# Anti-Virus Comparative
# No. 21, February 2009


## Detección bajo demanda de programas maliciosos

incluye prueba de detección de falsos positivos y de velocidad de exploración bajo demanda

Idioma: español
Febrero de 2009
Última revisión: 2009-03-21

**www.av-comparatives.org**

# Contenidos

# Productos evaluados

- avast! Professional Edition 4.8
- AVG Anti-Virus 8.0
- AVIRA AntiVir Premium 8.2
- BitDefender Anti-Virus 2009
- Command Anti-Malware 5.0.8
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 3.0
- F-Secure Anti-Virus 2009
- G DATA AntiVirus 2009
- Kaspersky Anti-Virus 2009
- Kingsoft AntiVirus 2009
- McAfee VirusScan Plus 2009
- Microsoft Live OneCare 2.5
- Norman Antivirus & Anti-Spyware 7.10
- Sophos Anti-Virus 7.6.4
- Symantec Norton Anti-Virus 2009
- Trustport Antivirus 2.8

## Condiciones para la participación y metodología de evaluación

Las condiciones para la participación en nuestras evaluaciones se indican en la lista del documento sobre metodología disponible en http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf. Antes de proceder con este informe, se aconseja a los lectores la lectura del documento mencionado arriba. Los productos incluidos en nuestras pruebas ya son considerados muy buenos productos antivirus con tasas de detección bajo demanda relativamente elevadas, ya que éste es uno de los requisitos indispensables para poder participar. La participación se encuentra limitada a entre 16 y 18 productos antivirus de alta calidad, reconocidos y usados a nivel mundial, cuyos fabricantes accedieron a que sean evaluados e incluidos en este informe público. En esta prueba comparativa sólo se han incluido los fabricantes que detectaron más del 97% del Grupo de Prueba A (desde abril de 2006 hasta abril de 2008). Los nuevos participantes en condiciones para participar son Authentium y Kingsoft.

## Versiones de los productos evaluados

Los grupos de prueba de malware y los sistemas usados como bancos de prueba se congelaron a comienzos de febrero de 2009. Todos los productos fueron actualizados el 9 de febrero de 2009. En esta prueba pública se incluyeron los siguientes 17 productos:

- avast! Professional Edition 4.8.1335
- AVG Anti-Virus 8.0.234
- AVIRA AntiVir Premium 8.2.0.374
- BitDefender Anti-Virus 12.0.11.4
- Command Anti-Malware 5.0.8
- eScan Anti-Virus 10.0.946.341
- ESET NOD32 Antivirus 3.0.684.0
- F-Secure Anti-Virus 9.00.149
- G DATA AntiVirus 19.1.0.0
- Kaspersky Anti-Virus 8.0.0.506a
- Kingsoft AntiVirus 2008.11.6.63
- McAfee VirusScan Plus 13.3.117
- Microsoft Live OneCare 2.5.2900.20
- Norman Antivirus & Anti-Spyware 7.10.02
- Sophos Anti-Virus 7.6.4
- Symantec Norton Anti-Virus 16.2.0.7
- Trustport Antivirus 2.8.0.3011

Ciertos productos pueden ofrecer opciones/configuraciones adicionales, por ejemplo, para proveer protección adicional contra malware durante su ejecución (si no es detectado con antelación por la exploración en el acceso o bajo demanda).

Por favor, pruébelos en su propio sistema antes de tomar una decisión sobre la adquisición de un producto determinado basándose en estas pruebas. Los programas también cuentan con muchas otras características y existen otros factores importantes para tener en cuenta (como el precio, la facilidad de uso/administración, la compatibilidad, la interfaz gráfica de usuario, el idioma, la frecuencia de las actualizaciones, las funciones de sistemas de prevención de intrusiones (HIPS) o bloqueadores de comportamiento, etc.). A pesar de ser extremadamente importante, la tasa de detección de un producto sólo conforma uno de los aspectos del producto antivirus completo. Este año, AV-Comparatives también ofrecerá el informe de una prueba dinámica del producto completo (proactivo y normal), así como otros informes de evaluaciones que abarcan distintos aspectos/características de los productos.

## Comentarios

Como hoy en día, en la vida real, prácticamente todos los productos se ejecutan en forma predeterminada con las opciones de configuración en la máxima protección, o se cambian en forma automática a la mayor protección cuando se detecta una infección, hemos evaluado todos los productos en su configuración más alta (excepto Sophos). A continuación se encuentran algunas notas sobre las configuraciones usadas (la exploración de todos los archivos, etc., está siempre habilitada) y sobre algunas tecnologías que requieren explicación:

**avast:** en forma predeterminada se ejecuta automáticamente con la máxima configuración (en caso de una infección).

**AVG:** se ejecuta con la máxima configuración en forma predeterminada.

**AVIRA:** usa en forma predeterminada una heurística media sin habilitar todas las categorías adicionales. AVIRA ya ha solicitado el año pasado que se evaluara su producto con todas las categorías adicionales habilitadas y con el nivel máximo de heurística. Por ese motivo, les recomendamos a los usuarios que también configuren la heurística en su mayor nivel.

**BitDefender:** se ejecuta con la máxima configuración en forma predeterminada.

**Command:** se ejecuta con la heurística en su configuración alta en forma predeterminada (que también concuerda con la configuración máxima recomendada por Authentium). Además, Command cuenta con un modo de heurística en nivel máximo, pero no se recomienda habilitarlo (debido a la excesiva cantidad de falsos positivos que genera).

**eScan:** se ejecuta con la máxima configuración en forma predeterminada.

**ESET:** se ejecuta con la máxima configuración (webfilter) en forma predeterminada.

**F-Secure:** se ejecuta con la máxima configuración de exploración bajo demanda en forma predeterminada.

**G DATA:** se ejecuta con la máxima configuración en forma predeterminada (dependiendo del hardware).

**Kaspersky**: se ejecuta con una configuración heurística baja en forma predeterminada. Kaspersky ya ha solicitado el año pasado que evaluáramos su producto con la configuración heurística en su máximo nivel. Por ese motivo, les recomendamos a los usuarios que también configuren la heurística en el nivel alto.

**Kingsoft:** se ejecuta con la máxima configuración en forma predeterminada.

**McAfee:** En el producto de McAfee para el consumidor, la tecnología Artemis se llama Active Protection y se habilita en forma predeterminada sólo cuando está disponible una

conexión a Internet. Internet es el vector de infección más predominante, por lo que los resultados de las pruebas en las que existe una conexión a Internet representan las capacidades de detectar códigos maliciosos entrantes en forma más realista. Artemis fue evaluado al mismo tiempo de la actualización de los otros productos, por lo que no contó con una ventaja temporal sobre otros productos. La tecnología Artemis envía breves huellas de los archivos sospechosos sin ninguna información de identificación personal. En la actualidad, Artemis provee una protección casi instantánea además de las actualizaciones de archivos DAT de McAfee para los malware más predominantes. McAfee actualiza la forma en que Artemis detecta los malware por medio de sus firmas en archivos DAT.

**Microsoft:** se ejecuta con la máxima configuración en forma predeterminada.

**Norman:** se ejecuta con la máxima configuración en forma predeterminada.

**Sophos:** se ejecuta sin la detección de archivos sospechosos en forma predeterminada. Sophos (un producto corporativo) ya ha solicitado hace varios meses que este año se lo evalúe y se le otorgue la mención según su configuración predeterminada. Por motivos informativos, también incluimos los resultados de las pruebas en su configuración máxima (la detección de archivos sospechosos habilitada, etc.).

**Symantec:** se ejecuta con la heurística automática en forma predeterminada. Symantec ya ha solicitado el año pasado que se evaluara su producto con la heurística en su configuración avanzada, aunque casi no presentaba diferencia alguna. De todas formas, les recomendamos a los usuarios que también configuren la heurística en su nivel avanzado.

**TrustPort:** ya ha solicitado el año pasado que se evaluara su producto con la máxima configuración y sus dos motores habilitados (AVG y Norman), como ocurre mientras efectúa exploraciones en segundo plano (en el acceso).

## Resultados de las pruebas

En esta prueba hemos sido mucho más selectivos que en las pruebas anteriores – sólo los fabricantes cuyos productos detectaron más del 97% del Grupo de Prueba A (desde abril de 2006 hasta abril de 2008) han sido incluidos en esta evaluación comparativa.

Ahora es más difícil alcanzar menciones altas, ya que las menciones se basan únicamente en las tasas de detección del Grupo de Prueba B, que contiene malware de los últimos nueve meses (desde mayo de 2008 hasta comienzos de febrero de 2009). En este caso, las tasas de detección (porcentajes) pueden parecer menores que en las evaluaciones anteriores, donde contamos el puntaje alcanzado general basándonos tanto en el Grupo A como en el B (cuando el Grupo A queda bien cubierto por casi todos los fabricantes). Además, desde esta prueba en adelante, los falsos positivos detectados bajan el nivel de la mención. Que la Mención sea más baja no significa que el producto haya empeorado – de hecho, todos los productos han mejorado mucho: por ejemplo, en esta prueba Kingsoft obtiene 85% (basado sólo en el GRUPO B). Si hubiéramos contado igual que en años anteriores (GRUPO A + GRUPO B), Kingsoft habría obtenido alrededor de 92%.

### Tablas de resultados

| *Empresa* | | AVIRA | | Alwil Software | | AVG Technologies | | BitDefender | |
|---|---|---|---|---|---|---|---|---|---|
| *Producto* | | **AntiVir Premium** | | **avast! Professional** | | **AVG Anti-Virus** | | **BitDefender AV** | |
| *Versión del programa* | | 8.2.0.374 | | 4.8.1335 | | 8.0.234 | | 12.0.11.4 | |
| *Motor/versión de firmas* | | 8.02.00.76/7.01.01.248 | | 090209-0 | | 270.10.19/1941 | | *no disponible* | |
| **Mención alcanzada en la prueba** | | **ADVANCED** | | **ADVANCED** | | **STANDARD** | | **ADVANCED** | |
| **Cantidad de falsos positivos*** | | muchos | | muchos | | muchos | | muchos | |
| Velocidad de exploración bajo demanda* | | promedio | | rápida | | lenta | | lenta | |
| **TASAS DE DETECCIÓN:** | | | | | | | | | |
| **GRUPO A (abr '06 - abr '08)** | | APROBÓ | | APROBÓ | | APROBÓ | | APROBÓ | |
| **GRUPO B (may '08- ene '09):** | | | | | | | | | |
| Virus de Windows | 24.476 | 24.459 | 99,9% | 24.346 | 99,5% | 23.831 | 97,4% | 24.403 | 99,7% |
| Virus macro | 2.492 | 2.480 | 99,5% | 2.478 | 99,4% | 2.278 | 91,4% | 2.427 | 97,4% |
| Malware de script | 8.811 | 8.717 | 98,9% | 8.495 | 96,4% | 3.740 | 42,4% | 7.445 | 84,5% |
| Gusanos | 53.326 | 53.202 | 99,8% | 52.655 | 98,7% | 50.962 | 95,6% | 52.460 | 98,4% |
| Programas de puerta trasera/Bots | 253.892 | 253.232 | 99,7% | 249.199 | 98,2% | 244.363 | 96,2% | 250.134 | 98,5% |
| Troyanos | 912.104 | 908.950 | 99,7% | 896.338 | 98,3% | 845.088 | 92,7% | 893.896 | 98,0% |
| Otros malware | 19.827 | 19.645 | 99,1% | 18.599 | 93,8% | 15.838 | 79,9% | 18.772 | 94,7% |
| TOTAL | **1.274.928** | 1.270.685 | **99,7%** | 1.252.110 | **98,2%** | 1.186.100 | **93,0%** | 1.249.537 | **98,0%** |

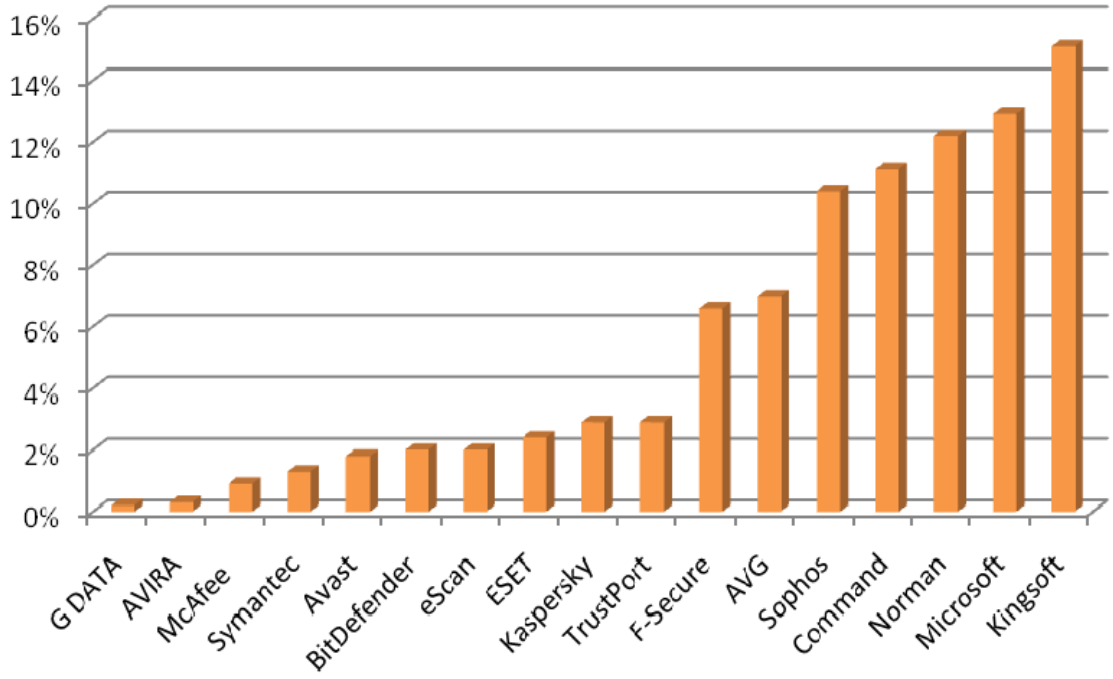
| *Empresa* | | Authentium | | MicroWorld | | F-Secure | | G DATA Security | |
|---|---|---|---|---|---|---|---|---|---|
| *Producto* | | **Command AM** | | **eScan ISS** | | **F-Secure Anti-Virus** | | **G DATA AntiVirus** | |
| *Versión del programa* | | 5.0.8 | | 10.0.946.341 | | 9.00.149 | | 19.1.0.0 | |
| *Motor/versión de firmas* | | *20090209* | | *no disponible* | | 8.10.14240 | | 19.3715 / 19.219 | |
| **Mención alcanzada en la prueba** | | **TESTED** | | **ADVANCED** | | **ADVANCED** | | **ADVANCED** | |
| **Cantidad de falsos positivos*** | | muchos | | muchos | | pocos | | muchos | |
| Velocidad de exploración bajo demanda* | | promedio | | lenta | | lenta | | promedio | |
| **TASAS DE DETECCIÓN:** | | | | | | | | | |
| **GRUPO A (abr '06 - abr '08)** | *1.820.238* | APROBÓ | | APROBÓ | | APROBÓ | | APROBÓ | |
| **GRUPO B (may '08- ene '09):** | | | | | | | | | |
| Virus de Windows | 24.476 | 21.309 | 87,1% | 24.365 | 99,5% | 23.906 | 97,7% | 24.469 | ~100% |
| Virus macro | 2.492 | 2.485 | 99,7% | 2.438 | 97,8% | 2.470 | 99,1% | 2.492 | 100% |
| Malware de script | 8.811 | 6.248 | 70,9% | 7.444 | 84,5% | 8.293 | 94,1% | 8.668 | 98,4% |
| Gusanos | 53.326 | 42.380 | 79,5% | 52.458 | 98,4% | 50.560 | 94,8% | 53.273 | 99,9% |
| Programas de puerta trasera/Bots | 253.892 | 231.252 | 91,1% | 250.125 | 98,5% | 239.171 | 94,2% | 253.492 | 99,8% |
| Troyanos | 912.104 | 816.239 | 89,5% | 893.927 | 98,0% | 847.458 | 92,9% | 910.211 | 99,8% |
| Otros malware | 19.827 | 13.118 | 66,2% | 18.770 | 94,7% | 18.922 | 95,4% | 19.667 | 99,2% |
| TOTAL | **1.274.928** | 1.133.031 | **88,9%** | 1.249.527 | **98,0%** | 1.190.780 | **93,4%** | 1.272.272 | **99,8%** |

| *Empresa* | | Kaspersky Labs | | Kingsoft | | McAfee | | Microsoft | |
|---|---|---|---|---|---|---|---|---|---|
| *Producto* | | **Kaspersky AV** | | **Kingsoft AntiVirus** | | **McAfee VirusScan+** | | **Microsoft OneCare** | |
| *Versión del programa* | | 8.0.0.506a | | 2008.11.6.63 | | 13.3.117 | | 2.5.2900.20 | |
| *Motor/versión de firmas* | | *no disponible* | | *2009.2.8.1* | | 5300.2777 / 5521 | | 1.51.391.0 | |
| **Mención alcanzada en la prueba** | | **ADVANCED+** | | **TESTED** | | **ADVANCED+** | | **STANDARD** | |
| **Cantidad de falsos positivos*** | | pocos | | muchos | | pocos | | muy pocos | |
| Velocidad de exploración bajo demanda* | | promedio | | rápida | | promedio | | promedio | |
| **TASAS DE DETECCIÓN:** | | | | | | | | | |
| **GRUPO A (abr '06 - abr '08)** | *1.820.238* | APROBÓ | | APROBÓ | | APROBÓ | | APROBÓ | |
| **GRUPO B (may '08- ene '09):** | | | | | | | | | |
| Virus de Windows | 24.476 | 24.297 | 99,3% | 22.096 | 90,3% | 24.425 | 99,8% | 23.400 | 95,6% |
| Virus macro | 2.492 | 2.470 | 99,1% | 1.204 | 48,3% | 2.492 | 100% | 2.190 | 87,9% |
| Malware de script | 8.811 | 8.362 | 94,9% | 4.010 | 45,5% | 6.673 | 75,7% | 6.312 | 71,6% |
| Gusanos | 53.326 | 52.295 | 98,1% | 45.867 | 86,0% | 52.909 | 99,2% | 46.529 | 87,3% |
| Programas de puerta trasera/Bots | 253.892 | 247.054 | 97,3% | 223.022 | 87,8% | 252.692 | 99,5% | 213.611 | 84,1% |
| Troyanos | 912.104 | 884.422 | 97,0% | 774.888 | 85,0% | 906.128 | 99,3% | 803.069 | 88,0% |
| Otros malware | 19.827 | 19.160 | 96,6% | 11.569 | 58,3% | 17.889 | 90,2% | 15.385 | 77,6% |
| TOTAL | **1.274.928** | 1.238.060 | **97,1%** | 1.082.656 | **84,9%** | 1.263.208 | **99,1%** | 1.110.496 | **87,1%** |

| *Empresa* | | ESET | | Norman ASA | | Symantec | | Sophos | |
|---|---|---|---|---|---|---|---|---|---|
| *Producto* | | **NOD32 Antivirus** | | **Norman AV+AS** | | **Norton Anti-Virus** | | **Sophos Anti-Virus** | |
| *Versión del programa* | | 3.0.684.0 | | 7.10.02 | | 16.2.0.7 | | 7.6.4 | |
| *Motor/versión de firmas* | | 3839.1180 | | 6.00.06 | | 110208v / 91468 | | 2.83.3 / 4.38E+180 | |
| **Mención alcanzada en la prueba** | | **ADVANCED+** | | **TESTED** | | **ADVANCED+** | | **STANDARD** | |
| **Cantidad de falsos positivos*** | | pocos | | muchos | | pocos | | pocos | |
| Velocidad de exploración bajo demanda* | | promedio | | lenta | | rápida | | promedio | |
| **TASAS DE DETECCIÓN:** | | | | | | | | | |
| **GRUPO A (abr '06 - abr '08)** | *1.820.238* | APROBÓ | | APROBÓ | | APROBÓ | | APROBÓ | |
| **GRUPO B (may '08- ene '09):** | | | | | | | | | |
| Virus de Windows | 24.476 | 24.039 | 98,2% | 22052 | 90,1% | 24.427 | 99,8% | 24.465 | ~100% |
| Virus macro | 2.492 | 2.492 | 100% | 2434 | 97,7% | 2.492 | 100% | 2.308 | 92,6% |
| Malware de script | 8.811 | 8.505 | 96,5% | 3962 | 45,0% | 7.549 | 85,7% | 8.517 | 96,7% |
| Gusanos | 53.326 | 51.794 | 97,1% | 46861 | 87,9% | 52.699 | 98,8% | 46.757 | 87,7% |
| Programas de puerta trasera/Bots | 253.892 | 249.399 | 98,2% | 224683 | 88,5% | 251.575 | 99,1% | 226.595 | 89,2% |
| Troyanos | 912.104 | 890.002 | 97,6% | 806290 | 88,4% | 900.425 | 98,7% | 819.102 | 89,8% |
| Otros malware | 19.827 | 18.523 | 93,4% | 13187 | 66,5% | 19.282 | 97,3% | 14.963 | 75,5% |
| TOTAL | **1.274.928** | 1.244.754 | **97,6%** | 1.119.469 | **87,8%** | 1.258.449 | **98,7%** | 1.142.707 | **89,6%** |

| *Empresa* | | Trustport |
|---|---|---|
| *Producto* | | **TrustPort AV** |
| *Versión del programa* | | 2.8.0.3011 |
| *Motor/versión de firmas* | | *no disponible* |
| **Mención alcanzada en la prueba** | | **ADVANCED** |
| **Cantidad de falsos positivos*** | | muchos |
| Velocidad de exploración bajo demanda* | | lenta |
| **TASAS DE DETECCIÓN:** | | |
| **GRUPO A (abr '06 - abr '08)** | *1.820.238* | APROBÓ |
| **GRUPO B (may '08- ene '09):** | | |
| Virus de Windows | 24.476 | 24.305 99,3% |
| Virus macro | 2.492 | 2.461 98,8% |
| Malware de script | 8.811 | 5.319 60,4% |
| Gusanos | 53.326 | 52.467 98,4% |
| Programas de puerta trasera/Bots | 253.892 | 251.163 98,9% |
| Troyanos | 912.104 | 884.630 97,0% |
| Otros malware | 19.827 | 17.359 87,6% |
| TOTAL | **1.274.928** | 1.237.704 **97,1%** |

## Gráfico de muestras no detectadas (cuanto más bajo, mejor)




*Por favor, no deje de leer la segunda parte de este informe (que se publicará dentro de algunos meses), donde se incluirá la prueba retrospectiva, que evalúa si los productos antivirus están detectando en forma correcta los malware nuevos/desconocidos. Con frecuencia durante este año, seguiremos publicando en nuestro sitio Web los informes de evaluaciones posteriores que abarquen otros aspectos de los distintos productos.*

*Los resultados de nuestras pruebas de exploración bajo demanda en líneas generales también son aplicables para la exploración en el acceso (si se usa la misma configuración), pero no para las tecnologías de protección que actúan durante la ejecución (como los* sistemas de prevención de intrusiones *[HIPS], bloqueadores de comportamiento, etc.).*

*Una buena tasa de detección sigue siendo una de las características de mayor importancia, determinación y confiabilidad de un programa antivirus. Además, la mayoría de los productos ya proveen al menos algún tipo de* sistema de prevención de intrusiones *(HIPS) – basándose en el comportamiento u otras funciones para bloquear (o al menos advertir sobre la posibilidad de existencia) de acciones maliciosas, por ejemplo, durante la ejecución del malware, cuando todos los demás mecanismos de detección/protección en el acceso y bajo demanda han fallado. Evaluaremos estos tipos de características especiales de protección en el transcurso de este año.*

*Aunque realicemos diversas pruebas y mostremos distintos aspectos de los programas antivirus, se recomienda a los usuarios evaluar los programas por sí mismos para formarse una opinión personal sobre ellos. Los datos de las pruebas o las reseñas sólo sirven de guía para ciertos aspectos que los usuarios no pueden evaluar por sus medios. Les sugerimos a los lectores que también investiguen otros resultados de pruebas independientes llevadas a cabo por distintas organizaciones evaluadoras independientes, para obtener una mejor visión general sobre las capacidades de detección y protección de los diversos productos en distintos escenarios de prueba y con diversos grupos de prueba.*

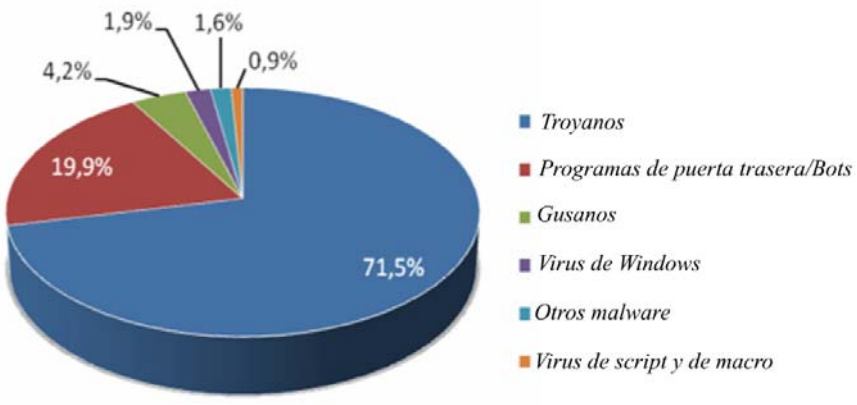
## Reseña de los resultados

El grupo de prueba se dividió en dos partes. Los porcentajes mostrados abajo corresponden al GRUPO B, que sólo incluye malware de los últimos 9 meses. En consecuencia, los porcentajes van a ser menores que en las evaluaciones anteriores. El GRUPO A queda cubierto muy bien (>97%) por todos los productos evaluados e incluye malware desde abril de 2006 hasta abril de 2008. ¡Recomendamos también tener en consideración las tasas de detección de falsos positivos (que figuran en la próxima página) cuando analice las tasas de detección provistas a continuación!

**Tasas de detección totales[1]:**

| | | |
|---|---|---|
| 1. | G DATA | 99.8% |
| 2. | AVIRA | 99.7% |
| 3. | McAfee[2] | 99.1% |
| 4. | Symantec | 98.7% |
| 5. | Avast | 98.2% |
| 6. | BitDefender, eScan | 98.0% |
| 7. | ESET | 97.6% |
| 8. | Kaspersky, TrustPort | 97.1% |
| 9. | F-Secure | 93.4% |
| 10. | AVG | 93.0% |
| 11. | Sophos | 89.6% |
| 12. | Command | 88.9% |
| 13. | Norman | 87.8% |
| 14. | Microsoft | 87.1% |
| 15. | Kingsoft | 84.9% |

El GRUPO B contiene cerca de 1.3 millones de muestras de malware. El grupo de prueba utilizado está formado por:




[1] Estimamos que el margen de error restante correspondiente a estas tasas de detección es de 0,4%.
[2] McAfee VirusScan Plus 13.3 viene con la tecnología Artemis en tiempo real "in-the-cloud" habilitada en forma predeterminada. Para ciertos usuarios puede ser importante saber cuál es la base mínima de detección de McAfee, en caso de que la conexión a Internet no esté disponible. Por esa razón también hemos medido la tasa de detección de McAfee sin conexión a Internet. **La tasa de detección de McAfee sin conexión a Internet fue del 95.2%.**

# Prueba de falsos positivos

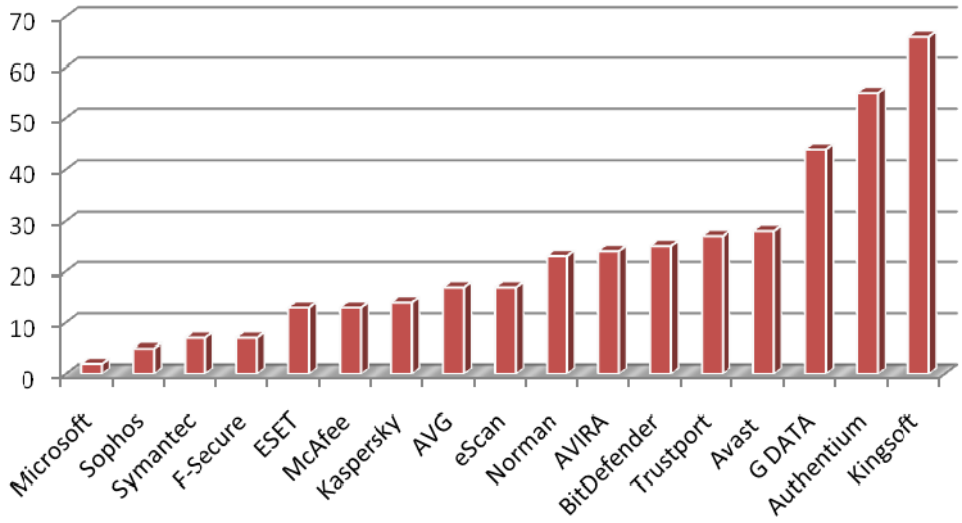
Para evaluar mejor la calidad de las capacidades de detección de productos antivirus, también ofrecemos una prueba de falsos positivos. Los falsos positivos pueden causar tantos problemas como una infección real. Por favor, tenga en cuenta la tasa de falsos positivos cuando evalúe las tasas de detección, ya que un producto que tiende a generar falsos positivos logra más fácilmente puntajes altos de detección.

## Resultados de falsos positivos detectados

Cantidad de falsos positivos encontrados en nuestro grupo de muestras limpio (cuanto más bajo, mejor):

| | | | |
|---|---|---|---|
| 1. | Microsoft | 2 | muy pocos falsos positivos |
| 2. | Sophos | 5 | |
| 3. | Symantec, F-Secure | 7 | pocos falsos positivos |
| 4. | ESET, McAfee | 13 | |
| 5. | Kaspersky | 14 | |
| 6. | AVG, eScan | 17 | |
| 7. | Norman | 23 | |
| 8. | AVIRA | 24 | |
| 9. | BitDefender | 25 | |
| 10. | Trustport | 27 | muchos falsos positivos |
| 11. | Avast | 28 | |
| 12. | G DATA | 44 | |
| 13. | Authentium | 55 | |
| 14. | Kingsoft | 66 | |

El gráfico que aparece a continuación muestra la cantidad de falsos positivos detectados en nuestro grupo de archivos limpios por los productos antivirus evaluados.



## Detalles sobre los falsos positivos detectados

En la evaluación de programas antivirus es importante medir no sólo las capacidades de detección sino también la confiabilidad – uno de cuyos aspectos es, por cierto, la tendencia del producto a identificar archivos limpios como si estuvieran infectados. Ningún producto es inmune a la detección de falsos positivos, pero existen diferencias entre ellos y el objetivo es medirlas. Nadie tiene todos los archivos legítimos existentes y en consecuencia no es posible efectuar una prueba de falsos positivos "definitiva". Lo que sí es posible y razonable es crear y usar un grupo de archivos limpios que sea independiente. Si en ese grupo un producto generó, por ejemplo, 100 falsos positivos y otro sólo 50, es probable que el primero sea más propenso a detectar falsos positivos que el segundo. Esto no significa que el producto que detectó 50 no detecte más de 50 en la realidad, pero aún así, el número relativo obtenido es importante.

Todos los falsos positivos que aparecen en la lista fueron informados y enviados a los fabricantes de los productos antivirus para su verificación y ya se han arreglado. No se tuvieron en cuenta los falsos positivos provocados por datos no codificados en archivos del programa antivirus. Si un producto generó varios falsos positivos sobre el mismo paquete, aquí se cuenta como si fuera uno solo (es por eso que denominamos todo el software en general como paquete: "package"). Los cracks, keygens, etc., u otras aplicaciones y herramientas cuestionables, así como los falsos positivos distribuidos por fabricantes u otras fuentes no independientes no se cuentan aquí como falsos positivos. A continuación se encuentran los falsos positivos que hemos observado en nuestro grupo independiente de archivos limpios. En el futuro, presentaremos esta lista como un documento separado y no la incluiremos en el informe de la evaluación.

### Microsoft

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| BackProtection package | Trojan:Win32/Vhorse.EY |
| InkScapePortable package | VirTool:Win32/Obfuscator.C |

Microsoft OneCare tuvo 2 falsos positivos.

### Sophos

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| eScan package | Istbar |
| PhotoMatix package | Mal/Generic-A |
| RegistryHealer package | Mal/HckPk-A |
| SpyCop package | Mal/VB-A |
| TorChat package | Mal/HckPk-E |

Sophos tuvo 5 falsos positivos en la configuración predeterminada. Con la opción para detección de archivos sospechosos habilitada, generó 68 falsos positivos; alrededor de 20.000 muestras de malware adicionales serían detectadas con la opción para detección de archivos sospechosos habilitada. Como Sophos es un producto para usuarios corporativos, donde las computadoras son administradas por un administrador, los falsos positivos descubiertos no se consideran un problema. Estos archivos son técnicamente falsos positivos, pero es probable que los administradores deseen enterarse de la existencia de dichas aplicaciones.

## Symantec

| Falsos positivos encontrados en algunas partes de | Detected as |
|---|---|
| 0190warner package | Suspicious.MH690 |
| Burn4Free package | SecurityRisk.NavHelper |
| CL08 package | Trojan Horse |
| CSFireMonitor package | Downloader |
| NirCmd package | Backdoor.Trojan |
| OpenOffice package | Suspicious.MH690 |
| RegCool package | Backdoor.Bifrose |

Symantec Norton Anti-Virus tuvo 7 falsos positivos.

## F-Secure

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| CSFireMonitor package | Trojan-Downloader.Win32.Small.afxn |
| eScan package | Trojan.Win32.Genome.erg |
| GoogleTool package | SMS-Flooder.Win32.Delf.l |
| Lektora package | Email-Worm.Win32.Skybag.c |
| NetMeter package | Backdoor.Win32.Delf.kxp |
| Photomatix package | Net-Worm.Win32.Kolabc.dtf |
| SweetDream package | Trojan.Win32.Agent.bkjm |

F-Secure tuvo 7 falsos positivos.

## ESET

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| 6-Zip package | Win32/Agent |
| BattlestationsMidway package | Win32/Statik |
| dotWidget package | Win32/Statik |
| F1Challenge package | Win32/Genetik |
| FineReaderPro package | Win32/Statik |
| InkScapePortable package | Win32/Spy.Agent |
| IZArc package | Win32/Statik |
| JkDefrag package | Win32/Packed.Autoit.Gen |
| KnightsOfHonor package | Win32/Statik |
| Musketeers package | Win32/Statik |
| PunicWar package | Win32/Statik |
| T-Online package | NewHeur_PE |
| WinDVD package | Win32/Genetik |

ESET NOD32 tuvo 13 falsos positivos.

## McAfee

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| 6-Zip package | Generic.dx |
| AutoStartAdmin package | Generic!Artemis |

| | |
|---|---|
| CDDVDBurner package | Generic.dx |
| FileFolderUnlocker package | Generic!Artemis |
| GoogleDesktop package | Generic.dx |
| GoogleTool package | Generic Flooder |
| MultiInstall package | Generic!Artemis |
| Noctramic package | Generic!Artemis |
| RegRun package | Generic!Artemis |
| RootkitUnhooker package | Generic.dx |
| Soldner package | Generic!Artemis |
| TaskManager package | PWS-LDPinch |
| XPTweaker package | Generic!Artemis |

McAfee con Artemis tuvo 13 falsos positivos.

## Kaspersky

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| CleanCenter package | Backdoor.Win32.SdBot.itt |
| CSFireMonitor package | Trojan-Downloader.Win32.Small.afxn |
| Downutube package | Trojan-Downloader.Win32.Generic |
| DVDIdentifier package | Trojan.Win32.Generic |
| eScan package | Trojan.Win32.Genome.erg |
| GoogleTool package | SMS-Flooder.Win32.Delf.l |
| Lektora package | Email-Worm.Win32.Skybag.c |
| NetMeter package | Backdoor.Win32.Delf.kxp |
| PAR package | Trojan-Dropper.Script.Generic |
| Photomatix package | Net-Worm.Win32.Kolabc.dtf |
| PicSize package | Trojan-Dropper.Script.Generic |
| SweetDream package | Trojan.Win32.Agent.bkjm |
| WinMerge package | Email-Worm.Script.Generic |
| WinPlosion package | Trojan.Win32.Hooker.t |

Kaspersky tuvo 14 falsos positivos.

## AVG

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| AVIRA package | Generic11.BJHA |
| BattleMaps package | Win32/Heur |
| BlackMirror package | Downloader.Swizzor |
| BlazeMediapro package | Generic12.BLDZ |
| CDDVDBurner package | Generic10.VAH |
| CreateMovie package | BackDoor.Hupigon4.AEWM |
| Cubes package | Win32/Heur |
| FreeMSNWinks package | Generic6.IYW |
| HotLaunch package | Generic12.BLDZ |
| InkScapePortable package | Obfustat.NPF |
| Linkman package | SHeur.ERY |
| PCDoorGuard package | BackDoor.Generic10.LFG |
| SmartMorph package | Generic12.BLDZ |
| Soldner package | PSW.Generic6.FR |

| | |
|---|---|
| Sophos package | Agent.AOUE |
| StartKiller package | Generic12.BLDZ |
| SummerBound package | Generic12.BLDZ |

AVG tuvo 17 falsos positivos.

## eScan

| **Falsos positivos encontrados en algunas partes de** | **Detectados como** |
|---|---|
| ApplicationAccessServer package | Trojan.Spy.Sigatar.5041.B |
| BitTorrent package | Trojan.Generic.376185 |
| CDDVDBurner package | Trojan.Generic.97211 |
| CFOS package | Trojan.Heur.GM.0440616120 |
| CityGuide package | Trojan.AgentMB.Delf.HZGAB0939497 |
| CL08 package | Trojan.Generic.430620 |
| GoogleTool package | Trojan.Generic.1267563 |
| HPRestore package | BAT.KillAV.Gen |
| InkScapePortable package | Trojan.Generic.103962 |
| LogMeIn package | Virtool.903 |
| MediaConverter package | Backdoor.Generic.148978 |
| PCSecurityTest package | Trojan.Generic.1397003 |
| PowerTools package | Macro.VBA |
| Putty package | Worm.Generic.15375 |
| SmartNIC package | Trojan.Downloader.JLPF |
| Word2Web package | Macro.VBA |
| Zattoo package | Trojan.Generic.1372495 |

eScan tuvo 17 falsos positivos.

## Norman

| **Falsos positivos encontrados en algunas partes de** | **Detectados como** |
|---|---|
| AudioVideo2Exe package | W32/Packed_Upack.A |
| Azureus package | DLoader.LOXQ |
| BookmarkBuddy package | Ircbot.YJP |
| dBPower package | W32/Malware.ERCK |
| Firefox package | HTML/Iframe.gen.A |
| GPSphoto package | W32/Joiner.BRV.dropper |
| IconHider package | W32/Webmoner.ABJ |
| Insaniquarium package | W32/Smalltroj.IBLY |
| JSplit package | W32/Crypto |
| Kazaa package | W32/Packed_PeX.B |
| MaulwurfsMover package | Suspicious_F.gen |
| Nero package | W32/OnLineGames.HUPN |
| NirCmd package | Smalldoor.CGNH |
| PocketChess package | W32/Agent.GZWS.dropper |
| RadLight package | Malware.DNHL |
| PDPSoftware package | Malware.FNSF |
| RivaTuner package | W32/Agent.IQHH |
| StreamRipper package | NetworkWorm.EMS |
| TaskManager package | W32/LdPinch.SFX |

| | |
|---|---|
| TyperShark package | W32/Smalltroj.IBLY |
| Vitascene package | W32/EMailWorm.BES |
| XP-AS package | Antivirus2008.PU |
| Zuma package | W32/Smalltroj.IBLU |

Norman tuvo 23 falsos positivos.

## AVIRA

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| 3DScreensaver package | TR/Spy.8369026.A |
| 6-Zip package | TR/Agent.239371.A |
| AdKiller package | HEUR/Malware |
| BOM package | HEUR/HTML.Malware |
| CDSearch package | HEUR/HTML.Malware |
| ClipBoardRecorder package | HEUR/Malware |
| CSFireMonitor package | DR/Dldr.Small.afxn |
| DashBoard package | HEUR/Malware |
| DrWeb package | TR/QQShou.EO.1 |
| Edimax driver package | SPR/Hacktool.57344 |
| EKalkulator package | TR/Crypt.ULPM.Gen |
| EUPrice package | HEUR/Macro.Word95 |
| GoogleTool package | DR/Flood.Delf.L |
| HP scanner package | HEUR/Malware |
| InternetDownloadManager package | TR/Crypt.XPACK.Gen |
| iRejectTrash package | HEUR/Malware |
| LaunchExpress package | HEUR/Malware |
| MSI WLAN package | ADSPY/Agent.emg |
| NeighborsFromHell package | TR/Dropper.Gen |
| Paraworld package | TR/Downloader.Gen |
| PCDoorGuard package | BDS/Beasty.A |
| SmartProtector package | TR/Agent.593920.A |
| StickSecurity package | HEUR/Malware |
| TrendMicro package | TR/Hijacker.Gen |

AVIRA tuvo 24 falsos positivos.

## BitDefender

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| ApplicationAccessServer package | Trojan.Spy.Sigatar.5041.B |
| BitTorrent package | Trojan.Generic.376185 |
| Browster package | Win32.ExplorerHijack |
| CDDVDBurner package | Trojan.Generic.97211 |
| CFOS package | Trojan.Heur.GM.0440616120 |
| CityGuide package | Trojan.AgentMB.Delf.HZGAB0939497 |
| CL08 package | Trojan.Generic.430620 |
| DiaShowPro package | Packer.Morphine |
| FotoWorks package | Packer.Morphine |
| GoogleTool package | Trojan.Generic.1267563 |
| Haushaltsbuch package | Generic.PWS.Games.4.4E81B454 |

| | |
|---|---|
| HPRestore package | BAT.KillAV.Gen |
| InkScapePortable package | Trojan.Generic.103962 |
| LogMeIn package | Virtool.903 |
| MediaConverter package | Backdoor.Generic.148978 |
| PCSecurityTest package | Trojan.Generic.1397003 |
| PowerTools package | Macro.VBA |
| Putty package | Worm.Generic.15375 |
| ShopToDate package | Trojan.Generic.1287015 |
| SKS_CD package | Trojan.Generic.1055076 |
| SmartNIC package | Trojan.Downloader.JLPF |
| TeamSpeak package | Trojan.Pws.Hooker.TR |
| Word2Web package | Macro.VBA |
| Zattoo package | Trojan.Generic.1372495 |

Bitdefender tuvo 25 falsos positivos.

## TrustPort

| **Falsos positivos encontrados en algunas partes de** | **Detectados como** |
|---|---|
| AudioVideo2Exe package | W32/Packed_Upack.A |
| AVIRA package | Generic11.BJHA |
| Azureus package | DLoader.LOXQ |
| BookmarkBuddy package | Ircbot.YJP |
| CDDVDBurner package | Generic10.VAH |
| CreateMovie package | BackDoor.Hupigon4.AEWM |
| dBPower package | W32/Malware.ERCK |
| Firefox package | HTML/Iframe.gen.A |
| GPSphoto package | W32/Joiner.BRV.dropper |
| IconHider package | W32/Webmoner.ABJ |
| Insaniquarium package | W32/Smalltroj.IBLY |
| JSplit package | W32/Crypto |
| Kazaa package | W32/Packed_PeX.B |
| MaulwurfsMover package | Suspicious_F.gen |
| NirCmd package | Smalldoor.CGNH |
| PCDoorGuard package | BackDoor.Generic10.LFG |
| PocketChess package | W32/Agent.GZWS.dropper |
| RadLight package | Malware.DNHL |
| RivaTuner package | W32/Agent.IQHH |
| Soldner package | PSW.Generic6.FR |
| Sophos package | Agent.AOUE |
| StreamRipper package | NetworkWorm.EMS |
| TaskManager package | W32/LdPinch.SFX |
| TyperShark package | W32/Smalltroj.IBLY |
| Vitascene package | W32/EMailWorm.BES |
| XP-AS package | Antivirus2008.PU |
| Zuma package | W32/Smalltroj.IBLU |

TrustPort tuvo 27 falsos positivos.

## Avast

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| 3DScreensaver package | Win32:Trojan-gen { Otro } |
| 0190warner package | Win32:Rootkit-gen [Rootkit] |
| Burn4Free package | Win32:Navexcel-H [Troyano] |
| CDDVDBurner package | Win32:Trojan-gen { Otro } |
| CheckMail package | Win32:Trojan-gen { Otro } |
| CL08 package | Win32:Trojan-gen { Otro } |
| CreateMovie package | Win32:Trojan-gen { Otro } |
| CSFireMonitor package | Win32:Trojan-gen { Otro } |
| CTManager package | Win32:Trojan-gen { Otro } |
| Dirwat package | Win32:Trojan-gen { Otro } |
| edVARdo package | Win32:Trojan-gen { Otro } |
| ExelockExpress package | Win32:Trojan-gen { Otro } |
| FolderPatrol package | Win32:Trojan-gen { Otro } |
| FTP4Pro package | Win32:Delf-GJF [Troyano] |
| GoogleTool package | Win32:Trojan-gen { Otro } |
| iNetQuery package | Win32:Trojan-gen { Otro } |
| iPodAccess package | Win32:Trojan-gen { Otro } |
| LockFolderXP package | Win32:Trojan-gen { Otro } |
| MDAdressbuch package | Win32:Delf-GJF [Troyano] |
| NetMeter package | Win32:Trojan-gen { Otro } |
| Noctramic package | Win32:Hgweb-B [Troyano] |
| PDFExplorer package | Win32:Trojan-gen { Otro } |
| PhotoMatix package | Win32:Trojan-gen { Otro } |
| SharpEye package | Win32:SkiMorph [Cryptovirus] |
| SKS package | Win32:Trojan-gen { Otro } |
| StartpageSave package | Win32:Trojan-gen { Otro } |
| Suse package | ELF:Race-D [Exploit] |
| Winter package | Win32:Trojan-gen { Otro } |

Avast tuvo 28 falsos positivos.

## G DATA

| Falsos positivos encontrados en algunas partes de | Detectados como |
|---|---|
| 0190warner package | Win32:Badya |
| 3DScreensaver package | Win32:Badya |
| ApplicationAccessServer package | Trojan.Spy.Sigatar.5041.B |
| BitTorrent package | Trojan.Generic.376185 |
| Burn4Free package | Win32:Badya |
| CDDVDBurner package | Win32:Badya |
| CFOS package | Trojan.Heur.GM.0440616120 |
| CheckMail package | Win32:Badya |
| CityGuide package | Trojan.AgentMB.Delf.HZGAB0939497 |
| CL08 package | Trojan.Generic.430620 |
| CreateMovie package | Win32:Badya |
| CSFireMonitor package | Win32:Badya |
| CTManager package | Win32:Badya |
| Dirwat package | Win32.Daum.A |

| | |
|---|---|
| edVARdo package | Win32:Badya |
| ExelockExpress package | Win32:Badya |
| FolderPatrol package | Win32:Badya |
| FTP4Pro package | Win32:Badya |
| GoogleTool package | Win32:Badya |
| HPRestore package | BAT.KillAV.Gen |
| iNetQuery package | Win32:Badya |
| InkScapePortable package | Trojan.Generic.103962 |
| iPodAccess package | Win32:Trojan-gen { Otro } |
| LockFolderXP package | Win32:Badya |
| LogMeIn package | Virtool.903 |
| MDAdressbuch package | Win32:Badya |
| MediaConverter package | Backdoor.Generic.148978 |
| NetMeter package | Win32:Trojan-gen { Otro } |
| Noctramic package | Win32:Badya |
| PCSecurityTest package | Trojan.Generic.1397003 |
| PDFExplorer package | Win32:Trojan-gen { Otro } |
| PhotoMatix package | Win32:Trojan-gen { Otro } |
| PowerTools package | Macro.VBA |
| Putty package | Worm.Generic.15375 |
| SharpEye package | Win32:SkiMorph [Cryptovirus] |
| SKS package | Win32:Trojan-gen { Otro } |
| SmartNIC package | Trojan.Downloader.JLPF |
| StartpageSave package | Win32:Trojan-gen { Otro } |
| Suse package | ELF:Race-D [Expl] |
| Winter package | Win32:Trojan-gen { Otro } |
| Word2Web package | Macro.VBA |
| Zattoo package | Trojan.Generic.1372495 |

G DATA tuvo 44 falsos positivos.

## Command

| **Falsos positivos encontrados en algunas partes de** | **Detectados como** |
|---|---|
| 3DScreensaver package | W32/Malware!1b74 |
| 320mph package | W32/Backdoor2.YMQ |
| Air2Mp3 package | W32/Banload.E.gen!Eldorado |
| AnimateDesktop package | W32/Heuristic-187!Eldorado |
| AVIRA package | W32/Agent.K.gen!Eldorado |
| Blitzkrieg package | W32/IRCBot-based!Maximus |
| Budgeter package | W32/Backdoor2.RWA |
| Burn4Free package | W32/Malware!e664 |
| CDDVDBurning package | W32/Heuristic-210!Eldorado |
| ClonyXXL package | W32/Heuristic-210!Eldorado |
| CookieCooker package | Security_Risk |
| CPUZ package | W32/Downldr2.DYOA |
| DM package | W32/OnlineGames.F.gen!Eldorado |
| DriveImage package | W32/D_Downloader!GSA |
| DriveIndexTool package | W32/Autoit.B |
| DrWeb package | W32/Downloader.N.gen!Eldorado |
| Enfish package | W32/Threat-SysAdderSml!Eldorado |

| | |
|---|---|
| ePaper package | SWF/Downloader.D!Camelot |
| EzDesk package | Security_Risk |
| FileAnalyser package | W32/Backdoor.AJKH |
| FlashGet package | W32/Malware!0e45 |
| Generals package | W32/IRCBot-based!Maximus |
| GIMP package | W32/Onlinegames.gen |
| Gothic package | W32/Trojan.BHOT |
| iNetControl package | W32/NewMalware-Rootkit-I-based!Maximus |
| JAlbum package | SWF/Downloader.D!Camelot |
| Kasperky package | W32/Heuristic-KPP!Eldorado |
| KCFM package | W32/BankerP.FJ |
| McAfee package | W32/Blocker-based!Maximus |
| Memtest package | Heuristic-90 |
| Myth package | W32/IRCBot-based!Maximus |
| NGame package | W32/AV2008.E |
| OutlookTuner package | W32/Heuristic-CO2!Eldorado |
| PCWizard package | W32/Heuristic-USU!Eldorado |
| Pidgin package | W32/Onlinegames.gen |
| Powerstrip package | W32/Heuristic-210!Eldorado |
| RadioRipper package | W32/Trojan3.CC |
| RegCool package | W32/Backdoor.AJKH |
| RootkitUnhooker package | W32/Heuristic-210!Eldorado |
| Sims package | W32/Hijack.A.gen!Eldorado |
| Stammbaum package | W32/Downloader.B.gen!Eldorado |
| TaskManager package | W32/Heuristic-210!Eldorado |
| TCPfilter package | W32/Backdoor2.DARJ |
| ThirdReich package | W32/IRCBot-based!Maximus |
| TrendMicro package | W32/Downldr2.FCFK |
| TweakPower package | W32/Backdoor.AJKH |
| UltraStar package | W32/Zlob.R.gen!Eldorado |
| Unreal package | W32/Heuristic-119!Eldorado |
| UPACK compression tool package | W32/Virut.AI!Generic |
| USBtray package | W32/Banload.C.gen!Eldorado |
| WebZip package | W32/Downloader.L.gen!Eldorado |
| WinMHT package | W32/Downloader.L.gen!Eldorado |
| WinSplit package | W32/AV2008.C |
| Worms3D package | W32/IRCBot-based!Maximus |
| XPTweaker package | W32/Heuristic-210!Eldorado |

Command tuvo 55 falsos positivos. Por favor, tenga en cuenta que Command es un participante nuevo en nuestras pruebas. Confiamos en que durante la próxima evaluación la cantidad de falsos positivos sea mucho menor.

## Kingsoft

| **Falsos positivos encontrados en algunas partes de** | **Detectados como** |
|---|---|
| ACER driver package | Win32.Troj.Monder.475648 |
| AlbumCoverArt package | Win32.Troj.StartPage.a.1585049 |
| Animation package | Win32.Hack.ThinlPackerT.a.378833 |
| Astra package | Win32.Hack.HacDef.1245184 |
| Autoruns package | Win32.Troj.Chuzy.352256 |

| | |
|---|---|
| BaldursGate package | Win32.Hack.Kelebek.1120149 |
| CCleaner package | Win32.Troj.Selfish.1497584 |
| ClonyXXL package | Worm.Roron.136332 |
| ColoringBook package | Win32.Troj.Unknown.az.186112 |
| CounterStrike package | Worm.Roron.136332 |
| CPUZ package | Win32.TrojDownloader.Small.624231 |
| Creative driver package | Win32.Troj.Obfuscated.40960 |
| DarkHorizons package | Win32.Troj.Unknown.az.186112 |
| eMule package | Win32.Troj.Agent.3534076 |
| FAR package | Win32.Troj.Taris.1418369 |
| Fifa package | Win32.Hack.Beastdoor.1154875 |
| Folder2ISO package | Win32.TrojDownloader.Delf.us.3174400 |
| F-Secure package | Win32.Hack.ThinlPackerT.a.378833 |
| Gothic2 package | Win32.PSWTroj.Nilage.42496 |
| Grep package | Win32.Troj.VB.96768 |
| HotSpotShield package | Win32.Troj.Agent.oe.1035231 |
| HoverWheel package | Win32.Hack.IRCBot.1444845 |
| IceAge2 package | Win32.Hack.ThinlPackerT.a.378833 |
| Intel driver package | Win32.Hack.ThinlPackerT.a.378833 |
| Less package | Win32.Troj.Agent.15872 |
| LoginControl package | Win32.VirInstaller.Agent.508937 |
| MagischesAuge package | Win32.Hack.ThinlPackerT.a.378833 |
| MapInfo package | Win32.Troj.Varvar.292864 |
| MapleXP package | Win32.VirInstaller.Agent.842830 |
| Medion driver package | Win32.Troj.Hidrag.110592 |
| MIRC package | Win32.Troj.Plutor.1007616 |
| MS Links package | Win32.Troj.SysJunkT.hh |
| MS Office97 package | Win32.Troj.Undersor__5B.318976 |
| MS Windows95 package | Worm.Ganda__3E514.70199 |
| MS Windows95 SP1 package | Win32.Troj.Pres__130B9A.66672 |
| MS Windows98 package | Worm.Ganda__6A7DE.70199 |
| MS Windows2000 package | Worm.Ridnu.4880 |
| MS WindowsXP package | Win32.Troj.Patched.14336 |
| MS WindowsXP SP1 package | Worm.Polip.274432 |
| MS WindowsXP SP2 package | Worm.Polip.388608 |
| MS WindowsXP SP3 package | Worm.Wast__66F897.156550 |
| MS WindowsME package | Win32.Troj.Pres__CCA2FB.81920 |
| MS Works package | Win32.Hack.ThinlPackerT.a.378833 |
| NortonSystemWorks package | Worm.Brontok.176911 |
| PCW package | JS.Agent.dg.4982 |
| PEiD package | Win32.Troj.Sality.158720 |
| Perl package | VBS.DNAOrder.aa.35780 |
| PowerStrip package | Win32.Hack.Huigezi.1012719 |
| ProcessExplorer package | Win32.Troj.Stagol.192512 |
| RegistryMonitor package | Win32.Troj.Taris.98304 |
| RegistryOptimierer package | Worm.Beagle.102400 |
| Resistance package | Win32.Troj.JunkDll.ao.147559 |
| SataRaid package | Win32.Troj.Virut.905216 |
| Scanner package | Win32.Troj.Sality.160256 |
| ShellOut package | Win32.Joke.MovingMouse.k.20480 |
| SIW package | Win32.Troj.Tvido.1598976 |
| SpaceShooter package | Win32.Hack.Kelebek.1120149 |

| | |
|---|---|
| SQL package | Win32.Troj.Selfish.90166 |
| TCPview package | Win32.PSWTroj.LdPinch.94208 |
| T-Online package | Win32.Hack.ThinlPackerT.a.378833 |
| Unreal package | Win32.Hack.Shark.429069 |
| Video2Brain package | Win32.Hack.ThinlPackerT.a.378833 |
| WinRAR package | Win32.Troj.Selfish.1004712 |
| WinRoll package | Win32.Troj.OnLineGames.of.15360 |
| WISO package | Win32.Hack.ThinlPackerT.a.378833 |
| Zzzap package | Win32.IRC.Flood.n.2103523 |

Kingsoft tuvo 66 falsos positivos, de los cuales algunos fueron archivos del sistema operativo. Por favor, tenga en cuenta que Kingsoft es un participante nuevo en nuestras pruebas. Confiamos en que durante la próxima evaluación la cantidad de falsos positivos sea mucho menor.

Kingsoft es el primer fabricante de China con el valor suficiente para desafiar el reto de nuestra evaluación internacional. Antes de que un producto pueda formar parte de nuestras pruebas públicas principales, primero es necesario que apruebe nuestros requerimientos mínimos. No son muchos los fabricantes chinos que reúnen los requisitos para participar en nuestras evaluaciones internacionales.

## Influencia de los falsos positivos en las menciones

Por favor, recuerde que – como ya habíamos anunciado el año pasado – los falsos positivos detectados en nuestras pruebas ahora provocan que las menciones otorgadas sean inferiores. Los rótulos para falsos positivos encontrados en nuestro grupo de archivos limpios no se modificaron, así como los rangos de tasas de detección. Las menciones se otorgan según se muestra en la siguiente tabla:

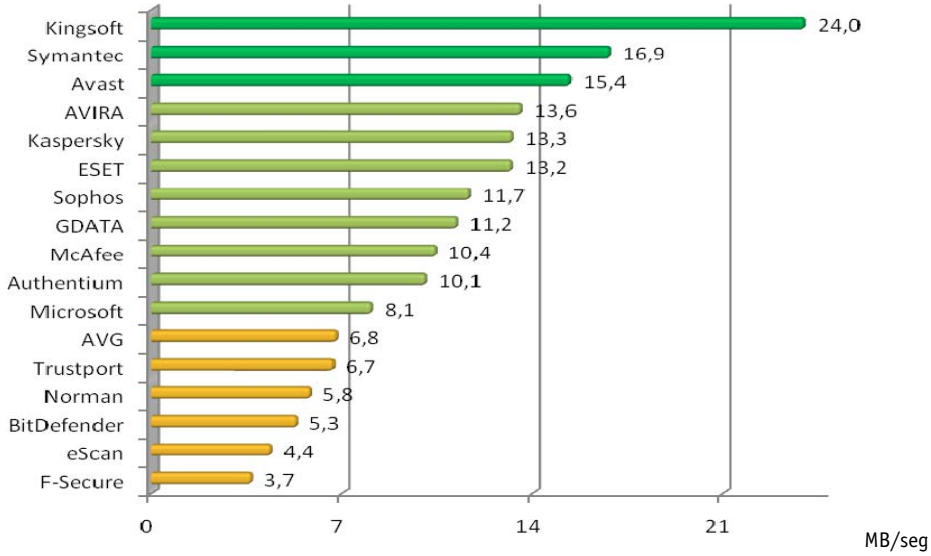
| | **Tasas de detección** | | | |
|---|---|---|---|---|
| | **<87%** | **87 - 93%** | **93 - 97%** | **97 - 100%** |
| **Pocos** (de 0 a 15 falsos positivos) | **tested** | **STANDARD** | **ADVANCED** | **ADVANCED+** |
| **Muchos** (de 16 a 100 falsos positivos) | **tested** | **tested** | **STANDARD** | **ADVANCED** |

*Al tener rangos fijos (en especial por los falsos positivos) a veces puede resultarles un poco difícil a los fabricantes aceptar que bajaron a una categoría menor debido simplemente a algunos falsos positivos detectados de más en nuestro grupo de archivos limpios. Pero tenemos la opinión de que los rangos ya son lo bastante generosos (en especial considerando que todos los fabricantes siempre obtienen las muestras de falsos positivos una vez terminada la evaluación y pueden solucionar el problema, mientras que nuestro grupo de archivos limpios no crece tanto con el paso del tiempo).*

*No modificaremos los rangos para contentar a algunos fabricantes. Les sugerimos a los fabricantes seguir mejorando sus productos; de esa forma obtendrán menciones más altas cuando lo merezcan según los resultados obtenidos. Las nuevas reglas aplicadas ya se habían informado el año pasado. Es posible que los fabricantes que habrían obtenido menciones más elevadas si sólo tuviéramos en cuenta las tasas de detección estén desconformes con la implementación de dichos requerimientos más estrictos para otorgar las menciones.*

## Prueba de velocidad de exploración

Los productos antivirus tienen diferentes velocidades de exploración debido a diversas razones. Hay que tener en cuenta la confiabilidad de la tasa de detección de un producto antivirus; si usa la emulación de códigos, si es capaz de detectar virus polimórficos complicados, si hace una exploración heurística profunda y una exploración para detectar rootkits activos, si el soporte de desempaquetamiento y descompresión es profundo y exhaustivo, si tiene exploradores de seguridad adicionales, etc. Además, algunos productos usan tecnologías para reducir los tiempos de exploración en exploraciones subsiguientes salteándose archivos que ya fueron explorados con antelación. Como deseamos conocer la velocidad de exploración (cuando los archivos realmente están siendo explorados en búsqueda de malware) y no la velocidad para saltearse archivos, dichas tecnologías no se tienen en cuenta en esta evaluación. Creemos que ciertos fabricantes deberían informarles a los usuarios en forma más clara sobre las exploraciones que optimizan el rendimiento; y luego dejar que el usuario decida si prefiere una exploración de rendimiento mejorado (que no vuelve a controlar todos los archivos, presentando el riesgo potencial de pasar por alto archivos infectados) o una exploración que ofrezca una seguridad completa. El siguiente gráfico muestra la tasa de transferencia en MB/seg (cuanto más alto es más veloz) de los diversos productos antivirus mientras hacen una exploración (bajo demanda) en la configuración máxima de nuestro grupo completo de archivos limpios (usados para la prueba de falsos positivos). La tasa de transferencia de la exploración variará de acuerdo al grupo de archivos limpios[3], las configuraciones y el hardware usado.




La tasa de transferencia promedio para la exploración antivirus (velocidad de exploración) se calcula tomando el tamaño en MB del grupo de archivos limpios dividido por el tiempo en segundos empleado hasta el momento en que finaliza la exploración. La tasa de transferencia de la exploración de esta prueba no puede ser comparada con pruebas futuras o con otras pruebas, ya que varía debido al grupo de archivos usados, hardware, etc. Las pruebas de velocidad de exploración se realizaron en equipos con Windows XP SP3, en máquinas idénticas Intel Core 2 Duo E8300/2.83GHz 2GB RAM, con discos SATA II.

[3] Para saber la velocidad que tendrá cada producto en *su* computadora mientras explora *sus* archivos, le recomendamos que pruebe los productos usted mismo.

## Niveles de menciones alcanzados en esta prueba

AV-Comparatives otorga un sistema de menciones de 3 niveles (STANDARD, ADVANCED y ADVANCED+). Como este informe también incluye las tasas de detección originales sin evaluar los falsos positivos (ver página 13), en lugar de incluir sólo las menciones, los usuarios a quienes no les importan los falsos positivos si lo desean pueden basarse solamente en ese puntaje. Ahora es más difícil obtener menciones altas porque las menciones se basan en las tasas de detección del GRUPO B, que sólo incluye malware de los últimos nueve meses (desde mayo de 2008 hasta comienzos de febrero de 2009). En este caso las tasas de detección (porcentajes) son inferiores que en las últimas pruebas, donde contamos el puntaje alcanzado general basándonos tanto en el Grupo A como en el B (cuando el Grupo A queda bien cubierto por casi todos los fabricantes). Además, la detección de falsos positivos ahora afecta el nivel de mención que se otorga.

| **MENCIONES**<br>(basadas en las tasas de detección y los falsos positivos) | **PRODUCTOS**<br>(sin un orden específico)[4] |
|---|---|
|  | ✓ Symantec<br>✓ ESET<br>✓ Kaspersky<br>✓ McAfee[5] |
|  | ✓ G DATA*<br>✓ AVIRA*<br>✓ Avast*<br>✓ BitDefender*<br>✓ eScan*<br>✓ TrustPort*<br>✓ F-Secure |
|  | ✓ AVG*<br>✓ Sophos<br>✓ Microsoft |
|  | ✓ Authentium*<br>✓ Norman*<br>✓ Kingsoft |

*: productos que obtuvieron una mención inferior debido a los falsos positivos

Las menciones no se basan solamente en las tasas de detección – también se tienen en cuenta los falsos positivos encontrados en nuestro grupo de archivos limpios. Un producto que detecta con éxito un alto porcentaje de malware pero genera falsos positivos no es necesariamente mejor que un producto que detecta menos malware pero que garantiza una menor detección de falsos positivos.

[4] Sugerimos que consideren todos los productos con la misma mención como equivalentes en cuanto a calidad.
[5] McAfee sin Artemis habría obtenido la mención ADVANCED, por favor, lea los comentarios de páginas 6 y 13.

## Copyright y descargos

Esta publicación tiene Copyright © 2009 por AV-Comparatives e.V. ®. Cualquier uso de los resultados, etc. en forma total o parcial, SÓLO está permitido tras el acuerdo por escrito extendido por la junta directiva de AV-Comparatives e.V., en forma previa a cualquier publicación. AV-Comparatives e.V. y sus evaluadores no podrán ser considerados responsables por cualquier daño o pérdida que ocurra como resultado de (o relacionado a) el uso de la información provista en este documento. Tomamos todos los recaudos posibles para asegurar la precisión de los datos básicos, pero no se podrá hacer responsable a ningún representante de AV-Comparatives e.V. por la exactitud de los resultados de las pruebas. No ofrecemos ninguna garantía de que la información o el contenido provisto en cualquier momento determinado sean correctos, completos o apropiados para un propósito específico. Ningún otro individuo involucrado en la creación, producción o distribución de los resultados de las pruebas podrá considerarse responsable por cualquier pérdida de beneficios o daño indirecto, especial o consecuente que surja de (o esté relacionado a) el uso o incapacidad de usar los servicios provistos por el sitio Web, documentos de pruebas o cualquier material relacionado. AV-Comparatives e.V. es una organización austriaca registrada sin fines de lucro.

Para más información sobre AV-Comparatives y las metodologías de evaluación, por favor, visite nuestro sitio Web.

AV-Comparatives e.V. (marzo de 2009)

**THIS REPORT HAS BEEN TRANSLATED INTO SPANISH BY A THIRD PARTY.**

**WE DO NOT ASSUME ANY RESPONSABILITY FOR ITS CONTENT.**

**THE ORIGINAL ENGLISH VERSION OF THIS DOCUMENT CAN BE FOUND AT:**

http://www.av-comparatives.org/images/stories/test/ondret/avc_report21.pdf