Informe sobre la prueba Remediation

AV-TEST GmbH realizó la prueba comparativa por encargo de Enigma Software Group
Informe del 20 de agosto de 2018; actualizado el 20 de agosto de 2018

Resumen

En julio de 2018, 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 10 (RS3, 64 bits) limpio, utilizando la misma imagen de disco en varios ordenadores del mismo modelo.

El kit de malware utilizado en la prueba Remediation incluyó 12 códigos maliciosos y el proceso de prueba se dividió en dos fases. 1ª fase de la prueba: Como primer paso, se infectó la imagen con una muestra de malware y después se intentó instalar el producto de seguridad, escanear el ordenador y eliminar la amenaza detectada. 2ª fase de la prueba: En primer lugar, 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 y por completo 10 de los 12 muestras de malware, es decir, que ofreció un rendimiento muy bueno. El software de Enigma 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, actualmente hay que contar con una incorporación al escenario de amenazas de miles de programas maliciosos cada hora.

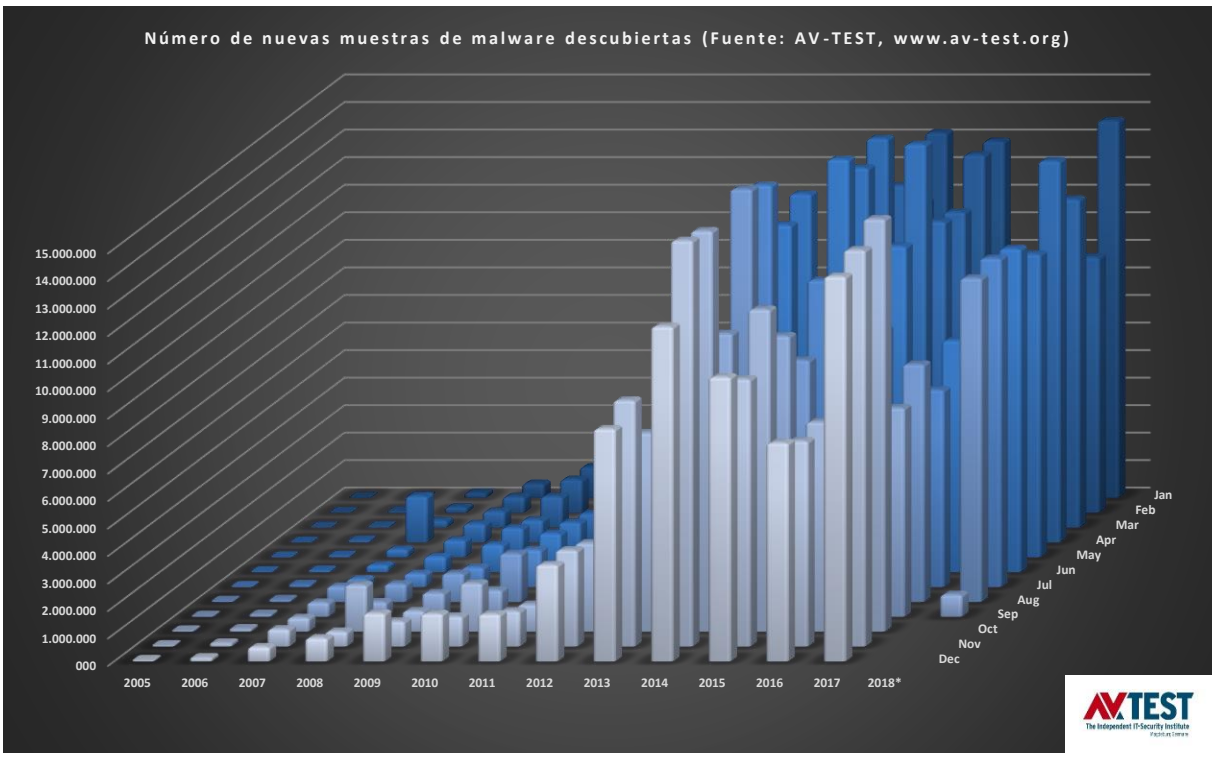


Gráfico 1: Nuevas muestras de malware al año

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 en los años siguientes. Actualmente hay más de 800 millones de muestras de malware en la base de datos de AV-TEST y, en el primer semestre de este año, los sistemas de detección de AV-TEST se incorporaban cada mes unos 10 millones de malwares nuevos.

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 2018 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 10 (RS3, 64 bits), incluyendo los hotfixes instalados en la versión y los parches disponibles a día 4 de junio de 2018.

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, solo quedaron restos de archivos inactivos (2 puntos)
c. Se detectó algo y se eliminó parcialmente, pero quedaron restos aún activos del software malicioso (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 la prueba abarcaba 12 programas maliciosos capaces de infectar Windows 10 (RS3, 64 bits).

Resultados de la prueba

El producto de Enigma Software Group volvió a alcanzar un resultado muy bueno de un 97,2 por ciento 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.

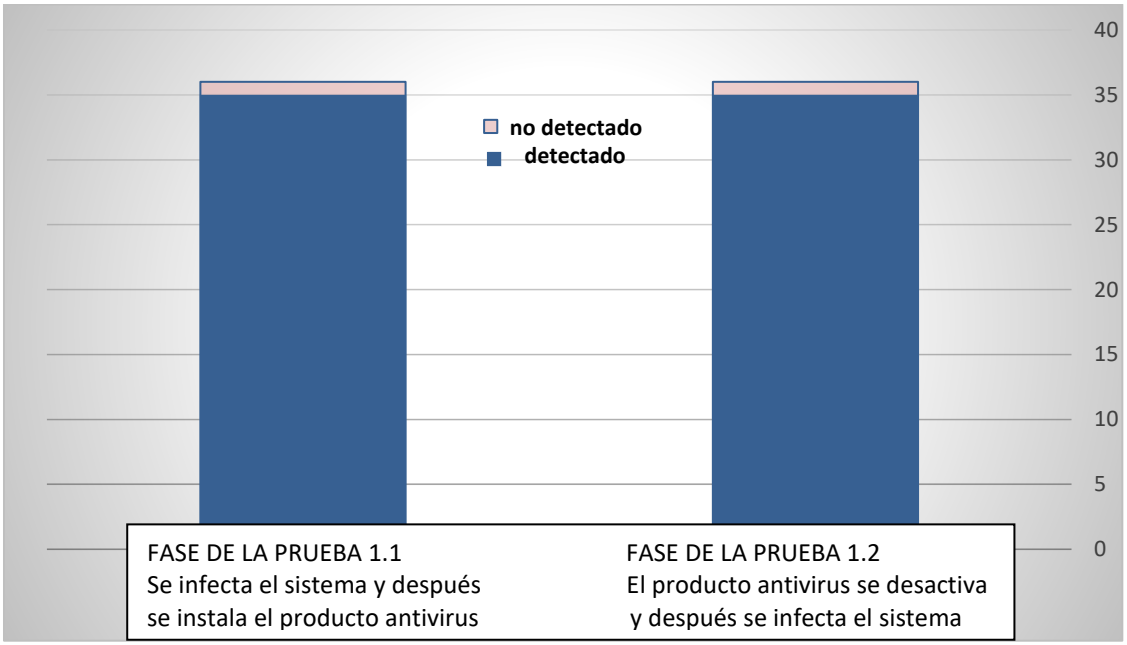
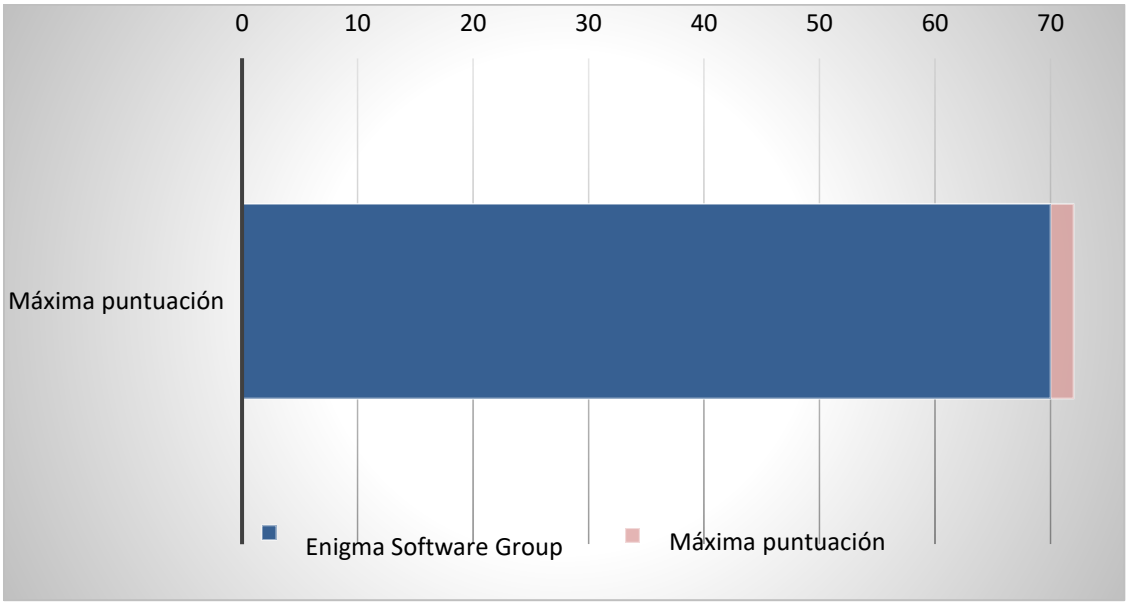


Gráfico 2: Resultado de la prueba de Remediation: fases 1.1 y +1.2

Cuando se comprobó el rendimiento de la limpieza en la fase de prueba 1.2, SpyHunter consiguió eliminar por completo 10 de los 12 muestras de malware. Tanto en la primera como en la segunda fase el programa no pudo eliminar solo una entrada del malware en el registro y sufriera una pequeña deducción.

La puntuación máxima que se podía obtener en la prueba era de 72 puntos. Como refleja claramente el gráfico 3, Enigma Software Group consiguió la valoración de 70 puntos.



Anexo

Información sobre la versión del software sometido a la prueba

Desarrollador, fabricante	Denominación del producto	Versión del programa
Enigma Software Group	SpyHunter 5	5.0.30.51

Lista de las muestras de malware utilizadas en la prueba Remediation

(SHA256)
0x10864dff8bcea96f842f6642bca59199b677e28e6e174c3e4d7b65391b0698b0
0x2942841f850c59c1f7bedd1922aca54c886bad1eb51b90b32af7d6b6b6e5cab4
0x5ba58146b785d5e72993430d95960486cbf9bf9429e5e3bf4fa2fe2e88f4e250
0x69bb101c4c53fe2a87ed2200dd46b7d82d92c86943e47a31ce7922455b92d345
0x70179938e6c056df16b1403615cc553a10a90297601446f95d6ad004ca1e29eb
0x86958f2f177eed14d6164d48a18cb15c12516bdb59f1125471d966f3e212b989
0x980f254b3954b3d7ded9772cad328d6872491fbd645ac3dae3d277620cfb88b7
0xac186a20bbec078f08788cc8a4a746de0139a061a6d2588787d217f019c2eb90
0xb3548b485e919e043b935b071ad54f37e1c996046fcfbefae51d76a437ee6a93
0xd8a3f066a3b961b4c8623e0d30e3e867fd7a1c9187aa396de8457df70b602efe
0xe275e10bea80834252aea1b5dba9a817b278b5c4a6d0594b01b1605de0b66f79
0xf92dd910c0c00e5924a27bbffcdb303e5f724b3caf540e844c3f82a291cc7a30