EFECTIVIDAD Y EFICIENCIA DE LOS ANTIVIRUS GRATUITOS COMBINADOS FRENTE AL MALWARE

EFFECTIVENESS AND EFFICIENCY OF FREE ANTIVIRUS SOFTWARE AGAINST MALWARE

Marlon Renné Navia Mendoza[1], Jorge Antonio Párraga Álava[1], Gustavo Gabriel Molina Garzón[1], José Armando Vidal Loor[2]

[1]Carrera Informática, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Campus Politécnico El Limón, Km 2.7, Calceta, Ecuador.

[2]Departamento Tecnológico, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Campus Politécnico El Limón, Km 2.7, Calceta, Ecuador.

Contacto: mnaviam@gmail.com

RESUMEN

El estudio consistió en evaluar cuatro antivirus gratuitos con el objetivo de observar su rendimiento y carga de trabajo producida, tanto de forma individual como de forma combinada, al momento de proteger un computador contra el malware, para determinar qué tan conveniente es utilizar más de un antivirus a la vez. Para este proceso, se utilizó computadores con S.O. Windows 7 Profesional de 64 bits con varios programas utilitarios de uso común. Los aspectos considerados en la evaluación fueron: la carga de trabajo en el sistema, la protección ante amenazas y la utilidad en general. Se emplearon utilidades adicionales, como AppTimer o BootRacer para medir los parámetros de funcionamiento del software instalado en el computador. Los resultados obtenidos han permitido inferir la eficiencia de los antivirus tanto de forma individual y combinada, con la diferencia que la segunda modalidad requiere más recursos.

Palabras clave: Malware, virus, evaluación, antivirus combinados.

ABSTRACT

Four free pieces of antivirus software were evaluated with the objective of examining their performance and produced functions, both individually and as a group, when used to protect computers against malware. The aim was to determine whether it is convenient to use more than a piece of antivirus software at a time. 64-bit S.O. Windows 7 Professional computers and common utility tools were used for the evaluation. The aspects considered for evaluation were as follows: produced functions on the system, protection against threats, and general serviceability. Additional utility tools (for example AppTimer and BootRacer) were used in order to monitor functioning parameters of the software installed on the computer. Through the obtained results, it was possible to gain insight into the efficiency of the evaluated pieces of software both individually and as a group the latter being more expensive.

Keywords: Malware, virus, evaluation, combined antivirus.

CC BY NC SA

Recibido: 30 de mayo del 2014
Aceptado: 04 de febrero del 2015
ESPAMCIENCIA 6(1): 45-49/2015

INTRODUCCIÓN

El software malicioso, o malware como se lo conoce de forma abreviada (*Maliciosus software*) es cualquier tipo de programa no deseado, diseñado para afectar, en menor o mayor medida, el funcionamiento o la seguridad de un equipo o sistema informático (Kramer y Bradfield, 2009). Avizienis *et al.* (2004) definen a la seguridad en informática como la combinación de los atributos de confidencialidad, integridad y disponibilidad; y es a estos atributos a los que afecta el malware.

El malware es cada vez más sofisticado. Muchas soluciones de prevención, como los antivirus, se están viendo superadas por estas amenazas. No solo porque aprovecha las ventajas de la tecnología, sino también por otros aspectos como la falta de una adecuada prevención, hasta el desconocimiento de ciertas normas por parte del usuario (Fuentes, 2008).

Si bien los virus son solo una forma de malware, el usuario común tiende a llamar virus a todo tipo de malware, de ahí que el software antimalware se lo promociona y conoce como antivirus. Dado que con el incremento en el uso de internet ha aumentado la cantidad de malware que puede afectar a un computador, también ha crecido la oferta de software antivirus para proteger no solo a los PC tradicionales, sino incluso a los dispositivos móviles, muchos de ellos en una versión gratuita.

Este trabajo tiene como objetivo principal determinar el mejor funcionamiento de la combinación de antivirus gratuitos para el sistema operativo Windows 7 Professional, en comparación con el desempeño individual.

MATERIALES Y MÉTODOS

La metodología de las pruebas se basó en lo realizado por Lai y Wren (2011) pero adaptado a los objetivos del presente trabajo. Los parámetros evaluados fueron:

Carga del sistema: Recursos utilizados normalmente por la instalación de antivirus en el computador:

- Cantidad de memoria RAM ocupada (En reposo y durante escaneo)
- Uso del CPU durante escaneo
- Tiempo de arranque del sistema
- Tiempo de inicio de aplicaciones

Protección:

- Cantidad de malware detectado
- Capacidad para eliminar o bloquear el malware
- Tiempo de análisis

Las evaluaciones se hicieron en computadores con las siguientes características a nivel de hardware: Procesador Intel Core i5 a 3 GHz, 6 GB de memoria RAM a 1333 MHz, disco duro ATA de 1.5 TB, unidad óptica de DVD-R/W.

En lo correspondiente al software se instaló el sistema operativo Windows 7 Profesional de 64 bits; además el paquete de Microsoft Office 2010©, y el navegador de internet Mozilla Firefox©. Con estos programas instalados se procedió a la clonación del sistema en un disco duro externo antes de proceder a la instalación del antivirus a evaluar. Esto, con la finalidad de prevenir cambios en el computador producto de la instalación y la eliminación de virus y antivirus.

También se instalaron las aplicaciones BootRacer 4.0 (Greatis Software LLC, 2013) y AppTimer. El primero se utilizó para verificar el rendimiento del sistema operativo cuando se inicializa, el segundo verificó el tiempo de demora de cargar un programa específico (Lai y Wren, 2011).

Para las pruebas se utilizaron cuatro antivirus en sus versiones gratuitas: Avast, AVG, Avira, y Panda Cloud; con la última versión al momento de realizar las pruebas. Se escogieron estos debido a que en varias revisiones se encontraban entre los que mejor se desempeñaban a nivel de aplicaciones gratuitas contra el malware.

Carga del sistema

En el computador, descrito anteriormente, se procedió a la instalación de uno o dos antivirus para cada evaluación. Con el programa BootRacer se determinó el tiempo desde que se presionaba el botón de encendido hasta que el computador cargaba completamente.

Una vez terminado el uso del BootRacer se establecía los tiempos en reposo, es decir mientras no se utilizaba ninguna aplicación por parte del usuario, de la memoria RAM y uso del CPU a través de la utilidad administrador de tareas de Windows. Para determinar el tiempo que demoraba iniciar Microsoft Word 2010 se utilizó el software AppTimer, el mismo que abría y cerraba el programa midiendo el tiempo de carga. Las operaciones de medición de tiempo, tanto de arranque del sistema como de car-

ga de programas, se repitieron cinco veces en cada caso. Con este procedimiento se obtuvo un tiempo promedio en cada indicador de evaluación.

Protección

Para realizar los respectivos análisis se utilizaron dos medios extraíbles: una memoria USB y un DVD. En ambos se grabó una colección de 170 archivos entre instaladores, ejecutables, comprimidos, documentos e imágenes; que en total sumaban 2.2 GB, y en donde se incluía 50 archivos de malware de diferentes características, principalmente troyanos y gusanos. Para cada antivirus y combinación de los mismos se escaneó ambos medios de almacenamiento y se registraron los siguientes parámetros: amenazas detectadas, archivos desinfectados/enviados a baúl y tiempo de escaneo.

Una vez obtenidos los datos se procedió a realizar un análisis descriptivo para observar desempeño de los antivirus estudiados y sus combinaciones.

RESULTADOS Y DISCUSIÓN

El gráfico 1 muestra la comparación de los valores obtenidos en el tiempo de arranque y carga del sistema operativo y la cantidad de memoria RAM total (sistema más aplicaciones) ocupada en reposo. Estos resultados indican que el antivirus con menor tiempo de arranque del sistema es el Avira (casi 30 seg.); mientras que los tiempos más alto fueron para las combinaciones Avast-AVG, AVG-Avira, y Avira-Panda con un tiempo de carga de más de 60 seg. Todos los demás antivirus y su instalación conjunta estuvieron dentro de este rango de tiempos. Por otra parte, Panda cloud fue el que más demoró, en comparación con el resto de instalaciones individuales, pasando los 40 seg. en promedio en las pruebas realizadas. La combinación de antivirus que menos tiempo de inicio del sistema tomó, fue Avast-Avira con 48 seg.

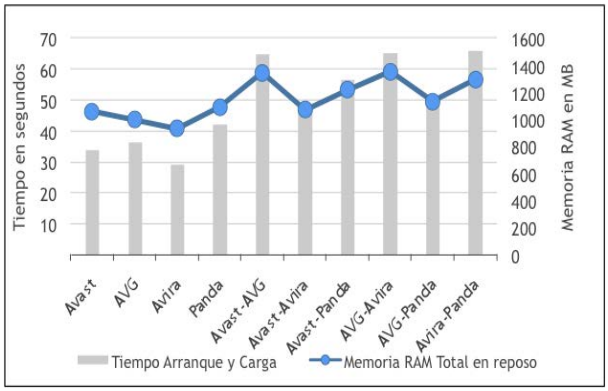

Gráfico 1. Comparación de valores de carga en el sistema para cada caso de instalación de antivirus

Respecto al uso total de memoria del computador en el gráfico 1 se observa que hay una tendencia similar al tiempo de arranque, por lo que se deduce que posiblemente exista una correlación. En instalación individual, Avira es el que menos memoria emplea, aproximadamente 930 MB; mientras que Avast y Panda llegan aproximadamente a 1060 MB. Al igual que en los tiempos de arranque del sistema, el uso total de memoria física se incrementa al usar más de un antivirus y sobrepasa los 1200 MB en la mayoría de los casos. En el uso de memoria RAM, cuando se dió la combinación de antivirus, se obtuvo como valor mínimo 1066 MB en la combinación Avast-Avira; como valores máximos aproximadamente 1350 MB en las combinaciones Avast-AVG y AVG-Avira.

Adicionalmente, se midió el tiempo de carga (arranque) de las aplicaciones Mozilla Firefox (Grafico 2) y Microsoft Word 2010 (Grafico 3). En ambos gráficos se muestran los tiempos promedio obtenidos en las pruebas. En el caso de Mozilla Firefox dejó la configuración inicial predeterminada para que abriera la página de inicio que aparece por defecto; mientras que Microsoft Word abría un documento en blanco.

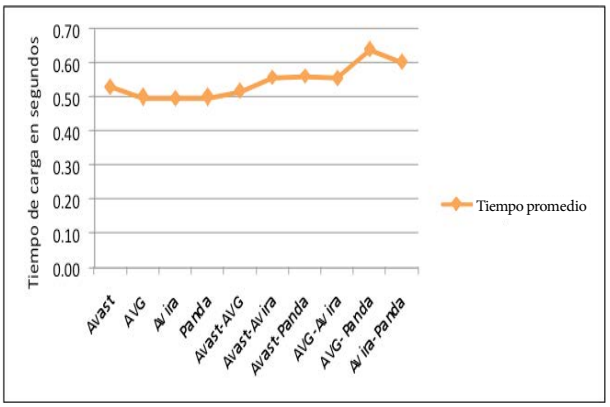

Gráfico 2. Tiempos de carga mínimo, máximo y promedio de aplicación Mozilla Firefox

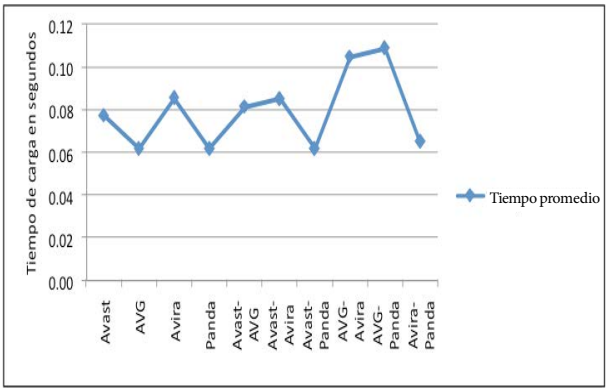

Gráfico 3. Tiempos de carga mínimo, máximo y promedio del inicio de aplicación Microsoft Word

En general, los resultados no presentan una variabilidad excesivamente marcada, a excepción de la combinación AVG-Panda que presenta un tiempo de carga en memoria ligeramente mayor respecto al resto; aunque para el arranque de Mozilla Firefox si se nota una tendencia similar a lo presentado en el gráfico 1, respecto a aumentar el tiempo al combinar dos antivirus.

En el gráfico 4 se muestra el tiempo de análisis en segundos y el número de malware detectado, la línea refleja los tiempos y las barras el tiempo en segundos, siendo el Panda el de mayor tiempo de análisis, sobrepasando los 900 seg; mientras el AVG demora menos de 100 seg, en los demás casos tienden a demorar alrededor de 200 seg.

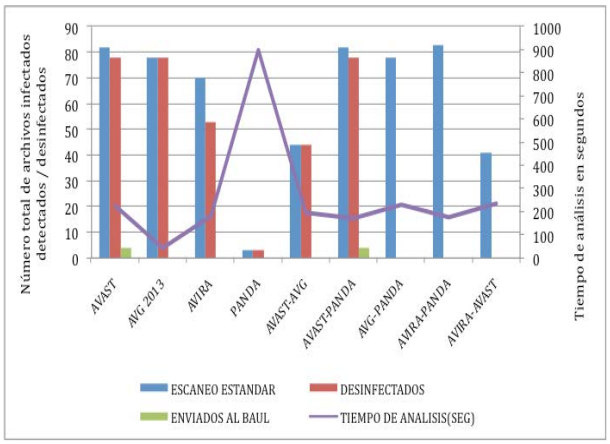

Gráfico 4. Desempeño de los antivirus y combinaciones en la búsqueda de malware

La cantidad de archivos desinfectados, o enviados a baúl, tanto por los antiviurs de forma individual como sus combinaciones, es similar a la totalidad de malware detectado en las pruebas. En la mayoría de los casos se detectó la mayor parte de los archivos infectados que se utilizaron para las pruebas; la excepción en este caso fue Panda, que no detectó la mayoría del malware que se encontraban en los medios. Si bien no se determinó el motivo exacto de esta respuesta, se presume que puede deberse a que su versión gratuita requiere una conexión permanente a internet.

Respecto a la cantidad de malware detectado y desinfectado no hay una gran diferencia entre la utilización de un antivirus o de dos; sin embargo, se nota cierta dificultad en la desinfección en este último caso. Así mismo, el tiempo de análisis se incrementa un poco con el uso de dos antivirus; la causa de la aparente disminución en la eficiencia se puede deber a la interferencia entre uno y otro antivirus; lo cual debe ser objeto de otro estudio. Cabe anotar que Bishop *et al.* (2011) en su estudio, donde trabajó con hasta 15 motores de antivirus combinados, concluye que a mayor número de antivirus es menor la probabilidad de que se dé un fallo en la detección de malware. Sin embargo, no menciona nada sobre la carga de trabajo y desempeño en general de los equipos en los que se hicieron las pruebas.

Por los resultados encontrados se puede afirmar que con el antivirus Avira se obtiene un menor tiempo de carga del sistema operativo y menor uso de sus recursos en cuanto a memoria RAM. En cuanto a la detección de virus no difiere del que más eliminó, que en este caso fue Avast, y el antivirus que menos demoró, alrededor de 100 segundos, fue AVG.

Una limitación del presente trabajo es la cantidad de antivirus estudiados en relación a la oferta del mercado; solo se han probado cuatro versiones gratuitas de uso personal, mientras el Instituto AV-Test (2014), por ejemplo, realiza pruebas de 25 productos solo para Windows 7. Aunque las versiones pagadas de antivirus suelen tener herramientas de protección adicionales, no implica necesariamente que se obtenga mayor seguridad y eficacia, como lo indica Hui (2010). Hay que tener presente que adquirir un determinado software antivirus, por lo general pagado, puede provocar en los usuarios una falsa sensación de seguridad ante el desconocimiento de otros aspectos importantes como el buen uso de contraseñas, por ejemplo.

Otro aspecto no considerado en este estudio y que puede ser objeto de propuestas o estudios similares, es el uso de antivirus en dispositivos móviles y la seguridad basada en la nube o internet (Cloud en inglés). La presencia de malware en los dispositivos móviles se está incrementando y evolucionando, a tal punto que su impacto puede llegar a ser mayor que el causado en los equipos de escritorio (Porter *et al.,* 2011). Estos aspectos los aborda Lin (2011) en su trabajo que incluye una propuesta de investigación sobre el tema. Sin embargo queda pendiente un estudio a profundidad del desempeño de los sistemas de seguridad basados en la nube.

Así mismo, se podrían realizar estudios comparativos con mecanismos de detección de malware no tradicionales como el presentado por Demme *et al.* (2013). Este trabajo muestra un mecanismo de detección de malware basado en métricas detectadas online a nivel de hardware, que podrían cubrir ciertas falencias del software antivirus.

CONCLUSIONES

El uso de recursos a nivel de memoria RAM, así como el tiempo de arranque y carga del sistema operativo, en general suele ser mayor cuando hay dos antivirus instalados que cuando hay solo uno.

Al momento de detectar malware, la combinación de dos antivirus obtuvo resultados ligeramente mejores que de forma individual. Así mismo, los tiempos de análisis son mayores cuando hay dos antivirus instalados.

Se puede indicar que no existe un antivirus, de los evaluados, que al combinarse con otro antivirus tenga mayor eficacia sin aumentar el uso de recursos. Sin embargo, la combinación Avast-Panda tiene los mejores valores en promedio en los aspectos evaluados

LITERATURA CITADA

- Avizienis, A; Laprie, J; Randell, B; Landwehr, C. 2004. Basics Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions of Dependable and Secure Computing. 1(1):11-33.
- AV-Test. 2014. Pruebas Usuarios Finales (en línea). Formato (HTML). Consultado el 1 de abril de 2014. Disponible en http://av-test.org/es/inicio/.
- Bishop, P; R. Bloomfield; I. Gashi; V. Stankovic. 2011. Diversity for Security: a Study with off-the-shelf Antivirus Engines. IEEE 22nd International Symposium on Software Reliability Engineering. (2011, Hiroshima, Japón) p. 11-19.
- Demme, J; Maycock, M; Schmits, J; Tang, A; Waksman, A; Sethumadhavan, S; Stolfo, S. 2013. On the Feasibility of Online Malware Detection with Performance Counters. ACM SIGARCH Computer Arquitecture News – ISCA'13. 41(3):559-570.
- Fuentes, L. 2008. Malware, una amenaza de Internet. Revista Digital Universitaria. UNAM. 9(4):3-6
- Greatis Software LLC. 2013. BootRacer (en línea). Formato (HTML). Consultado el 1 de abril de 2014. Disponible en http://www.greatis.com/bootracer/index.html.
- Hui, W. 2010. Brans, knowledge, and false sense of security. Information Management and Computer Security. 8(3):162-172.
- Kramer, S. y J. Bradfield. 2009. A general definition of malware. Journal of Computer Virology. Volume 6 Number 2. (FR). Disponible en http://www.springerlink.com.
- Lai, K. y D. Wren. (PassMark Software) 2011. Small Business Endpoint Protection Performance Benchmarks (en línea). Formato (PDF). Consultado el 1 de abril de 2014. Disponible en http://www.passmark.com.
- Lin, X. 2011. Survey on Cloud Based Mobile Security and A New Framework for Improvement. IEEE International Conference on Information and Automation. (2011, Shenzhen, China) p. 710-715.
- Porter, A; Finifter, M; Chin, E; Hanna, S; Wagner, D. 2011. A Survey of Mobile Malware in the Wild. Proceedings of the 1st ACM workshop on Security and Privacy in smartphones and mobile devices. (2011, New York, USA) p. 3-14.