Informe sobre la prueba Remediation

AV-TEST GmbH realizó la prueba por encargo de Enigma Software Group
Informe del 15 de febrero de 2017; actualizado el 15 de febrero de 2017

Resumen

En enero de 2017, AV-TEST examinó el rendimiento de las funciones de *Remediation* (término técnico inglés en cuanto a la detección, la eliminación y la limpieza) de SpyHunter, un producto de Enigma Software Group. La prueba se llevó a cabo en un sistema Windows 7 (SP1, 64 bits) limpio, utilizando la misma imagen de disco en varios ordenadores del mismo modelo.

El conjunto de malware utilizado en la prueba Remediation incluyó 20 softwares maliciosos y el proceso de prueba se dividió en dos fases. En la primera fase se infectó primero la imagen con una muestra de malware y después se intentó instalar el producto de seguridad, escanear el ordenador y eliminar la amenaza detectada. En la segunda fase de la prueba se desactivó la solución antivirus para poder infectar el sistema. A continuación se volvió a activar la solución antivirus y se reinició el sistema para asegurarse de que todos los componentes de la solución de seguridad funcionaban perfectamente. El último paso consistió en intentar limpiar el sistema y volver a escanearlo.

Tanto en la primera como en la segunda fase, SpyHunter eliminó con éxito el total de 20 programas maliciosos, es decir, que ofreció el máximo rendimiento posible.

El software consiguió neutralizar todos los componentes activos del malware y además borrar todos los restos de archivo que permanecían en el sistema.

Sinopsis

En vista del número de amenazas cada vez mayor que actualmente se desarrolla y disemina a través de Internet, el riesgo de una infección está aumentando. Mientras que hace solo unos años se publicaban nuevas amenazas cada par de días, hoy en día hay que contar con una incorporación al escenario de amenazas de miles de programas maliciosos cada hora.

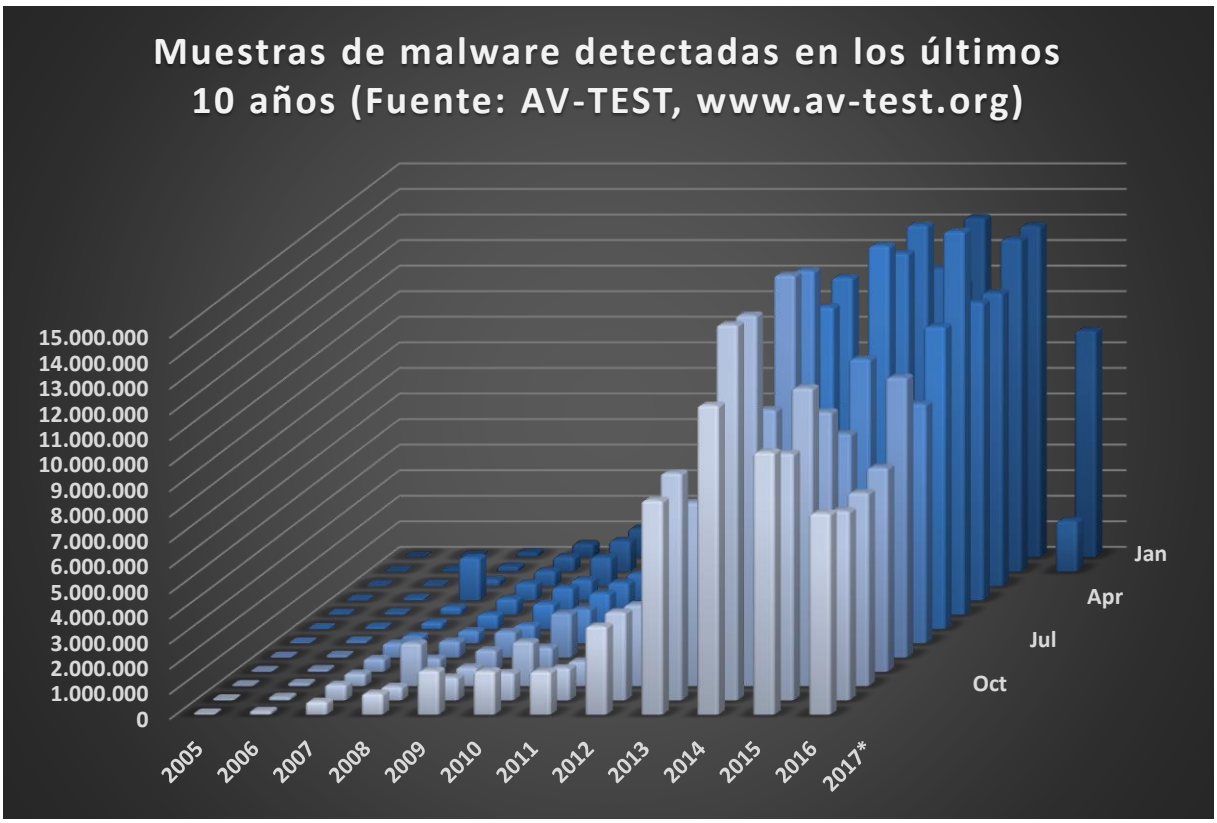


Gráfico 1: Nuevas muestras de malware al año

Mientras que, en el año 2000, AV-TEST reunía algo más de 170.000 muestras de malware nuevas, en 2013, la cifra de códigos maliciosos había ascendido ya a más de 80 millones. Echando un vistazo al gráfico 1 se comprueba que este incremento continúa en 2016. Actualmente hay más de 600 millones de muestras de malware en la base de datos de AV-TEST.

Los fabricantes de software de seguridad tienen que afrontar una cantidad ingente de nuevos malwares para proteger a sus clientes. Esta cantidad puede conllevar problemas, puesto que no siempre es posible proteger a tiempo un ordenador. Aunque haya instalado un software antivirus actualizado, el sistema puede ser infectado si transcurren varias horas entre el descubrimiento de un nuevo software malicioso y la puesta a disposición de las firmas pertinentes. En algunos casos puede ser demasiado tarde. Una infección puede ocasionar al usuario daños económicos si, por ejemplo, le roban datos confidenciales o no puede disponer del ordenador de forma eficiente hasta que el malware es eliminado por completo del sistema.

Teniendo esto en cuenta, las técnicas de Remediation cobran cada vez mayor importancia para poder volver a utilizar cuanto antes el ordenador infectado. No obstante, es imprescindible que el proceso de limpieza mediante estas técnicas sea fiable en dos aspectos:

1. El malware y todos sus componentes tienen que ser eliminados y se tienen que restablecer los sistemas infectados.
2. Ni los programas limpios ni el sistema deben sufrir daños durante el proceso de limpieza.

Producto sometido a la prueba

La prueba se llevó a cabo en enero de 2017 y AV-TEST utilizó la versión del software más actual disponible en ese momento:

- SpyHunter de Enigma Software Group

Método de prueba y valoración

Plataforma

Todas las pruebas fueron realizadas en ordenadores del mismo modelo con el siguiente hardware:

- CPU Intel Xeon Quad-Core X3360
- 4 GB RAM
- Disco duro de 500 GB (Western Digital)
- NIC Intel Pro/1000 PL (Gigabit Ethernet)

Como sistema operativo se utilizó Windows 7 (SP1, 64 bits), incluyendo los hotfixes instalados en la versión y los parches disponibles a día 3 de enero de 2017.

Método de prueba

La prueba Remediation se ejecutó en diez pasos aplicando el siguiente método:

1. **Un sistema limpio para cada malware**. Los sistemas de prueba se limpiaron y restablecieron antes de ser infectados con una sola de las muestras de malware.
2. **Ordenadores físicos**. Para la ejecución de la prueba se usaron únicamente ordenadores físicos; no se utilizaron entornos virtuales.
3. **Acceso a Internet**. Los ordenadores tuvieron acceso a Internet en todo momento para poder consultar la nube durante la prueba en caso de necesidad.
4. **Configuración del producto**. En todos los productos y sus herramientas de Remediation o herramientas de rescate con autoarranque se utilizaron los ajustes estándares, de acuerdo con la configuración de fábrica.
5. **Infección de los ordenadores de prueba.** Se infectó un ordenador nativo con un malware y luego se reinició. De este modo se garantizó que el malware estuviera completamente activo.
6. **Familias de malware y software malicioso (payloads)**. Respecto a las muestras para la prueba se tuvo en cuenta que no procedieran de la misma familia de malware o utilizaran el mismo software malicioso.
7. **Remediation usando todas las funciones del producto disponibles**.
    a. Se procuró instalar el producto de seguridad con la configuración estándar y se siguieron todas las indicaciones del producto para eliminar el malware.
    b. Si a. no era ejecutable, se debía intentar con una ***herramienta de reparación independiente o una herramienta de rescate*** (si se disponía de ella).

c. Si b. no era posible, debía utilizarse una ***solución con autoarranque*** independiente para eliminar la amenaza (si se disponía de ella).

8. **Comprobación de la eliminación del malware.** La comprobación del ordenador se realizó manualmente. Se comprobó si la eliminación había sido completa y si quedaban restos de archivos.
9. **Valoración del rendimiento en cuanto a la eliminación de malware.** El rendimiento de la herramienta y del conjunto de la solución de seguridad se valoró utilizando un sistema de puntuación acordado previamente.
10. **Repercusión excesiva de la función de Remediation.** En la prueba se comprobó, además, en qué medida una solución de seguridad aplica métodos agresivos para limpiar el sistema. Hay productos, por ejemplo, que eliminan por completo los archivos hosts o incluso directorios enteros, aunque esto no sea necesario para llevar a cabo con éxito el proceso de Remediation. El recurrir a estos métodos supondría la pérdida de puntos en la valoración.

Valoración de la efectividad

Se otorgaron puntos por cada muestra de malware utilizada de acuerdo con el siguiente sistema:

a. El malware se ha eliminado por completo (3 puntos)
b. El malware se ha detectado y eliminado, quedando solo restos de archivo inactivos (2 puntos)
c. Se detectó y eliminó algo parcialmente, pero quedaron restos del software malicioso aún activos (1 punto)
d. No se detectó el malware y, por tanto, no se eliminó (0 puntos)

A la hora de otorgar los puntos no se tuvo en cuenta a qué técnica de las disponibles se tuvo que recurrir para eliminar el malware. No obstante, debían utilizarse todas las técnicas. Si un producto eliminaba las entradas en el archivo hosts correspondientes a dicho producto, dejaba limpio el ordenador y dicho producto podía seguir funcionando correctamente y siendo actualizado, el producto debía recibir la máxima puntuación por su rendimiento en Remediation, aun cuando las entradas de otros fabricantes de software de seguridad permanecieran en el archivo hosts.

Muestras

El conjunto de prueba abarcaba 20 programas maliciosos capaces de infectar Windows 7 (SP1, 64 bits).

Resultados de la prueba

El producto de Enigma Software Group alcanzó la máxima puntuación tanto en la primera como en la segunda fase de la prueba. En el gráfico 2 puede ver los resultados de ambas fases de la prueba.

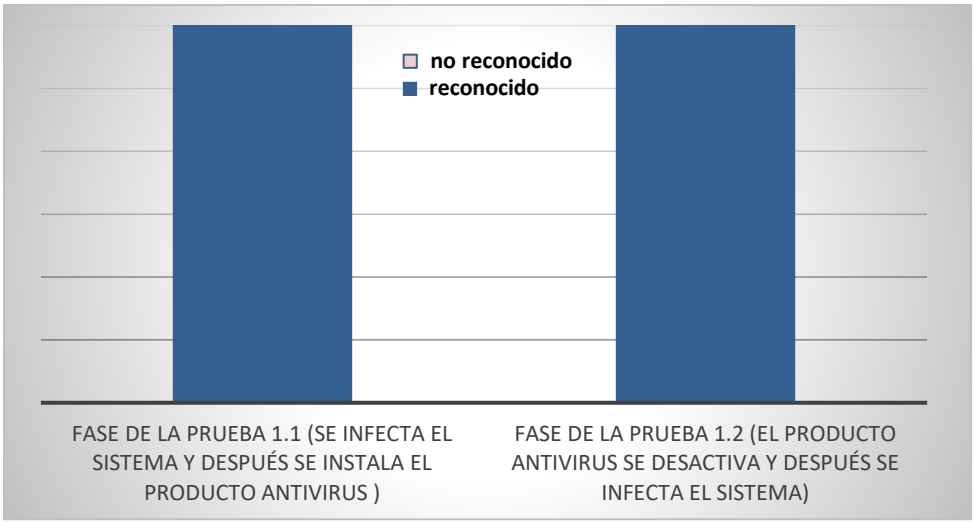
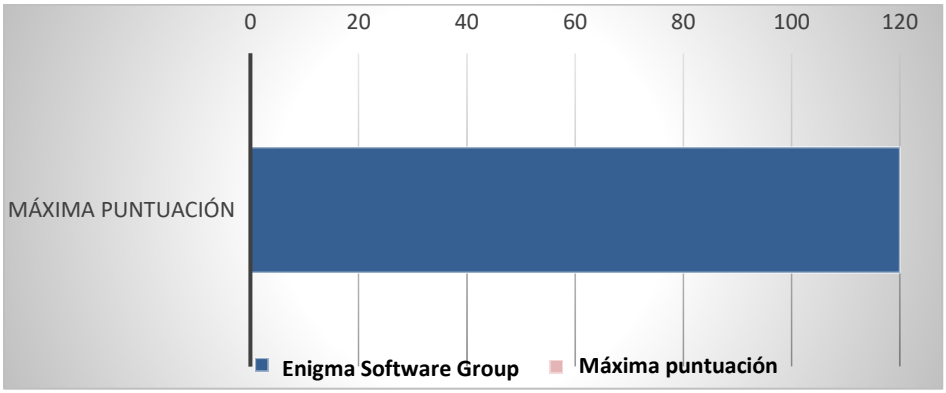


Gráfico 2: Resultado de la prueba de Remediation: fases 1.1 y 1.2

La puntuación máxima que se podía obtener en la prueba era de 120 puntos. Como refleja claramente el gráfico 3, Enigma Software Group consiguió la máxima valoración de 120 puntos. Cuando se comprobó el rendimiento de la limpieza en la fase de prueba 1.2, SpyHunter pudo limpiar por completo el sistema.

En la fase de prueba 1.1, el software consiguió asimismo un resultado perfecto limpiando al 100 por cien el sistema infectado.



Anexo

Información sobre la versión del software sometido a la prueba

Desarrollador, fabricante	Denominación del producto	Versión del programa	Motor/versión de la firma
Enigma Software Group	SpyHunter 4	4.24.3.4750	2017.01.17v01

Lista de las muestras de malware utilizadas en la prueba Remediation

(SHA256)
0x0248aef55dd424770217a568e6d6e621b08f010faecc3bdc889e815bdba562b7
0x2e9b4aa0d8f1fe0c8f75faaad8fea213cc982678925e883199d4e73316830e27
0x379d26795c02cd028f5fc33210b598228a8f23f9926bac365668e1044c30f496
0x3963f5795ab1c34ffe7ae23424b82631d24908c3c25bb5b703fba8403f63e7a8
0x496badd81af03f9a74f3fc321225d8376dc6aff613e2d2e4328fabf33fbe3853
0x4e5212dc24b5d6b3b6281db2ed33bc8b271151c11a1a7b6fc16d5a843aef7bc4
0x4f5bff64160044d9a769ab277ff85ba954e2a2e182c6da4d0672790cf1d48309
0x534ceed806ec84ae75fdd2e3f1c837cb1e263f52e03a73366a199f45456acfc2
0x5847e0b50f7279000e7335af0b0925b413718810cf5591d8ea253ae55893a197
0x6bf17b1dc8eb3b0ae6412bd2d71fe73832e9b4c7ba259d9d13e46427401c4145
0x73e7b43fed5fe22d58ba0c36080eb70f00640ea9e615d8e5ce1785d76d1f2a76
0x814d8c756520ebc86fcf8f544a352d17bb7636333a206c27bc0710320fabd279
0x90c1e0eb0eb37300e2177b465b9289daa910f2df2a6b5e63f3504958f7a71bc8
0x931339d73c08813699f40ff613083fc393e17fe99c1bdbdb2ea8038816b1c289
0xb3cf3567fab18b8a39277b33d0a89b2f0f79a7f2a3583ad663fd5d80f6c49546
0xd32ee2cf13429517274cda35c341861ab9d947533163da3154b74ca40b8161f6
0xd861451d5ee19419ac829bdba0622ce9e1edcc6ef9f1a6f5257ee0744771ae76
0xece08e1c4d119df6217853b7ef22bff31e0c58f9d204878b2e28e6ff9e1ba782
0xefbd13ee753e4b879616a020bdb77212abdf637e6c288ab48672276bb69d24d2
0xf93c7b95df816eed946a5028f44f3e9185baf63ccbcf66047331cfb3b5a2654a