Informe sobre la prueba Remediation

AV-TEST GmbH realizó la prueba por encargo de Enigma Software Group
Informe del 19 de mayo; actualizado el 24 de mayo de 2016

Resumen

En abril y mayo de 2016, AV-TEST comprobó el rendimiento de las funciones de *Remediation* (término técnico inglés en cuanto a la detección, la eliminación y la limpieza) de SpyHunter, un producto fabricado por Enigma Software Group. La prueba fue realizada en un sistema con Windows 7 (SP1, 64 bits) limpio y se utilizó la misma imagen de disco en varios ordenadores del mismo modelo.

El conjunto de malware utilizado en la prueba Remediation abarcaba 20 softwares maliciosos y el proceso de prueba tuvo lugar en dos fases. 1ª fase de la prueba: El primer paso consistió en infectar la imagen de disco con una muestra de malware. A continuación se intentó instalar el producto de seguridad, escanear el ordenador y eliminar la amenaza detectada. 2ª fase de la prueba: Al principio de esta fase de la prueba se desactivó la solución antivirus y se infectó 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 se habían instalado y activado correctamente. El último paso consistió en intentar limpiar el sistema y volver a escanearlo.

Durante la primera fase de la prueba, SpyHunter consiguió eliminar por completo 19 de los 20 programas maliciosos, lo cual es un resultado muy bueno. Durante la segunda fase, eliminó 16 de los 20 malwares, un resultado que aún puede considerarse bueno.

SpyHunter pudo neutralizar los componentes activos del malware que se hallaba en el ordenador. La mayoría de los archivos restantes eran archivos ejecutables del programa malicioso que habían sido almacenados en el sistema bajo "C:\Users\vtc\AppData\Roaming\". Solo en un caso fue SpyHunter incapaz de tratar los componentes activos del malware, de modo que el sistema permaneció infectado.

Sinopsis

En vista del creciente número de amenazas que se están desarrollando y diseminando a través de Internet, el riesgo de una infección está aumentando. Hace tan solo unos pocos años se publicaban amenazas cada par de días. Esto ha cambiado radicalmente y entretanto se calcula que cada hora surgen varios miles de nuevos programas maliciosos.

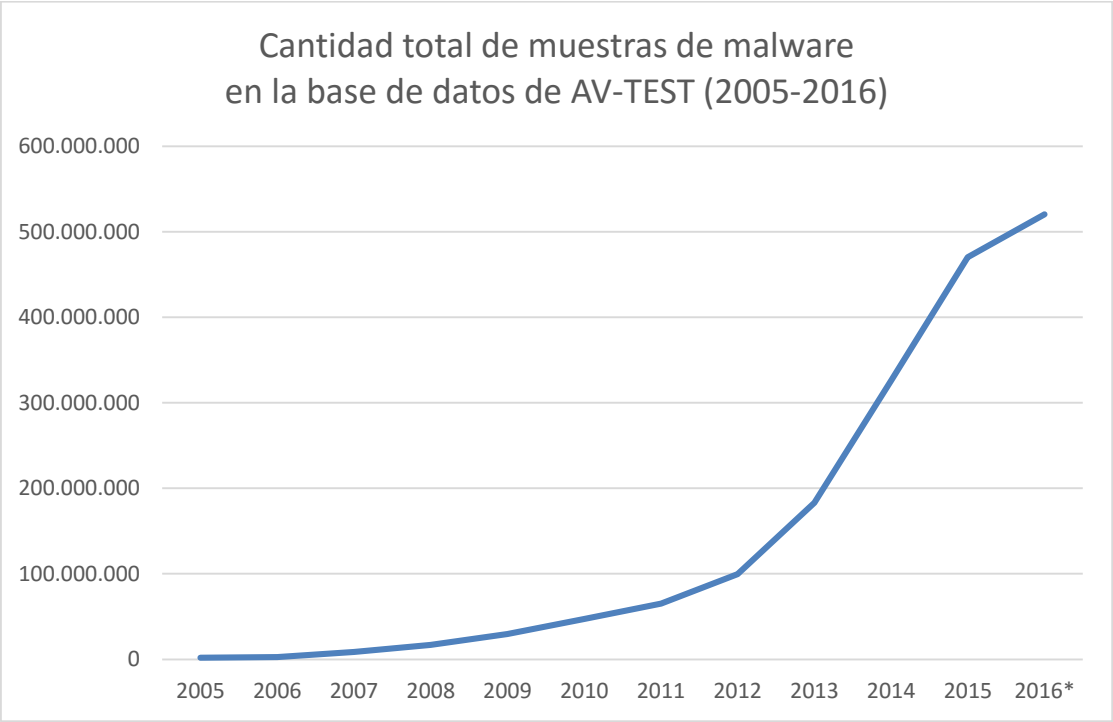


Gráfico 1: Nuevas muestras de malware al año

Mientras que en el año 2000, AV-TEST recopilaba más de 170.000 muestras de malware, el número había aumentado a más de 80 millones en 2013 y la cifra sigue aumentando en 2016. Este incremento aparece representado en el gráfico 1. Actualmente hay más de 500 millones de muestras de malware en la base de datos de AV-TEST.

Teniendo en cuenta esta evolución se puede partir de la base de que tan solo el hacer frente a semejante cantidad de nuevo software malicioso para proteger a sus clientes ya puede suponer un problema para los fabricantes de software de seguridad. No siempre es posible proteger a tiempo un ordenador frente a las amenazas. Aunque se haya instalado en el ordenador una versión actualizada del antivirus, este puede ser infectado, ya que desde que se descubre un nuevo malware hasta que se ponen a disposición las correspondientes firmas del virus transcurren varias horas. En algunos casos es demasiado tarde. Infecciones pueden causar al usuario pérdidas financieras si, por ejemplo, le roban datos confidenciales o no puede utilizar el ordenador de forma eficiente hasta que el malware es eliminado por completo del sistema.

Por ese motivo, el aspecto de la limpieza cobra cada vez una mayor importancia cuando es necesario volver a utilizar cuanto antes el ordenador infectado. A la hora de eliminar malware es estrictamente necesario que el proceso de limpieza 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

En la prueba llevada a cabo en abril/mayo de 2016, AV-TEST utilizó el siguiente software en su versión más actual:

- 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), inclusive todos los parches y hotfixes disponibles a 1 de mayo.

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 estándar, 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.** Durante el proceso de Remediation debían utilizarse todas las funciones del producto disponibles.
    a. Se debía procurar instalar el producto de seguridad con la configuración estándar. Se debían seguir en su totalidad 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, hasta qué punto 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 estas drásticas medidas no sean necesarias para llevar a cabo con éxito el proceso de Remediation. El uso de estos métodos supone la pérdida de puntos en la valoración.

Valoración de la efectividad

Por cada muestra de malware se otorgaron puntos siguiendo 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 qué técnica de las disponibles se utilizó 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 con los que se podía infectar Windows 7 (SP1, 64 bits).

Resultados de la prueba

En la primera fase de la prueba, el producto de Enigma Software Group obtuvo un resultado muy bueno y solo dejo en una ocasión restos de archivos en el sistema. En la segunda fase de la prueba, SpyHunter obtuvo 55 de los posibles 60 puntos. Ambos resultados aparecen representados en el gráfico 2.

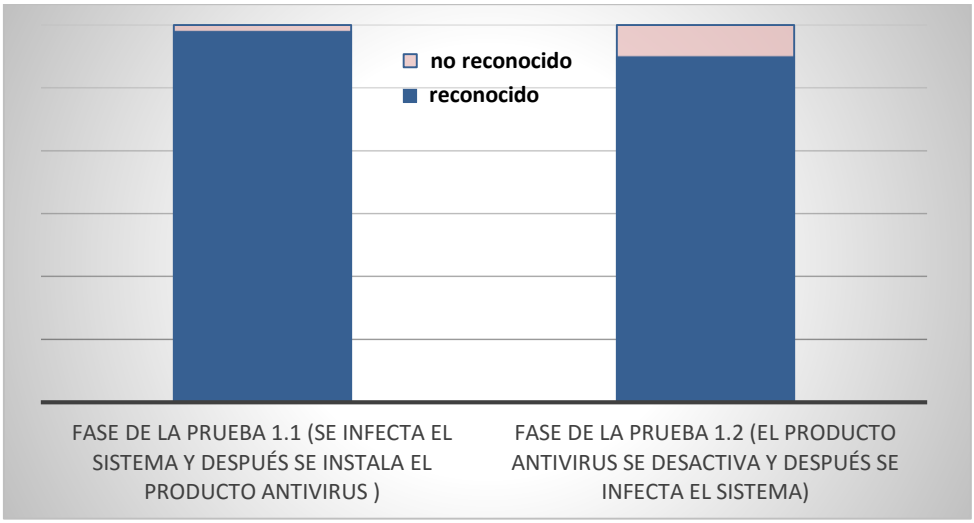
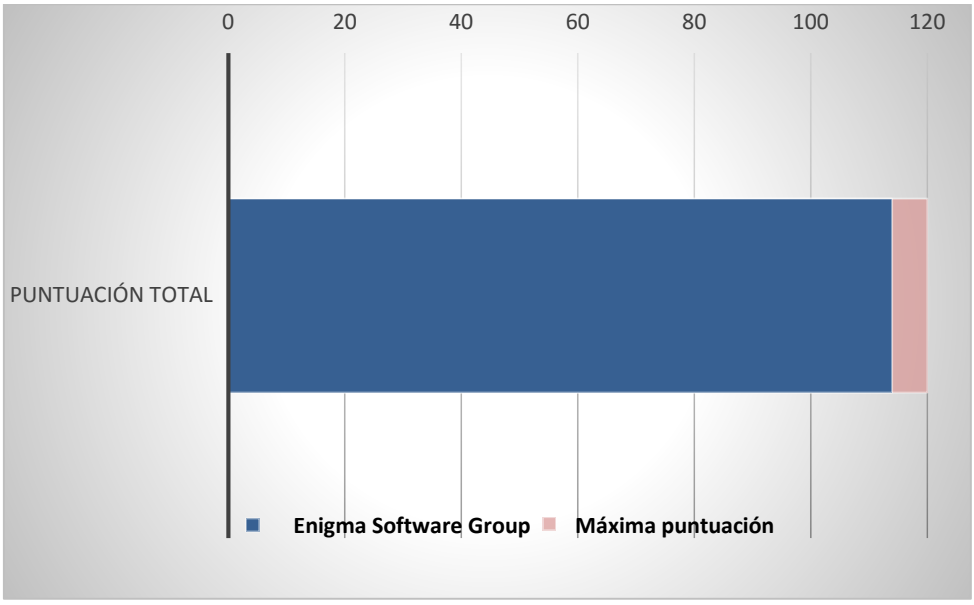


Gráfico 2: Resultado de la prueba Remediation: fases 1.1 y 1.2

La puntuación máxima que se podía obtener en la prueba era de 120 puntos. La puntuación total alcanzada por Enigma Software Group fue de 114 puntos, como muestra el gráfico 3. En cuanto al rendimiento referente a la limpieza, durante la segunda fase de la prueba se constató que no se habían eliminado por completo algunas infecciones. SpyHunter eliminó los componentes activos del malware que se hallaba en el ordenador. La mayoría de los restos de archivos eran archivos ejecutables del programa malicioso que habían sido almacenados en el sistema en la carpeta "C:\Users\vtc\AppData\Roaming\". SpyHunter no fue capaz de tratar los componentes activos del malware en un solo caso y el sistema permaneció infectado.

En la fase 1.1 de la prueba, no obstante, el producto obtuvo un resultado muy bueno y solo se permitió un fallo.



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	4.22.4.4657	2016.04.26v1

Lista de las muestras de malware utilizadas (prueba Remediation)

(SHA256)
0x026bb4f1db988785351ab7d3889c3b322b69398042ae7d52e8e4740e9618eec1
0x02c6d5aeb2ab78f781d72ba60d6f7ff7f5928d47a26ca8dcc4a5c1398850e62a
0x1e3a054ed8051c06a78dc37922c2297a5c3da51a84beb99bc2a487381851ede4
0x1eaef8613ab91e13484646dcb61f5721858066850124a7de5ffce2767bad2ff0
0x2164f112693ab13ef45f159a0444ea64b94942518e829aa55b7d277722b87179
0x2656834a0380bc4c830daef09cfafd038fd5e7727303b09170a8fe37c35a1e34
0x32f0a426e80fb26d098a22bf624d3fb21342372a2135337e9f06ffc4af442846
0x3436da965e7fdbde9a9836acc712ff437d5e7c49a821366451308e11555924f1
0x406ada699acb288bfa2755a9ebe807aa86b90f475b332799f925d85b0d195c61
0x443660d22f3c4bfdb2c2ff4d3e25dafd01f7002bcde53ad7bac8b777e700123a
0x56e24a3dc8b07ea6e08e3d4e4ba96e1e9101aca932523c34350fafbcff02ac85
0x5c596c8afd4656946f0a9741f2be4bb088dda26f1ddcf41eb8c427fbb6d1c3ec
0x60eeb661ad33aa50d9ce1355f9e70afde317411f81e7d0890f38ae28ea79b1b4
0x659896ed065fd59fb843022022a7796ec76620000c7c29a009c7f399898845cb
0x70b64248b23182827c8f52be598a4a10bf0784dc1d97e8721a528ec9cec3acc9

0x76c9c0758ea91e38f8cf47fcc01d597a213eed5f2001ff5f8f7763df236e6baf
0x882ac415de83252554349e3221c7bb5028da1db36b55f196f3cf0a9861ef4597
0x95a1d1207cc0a75eaaeef1a985b8c8bbe15a314c43f2b4d593033cf426bb9212
0x9a679f8745896abd8fbe1586eabc3690858f6d966f4a9c5eb52b6f3b64cd35dd
0xa3efd281adaf729075ee466793fe2a2a6972b746d15e9578355957fc7e7daee2

Tel. +49 391 6075460, Fax +49 391 6075469, Internet http://www.av-test.org