerous | 🟨 |
| TextScan package | Dangerous | 🟩 |
| TotalRecorder package | Dangerous | 🟩 |
| Wavosaur package | Dangerous | 🟥 |
| WinTBS package | Dangerous | 🟩 |
| Yabe package | DeepScan:Generic.MSIL.DownloaderB.420228B4 | 🟩 |

Tencent had 14 false alarms.

## VIPRE

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| Bitdefender package | Misc (General) | 🟩 |
| ComfortUpdater package | Gen:Variant.Ursu.220013 | 🟩 |
| ConnectionManager package | Virus.Generic | 🟨 |
| DropUpload package | Misc (General) | 🟩 |

| | | |
|---|---|---|
| E-Calc package | Gen:Variant.Symmi.61975 | 🟩 |
| Easybuch package | Misc (General) | 🟩 |
| FEAR package | Misc (General) | 🟩 |
| FileWorks package | Gen:Variant.Jacard.128910 | 🟩 |
| Herold package | Gen:Variant.Ursu.147178 | 🟩 |
| Mingw package | Misc (General) | 🟩 |
| MyPhoneExplorer package | Gen:Variant.Ursu.281421 | 🟨 |
| Qualimail package | Generic.Malware.SMH@mmg.0B88689C | 🟩 |
| TextScan package | Misc (General) | 🟩 |
| Zoner package | Misc (General) | 🟩 |

VIPRE had 14 false alarms.

## F-Secure

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| ComfortUpdater package | Gen:Variant.Ursu.220013 | 🟩 |
| EFcommander package | Suspicious | 🟩 |
| F1 package | Suspicious | 🟩 |
| FileWorks package | Gen:Variant.Jacard.128910 | 🟩 |
| GPLegends package | Suspicious | 🟩 |
| Herold package | Gen:Variant.Ursu.147178 | 🟩 |
| IeTester package | Gen:Variant.Ursu.231296 | 🟩 |
| KeePass package | Suspicious | 🟥 |
| MultiBrowser package | Suspicious | 🟩 |
| OpenOffice package | Suspicious | 🟩 |
| Qualimail package | Generic.Malware.SMH@mmg.0B88689C | 🟩 |
| Stinger package | Trojan:W32/Generic.bd6cc1b9af!Online | 🟥 |
| TakeABreak package | Suspicious | 🟩 |
| WinTBS package | Suspicious | 🟩 |
| Yabe package | DeepScan:Generic.MSIL.DownloaderB.420228B4 | 🟩 |

F-Secure had 15 false alarms.

## Panda

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| Bae package | Trj/Dtcontx.D | 🟨 |
| Bitdefender package | Blocked | 🟩 |
| ClearProg package | Blocked | 🟩 |
| ConnectionManager package | Blocked | 🟨 |
| DivX package | Blocked | 🟥 |
| Doppeldecker package | Blocked | 🟨 |
| DropUpload package | Blocked | 🟩 |
| Easybuch package | Blocked | 🟩 |
| EasyExif package | Blocked | 🟥 |
| EFcommander package | Trj/GdSda.A | 🟨 |
| EmailValidator package | Blocked | 🟩 |
| Encryption package | Blocked | 🟨 |
| Herold package | Blocked | 🟩 |

| | | |
|---|---|---|
| HP package | Blocked | 🟨 |
| Logik package | Blocked | 🟩 |
| MagicSkin package | Blocked | 🟨 |
| Melody package | Blocked | 🟩 |
| OpenOffice package | Blocked | 🟩 |
| PaperOffice package | Blocked | 🟩 |
| Perfekt package | Blocked | 🟩 |
| RegDefrag package | Blocked | 🟩 |
| Restore package | Blocked | 🟩 |
| Tickmeter package | Blocked | 🟩 |
| Tiscali package | Trj/CI.A | 🟩 |
| TKKG package | Blocked | 🟨 |
| Tonec package | Blocked | 🟩 |
| TotalRecorder package | Blocked | 🟩 |
| Zdataburn package | Blocked | 🟩 |

Panda had 28 false alarms.

## Microsoft

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| AddTime package | Trojan:Win32/Bitrep.B | 🟩 |
| AhnenForscher package | Exploit:097M/CVE-2017-8570.A | 🟩 |
| AxBx package | Trojan:Win32/Bitrep.B | 🟥 |
| ConnectionManager package | Trojan:Win32/Bitrep.B | 🟨 |
| CPserver package | Trojan:Win32/Bitrep.B | 🟥 |
| DVB package | Trojan:Win32/Bitrep.B | 🟨 |
| EA package | Trojan:Win32/Bitrep.B | 🟩 |
| EFcommander package | Trojan:Win32/Bitrep.B | 🟩 |
| Encryption package | Trojan:Win32/Bitrep.B | 🟩 |
| eRightSoft package | Trojan:Win32/Bitrep.B | 🟥 |
| FastStone package | Trojan:Win32/Bitrep.B | 🟩 |
| FileZilla package | Trojan:Win32/Bitrep.B | 🟩 |
| Fractalus package | Trojan:Win32/Zpevdo.A | 🟩 |
| Gotcha package | Trojan:Win32/Bitrep.B | 🟩 |
| Grub package | Trojan:Win32/Bitrep.B | 🟩 |
| IDUnlocker package | Trojan:Win32/Bitrep.B | 🟥 |
| MAF package | Trojan:Win32/Bitrep.B | 🟩 |
| Magix package | Trojan:Win32/Bitrep.B | 🟨 |
| MeldeMax package | Trojan:Win32/Bitrep.B | 🟩 |
| Merant package | Trojan:Win32/Bitrep.B | 🟨 |
| OOSoftware package | Trojan:Win32/Bitrep.B | 🟩 |
| OpenOffice package | Trojan:Win32/Bitrep.B | 🟩 |
| ShutdownManager package | Trojan:Win32/Bitrep.B | 🟨 |
| Syslog package | Trojan:Win32/Bitrep.B | 🟩 |
| SysReport package | Trojan:Win32/Bitrep.B | 🟩 |
| Tierpension package | Trojan:Win32/Bitrep.B | 🟨 |
| Tiscali package | Trojan:Win32/Bitrep.B | 🟩 |
| TKKG package | Trojan:Win32/Bitrep.B | 🟨 |
| Videowave package | Trojan:Win32/Bitrep.B | 🟩 |

| | | |
|---|---|---|
| Warner package package | Trojan:Win32/Bitrep.B | 🟩 |
| WinTBS package | Trojan:Win32/Bitrep.B | 🟩 |
| Youngzsoft package | Trojan:Win32/Vigorf.A | 🟩 |

Microsoft had 32 false alarms.

## McAfee

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| Abbyy package | JTI/Suspect.196665!fa788af98fe7 | 🟨 |
| Acer package | JTI/Suspect.196612!ef798271c092 | 🟧 |
| Asus package | JTI/Suspect.196612!603c617bdbe9 | 🟥 |
| Audacious package | JTI/Suspect.196612!f2be421f79f0 | 🟩 |
| Autodata package | JTI/Suspect.196612!e5d1dc02c85a | 🟨 |
| Bastian package | JTI/Suspect.196665!20801c0dd1e8 | 🟧 |
| ComfortUpdater package | JTI/Suspect.196612!b26126ae5c60 | 🟩 |
| ConnectionManager package | JTI/Suspect.196612!15becddd6d7b | 🟨 |
| CPserver package | GenericRXEU-UK!39EB5AE61795 | 🟧 |
| Databecker package | JTI/Suspect.196612!afa22c905e9d | 🟨 |
| Doppeldecker package | JTI/Suspect.196665!759d83a3dd67 | 🟨 |
| FileWorks package | JTI/Suspect.196612!3b0f5f8d1265 | 🟩 |
| GameSpy package | JTI/Suspect.196612!b8cfaec494db | 🟥 |
| Grub package | JTI/Suspect.196665!c4dcca9279b4 | 🟩 |
| HP package | JTI/Suspect.196612!ad29f0860a49 | 🟥 |
| IcyTower package | JTI/Suspect.196612!26cc6094a6bb | 🟥 |
| Lenovo package | JTI/Suspect.196612!2486b95c310c | 🟥 |
| Magix package | JTI/Suspect.196612!50abab1b2312 | 🟨 |
| MakeMulti package | JTI/Suspect.196665!2aef292f2c59 | 🟩 |
| Merant package | JTI/Suspect.196612!4a2541a02fc0 | 🟨 |
| Musikmaker package | JTI/Suspect.196612!d87fe5cef380 | 🟨 |
| NetClientManager package | JTI/Suspect.196612!26f3edfcbad0 | 🟩 |
| PackardBell package | JTI/Suspect.196612!1c84f9b992a4 | 🟧 |
| PEview package | JTI/Suspect.196612!c569075f3f94 | 🟨 |
| PowerDirector package | JTI/Suspect.196612!c331058776f4 | 🟨 |
| Quiz package | JTI/Suspect.196665!c64d4d966432 | 🟩 |
| Rainmeter package | JTI/Suspect.196612!7716a5b44ba9 | 🟨 |
| Restore package | JTI/Suspect.196612!31a1f20ae602 | 🟩 |
| Samsung package | JTI/Suspect.196612!1411bc7f6047 | 🟧 |
| SemSim package | JTI/Suspect.196612!4f49776bb467 | 🟨 |
| Skype package | GenericRXEL-QN!FA5555644483 | 🟧 |
| Tierpension package | JTI/Suspect.196612!31a3a19d8ee2 | 🟨 |
| TKKG package | JTI/Suspect.196612!80233c34803f | 🟨 |
| TotalRecorder package | JTI/Suspect.196612!97295fd52148 | 🟩 |
| WinWart package | JTI/Suspect.196612!b9820356dca7 | 🟩 |

McAfee had 35 false alarms.

## Quick Heal

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| Acer package | Suspicious | 🟨 |
| Aclive package | Trojan.ICGENERIC | 🟩 |
| AutoIt package | Trojan.ICGENERIC | 🟥 |
| CDDVDburner package | Trojan.Generic | 🟩 |
| Codeblocks package | Trojan.Scan | 🟥 |
| ComfortUpdater package | EE:Malwr.Heur.Ursu.220013 | 🟩 |
| Cresoeas package | Trojan.Fuery | 🟩 |
| DpWiper package | EE:Malwr.Heur.GZ.dmW | 🟩 |
| EasyExif package | Suspicious | 🟧 |
| EFcommander package | Suspicious | 🟩 |
| Elsword package | Trojanspy.Agent.19229 | 🟥 |
| FEAR package | Trojan.Azden | 🟩 |
| FileWorks package | Suspicious | 🟩 |
| Firefox package | Trojan.Ditertag | 🟧 |
| FreeRideGames package | Trojan.CGeneric | 🟥 |
| Gero package | Suspicious | 🟩 |
| Herold package | EE:Malwr.Heur.Ursu.147178 | 🟩 |
| IeTester package | EE:Malwr.Heur.Ursu.231296 | 🟩 |
| JewelQuest package | Suspicious | 🟥 |
| MediaServer package | Ransom.Ryzerlo.S4 | 🟨 |
| Merant package | Suspicious | 🟨 |
| MyPhoneExplorer package | EE:Malwr.Heur.Ursu.281421 | 🟨 |
| N64 package | Trojan.Fuerboos | 🟥 |
| NotepadPlus package | Trojan.UGeneric | 🟨 |
| PerfectMenu package | Trojan.Malagent.20271 | 🟩 |
| Performance package | Suspicious | 🟧 |
| Qualimail package | EE:Malware.Generic.SMH | 🟩 |
| SeekFreak package | Trojan.Azden | 🟩 |
| SpywareBlaster package | Trojan.VBCrypt.MF.7448 | 🟩 |
| StartOffice package | Trojan.GenericPMF.S2873074 | 🟥 |
| Tickmeter package | Suspicious | 🟩 |
| Tiscali package | Suspicious | 🟩 |
| ToolbarCop package | Trojan.VBCryptVMF.S2729126 | 🟨 |
| Wildtangent package | Trojan.IGENERIC | 🟥 |
| Yabe package | EE:Generic.MSIL.DownloaderB.420228B4 | 🟩 |

Quick Heal had 35 false alarms.

## Trend Micro

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| AddTime package | Suspicious | 🟩 |
| AntiDuplicate package | Suspicious | 🟩 |
| AVCutty package | Suspicious | 🟩 |
| AxBx package | Suspicious | 🟧 |

| | | |
|---|---|---|
| Bitdefender package | Suspicious | 🟩⬜⬜⬜⬜ |
| BMKbuddy package | Suspicious | 🟩⬜⬜⬜⬜ |
| ComfortUpdater package | Suspicious | 🟩⬜⬜⬜⬜ |
| ConnectionManager package | Suspicious | ⬜⬜🟨⬜⬜ |
| Databecker package | Suspicious | ⬜⬜🟨⬜⬜ |
| DropUpload package | Suspicious | 🟩⬜⬜⬜⬜ |
| DVDregion package | Suspicious | 🟩⬜⬜⬜⬜ |
| Easybuch package | Suspicious | 🟩⬜⬜⬜⬜ |
| EmailValidator package | Suspicious | 🟩⬜⬜⬜⬜ |
| Encryption package | Suspicious | ⬜⬜🟨⬜⬜ |
| FEAR package | Suspicious | 🟩⬜⬜⬜⬜ |
| Fractalus package | Suspicious | 🟩⬜⬜⬜⬜ |
| Gero package | Suspicious | 🟩⬜⬜⬜⬜ |
| GranParadiso package | Suspicious | ⬜🟩⬜⬜⬜ |
| Herold package | Suspicious | 🟩⬜⬜⬜⬜ |
| HotChime package | Suspicious | 🟩⬜⬜⬜⬜ |
| Jose package | Suspicious | ⬜🟩⬜⬜⬜ |
| Logik package | Suspicious | ⬜🟩⬜⬜⬜ |
| Macomfort package | Suspicious | ⬜🟩⬜⬜⬜ |
| MakeMulti package | Suspicious | ⬜🟩⬜⬜⬜ |
| Mingw package | Suspicious | 🟩⬜⬜⬜⬜ |
| NetClientManager package | Suspicious | 🟩⬜⬜⬜⬜ |
| OpenOffice package | Suspicious | ⬜🟩⬜⬜⬜ |
| Perfekt package | Suspicious | 🟩⬜⬜⬜⬜ |
| PowerVideo package | Suspicious | 🟩⬜⬜⬜⬜ |
| Quiz package | Suspicious | ⬜🟩⬜⬜⬜ |
| StartTime package | Suspicious | 🟩⬜⬜⬜⬜ |
| StartTime package | Suspicious | 🟩⬜⬜⬜⬜ |
| SubmitTwo package | Suspicious | 🟩⬜⬜⬜⬜ |
| Syslog package | Suspicious | 🟩⬜⬜⬜⬜ |
| TakeABreak package | Suspicious | 🟩⬜⬜⬜⬜ |
| TextScan package | Suspicious | 🟩⬜⬜⬜⬜ |
| Tickmeter package | Suspicious | 🟩⬜⬜⬜⬜ |
| Videowave package | Suspicious | 🟩⬜⬜⬜⬜ |
| WinTBS package | Suspicious | 🟩⬜⬜⬜⬜ |
| Zdataburn package | Suspicious | 🟩⬜⬜⬜⬜ |

Trend Micro had 40 false alarms.

## Symantec Norton

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| AddTime package | Heur.AdvML.C | ⬜🟩⬜⬜⬜ |
| AntiDuplicate package | Heur.AdvML.C | ⬜🟩⬜⬜⬜ |
| AnVir package | Trojan.Gen.2 | ⬜🟩⬜⬜⬜ |
| Avira package | Trojan Horse | ⬜🟩⬜⬜⬜ |
| Bastian package | Heur.AdvML.C | ⬜⬜⬜🟥⬜ |
| ComfortUpdater package | Heur.AdvML.C | 🟩⬜⬜⬜⬜ |
| Dexpot package | Heur.AdvML.C | ⬜🟩⬜⬜⬜ |

| | | |
|---|---|---|
| DivX package | Backdoor.Graybird | 🟥 |
| DVDregion package | Suspicious.Epi.3 | 🟩 |
| Easybuch package | Suspicious.Epi.3 | 🟩 |
| Encryption package | Heur.AdvML.A | 🟨 |
| FEAR package | Suspicious.Epi.3 | 🟩 |
| FileWorks package | Trojan.Gen.2 | 🟩 |
| FileZilla package | Suspicious.Epi.3 | 🟩 |
| FineReader package | Suspicious.Epi.3 | 🟥 |
| Forte package | Trojan.Gen.2 | 🟨 |
| iNetTimer package | Suspicious.Epi.3 | 🟩 |
| Jose package | Trojan.Gen.9 | 🟩 |
| Logik package | Suspicious.Epi.3 | 🟩 |
| Macomfort package | Download Insight | 🟩 |
| MagicSkin package | Heur.AdvML.B | 🟨 |
| MaxPasswords package | Heur.AdvML.C | 🟩 |
| Mediacoder package | Suspicious.Epi.3 | 🟨 |
| MODupRemover package | Trojan.Gen.9 | 🟩 |
| NetClientManager package | Heur.AdvML.C | 🟩 |
| OOSoftware package | Heur.AdvML.B | 🟩 |
| PaperOffice package | Heur.AdvML.C | 🟩 |
| PEbuilder package | Suspicious.Epi.3 | 🟩 |
| Perfekt package | Suspicious.Epi.3 | 🟩 |
| PowerVideo package | Suspicious.Epi.3 | 🟩 |
| Quiz package | Heur.AdvML.C | 🟩 |
| RegDefrag package | Download Insight | 🟩 |
| Spryzip package | Trojan.Gen.2 | 🟩 |
| StartTime package | Suspicious.Epi.3 | 🟩 |
| Stormcloud package | Suspicious.Epi.3 | 🟩 |
| SubmitTwo package | Download Insight | 🟩 |
| Syslog package | Heur.AdvML.B | 🟩 |
| SysReport package | Trojan.Gen.6 | 🟩 |
| TakeABreak package | Download Insight | 🟩 |
| TextScan package | Heur.AdvML.C | 🟩 |
| TKKG package | Download Insight | 🟨 |
| TrueCafe package | Download Insight | 🟨 |
| UpdateHelper package | Trojan Horse | 🟨 |
| Webcam package | Heur.AdvML.C | 🟨 |
| WinAmp package | Heur.AdvML.B | 🟨 |
| XTreme package | Heur.AdvML.C | 🟨 |
| Zoner package | Trojan.Dropper | 🟩 |

Symantec Norton had 47 false alarms.

## K7

| False alarm found in some parts of | Detected as | Supposed prevalence |
|---|---|---|
| 3DMark package | Trojan ( 0046628d1 ) | 🟧 |
| 3DTTT package | NetWorm ( 700000151 ) | 🟩 |
| Abbrevation package | Riskware ( 0040eff71 ) | 🟩 |
| AddTime package | Trojan ( 0001140e1 ) | 🟩 |
| Adobe package | Backdoor ( 004a942a1 ) | 🟥 |
| Alzip package | Riskware ( 0040eff71 ) | 🟧 |
| AntiCheat package | Riskware ( 0040eff71 ) | 🟥 |
| Avanquest package | Trojan ( 004ce0ea1 ) | 🟧 |
| AVCutty package | Riskware ( 0040eff71 ) | 🟩 |
| Bigiba package | Trojan ( 004ffa261 ) | 🟨 |
| Bitdefender package | Trojan ( 7000000f1 ) | 🟩 |
| BlueTooth package | Trojan ( 001a5abb1 ) | 🟥 |
| Borland package | Trojan ( 7000000f1 ) | 🟧 |
| Camou package | Trojan-Downloader ( 004f2a781 ) | 🟨 |
| CDDVDburning package | Trojan ( 005257651 ) | 🟩 |
| CSE package | Riskware ( 0040eff71 ) | 🟩 |
| Delphi package | Trojan ( 7000000f1 | 🟨 |
| Deskhedron package | Riskware ( 0040eff71 ) | 🟧 |
| Dino package | Riskware ( 0040eff71 ) | 🟩 |
| EM package | Riskware ( 0040eff71 ) | 🟩 |
| Emco package | Trojan ( 7000000f1 ) | 🟨 |
| F1 package | Riskware ( 0040eff71 ) | 🟩 |
| Global package | Trojan ( 004906d41 ) | 🟥 |
| GranParadiso package | Riskware ( 0040eff71 ) | 🟩 |
| GXTranscoder package | Riskware ( 0040eff71 ) | 🟩 |
| HDDLife package | Riskware ( 0040eff71 ) | 🟩 |
| HP package | Riskware ( 0040eff71 ) | 🟨 |
| HTML package | Riskware ( 0040eff71 | 🟩 |
| IcyTower package | Riskware ( 0040eff71 ) | 🟥 |
| iDump package | Riskware ( 00000a851 ) | 🟧 |
| IuWork package | Trojan ( 004d22751 ) | 🟧 |
| Lenovo package | Riskware ( f15000051 ) | 🟨 |
| Lezioni package | Riskware ( 0040eff71 ) | 🟩 |
| Logger package | Virus ( 7000000b1 ) | 🟨 |
| Macomfort package | Riskware ( 0040eff71 ) | 🟩 |
| Macromedia package | Trojan-Downloader ( 0017bc961 ) | 🟩 |
| MakeInstantPlayer package | Trojan ( 004d394f1 ) | 🟩 |
| MakeMulti package | Trojan ( 004de92c1 | 🟩 |
| Mixxx package | Riskware ( 0040eff71 ) | 🟧 |
| MouseOMeter package | Riskware ( f15000051 ) | 🟩 |
| MultiBrowser package | Riskware ( 0040eff71 ) | 🟩 |
| Need4Speed package | Trojan ( 0047648f1 ) | 🟥 |
| Opanda package | Riskware ( 0040eff71 ) | 🟧 |
| OpenOffice package | Trojan ( 003b1b581 ) | 🟩 |
| PCWizard package | Trojan ( 003cca981 ) | 🟨 |
| PEiD package | Riskware ( 0040eff71 ) | 🟧 |
| PhotoUpz package | Trojan ( 0053b4521 ) | 🟩 |

| | | |
|---|---|---|
| PPMate package | Trojan ( 0053b4521 ) | 🟥 |
| Qlogix package | Riskware ( 0040eff71 ) | 🟩 |
| StationRipper package | Riskware ( 0040eff71 ) | 🟩 |
| Tiscali package | Riskware ( 0040eff71 ) | 🟩 |
| TrueCafe package | Trojan ( 7000000f1 ) | 🟨 |
| UBCD package | Riskware ( 0040eff71 ) | 🟥 |
| Vistart package | Trojan ( 003d23081 ) | 🟥 |
| Wavosaur package | Riskware ( 0040eff71 ) | 🟥 |
| WB package | Trojan ( 004bc6de1 ) | 🟨 |
| Weather package | Riskware ( 0040eff71 ) | 🟩 |
| WinAmp package | Riskware ( 0040eff71 ) | 🟩 |
| WinRAR package | Riskware ( 0040eff71 ) | 🟨 |

K7 had 59 false alarms.

## Copyright and Disclaimer

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 (October 2018)