Informe del ensayo de reparación

El ensayo fue realizado a requerimiento de la EnigmaSoft Limited por la AV-TEST GmbH
Fecha del informe: 03 de Septiembre de 2018, última actualización con fecha del 04 de Septiembre de 2018

Resumen

En agosto de 2018 la AV-TEST realizó un ensayo para averiguar la capacidad de reparación de SpyHunter de la EnigmaSoft Limited. El ensayo se realizó en un sistema operativo limpio del tipo Windows 10 (RS3, 64 Bit) utilizando el mismo imagen de disco en varios ordenadores idénticos.

El malware para el ensayo de reparación consistía en 12 muestras divididas en dos partes. Parte 1: Inicialmente fue infectado el imagen con una muestra de malware. En el siguiente paso fue intentado instalar el programa de protección, escanear el ordenador y eliminar todas las amenazas detectadas. Parte 2: Aquí fue desactivado incialmente el software antivirus para poder infectar el sistema. Entonces el software antivirus fue reactivado y fue realizado un reinicio para garantizar el funcionamiento correcto de todos los componentes del software antivirus. Después se intentó reparar el sistema y realizar un escaneo adicional del sistema.

SpyHunter obtuvo en ambas partes del ensayo un resultado perfecto de 100%. El software de Enigma limpió todos los componentes activos y extrajo todos los artefactos de malware del sistema.

Descripción

Debido al número creciente de las amenazas publicadas y divulgadas actualmente por el internet, aumenta también el riesgo de que el sistema sufre una infección. Aún hace unos pocos años los nuevos virus sólo aparecieron cada pocos días. Hoy son en cada hora varios miles de nuevas amenazas.

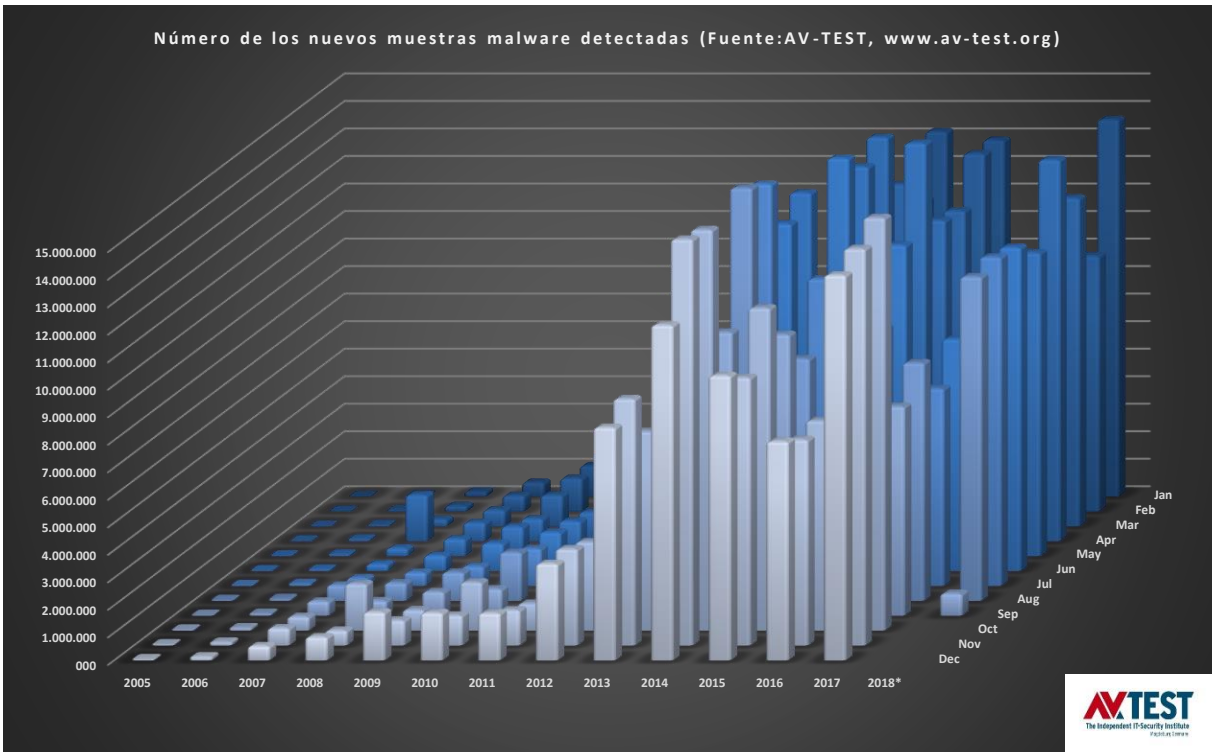


Figura 1: Nuevas muestras por año

En el año de 2000 AV-TEST detectó más de 170.000 nuevos muestras, en 2013 el número de las nuevas muestras ya había subido a más de 80.000.000. En los años sucesivos el número subió más como indica la gráfica en la figura 1. La base de datos de AV-TEST contiene actualmente más de 800 millones de muestras de malware. En el primer semestre del año de 2018 los sistemas de captación de AV-TEST registraron cada mes aproximadamente 10 millones de nuevas muestras.

La cantidad de nuevas muestras tiene que ser procesada por los proveedores de software anti-malware para proteger a sus clientes contra problemas. No siempre es posible proteger a tiempo un ordenador, dado que las firmas sólo son facilitadas cada pocas horas lo que a veces puede ser muy tarde. Infecciones causan pérdidas económicas porque sustrayen datos confidenciales o hacen que el ordenador ya no puede ser usado en forma productiva hasta que el malware fuese eliminado completamente del sistema.

Por eso las técnicas de reparación adquirieron cada vez más importancia para restablecer la utilidad de un ordenador infectado. El uso de tales técnicas implica que el proceso de limpieza resulte confiable de dos maneras:

1. El malware y todos sus componentes tienen que ser eliminados y todas las modificaciones dañinas tienen que ser canceladas
2. Debe ser evitado que las aplicaciones limpias o el propio sistema sufren daños por el proceso de limpieza

Producto ensayado

El ensayo se realizó en agosto de 2018. Para el mismo AV-TEST utilizó la última versión en aquel momento disponible del siguiente software:

- SpyHunter de EnigmaSoft Limited

Metodología y valoración

Plataforma

Todos los ensayos se realizaron en ordenadores idénticos provisto del siguiente hardware:

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

El ensayo se realizó en agosto de 2018. Para el mismo AV-TEST utilizó la última versión del siguiente software que estaba disponible en el momento del ensayo.

Metodología del ensayo

El ensayo de reparación se dividió en diez pasos según el método abajo descrito:

1. **Sistema limpio para cada muestra**. Los sistemas ensayados fueron puestos en un estado limpio antes de exponerlos a una de las muestras de malware.
2. **Ordenadores físicos**. Los sistemas utilizados para el ensayo fueron auténticos ordenadores físicos. No fueron utilizados ordenadores virtuales.
3. **Acceso al internet**. Los ordenadores tenían a cada momento acceso al internet para recurrir en su caso a consultas In-the-Cloud.
4. **Configuración del producto**. Todos los productos y sus correspondientes herramientas de reparación o herramientas de restablecimiento reiniciables funcionaron con las configuraciones estándard predefinidas.
5. **Infección de los ordenadores ensayados**. Un ordenador nativo fue infectado con una amenaza y entonces reiniciado. Tuvo que ser garantizado que la amenaza funcionaba plenamente.
6. **Familias modelo y payloads**. Las muestras ensayadas no eran de la misma familia ni tenían los mismos payloads.

7. **Reparación con utilización de todas las capacidades disponibles del producto**.
    a. Intentar la instalación del producto de seguridad con todas las configuraciones estándard. Asegurarse que sean observadas todas las instrucciones del producto necesarias para la eliminación.
    b. Si a. no funcione, intentar una solución con la herramienta ***stand-alone fix/recuperación*** (si disponible).
    c. Si b. no funcione, intentar la **solución del inicio** stand-alone (si disponible) y utilizar la misma para la reparación.
8. **Validación de la eliminación.** El ordenador fue inspeccionado en forma manuel para poder validar la correcta eliminación y la existencia de artefactos.
9. **Valoración de la capacidad de eliminación**. La eficiencia de la herramienta y de la solución de seguridad en su totalidad fue comprobada mediante el sistema de valoración previsto.
10. **Reparación demasiado agresiva**. El ensayo analizó también la agresividad de un producto durante la reparación. Por ejemplo hay productos que eliminan el archivo host o un directorio en su totalidad, aúnque no hubiera sido necesario para una reparación exitosa. Un tal comportamiento desvalora el producto.

Clasificación de la eficiencia

Para cada muestra ensayada se da puntos según el siguiente sistema:

a. Malware completamente eliminado (3)
b. Malware detectado y eliminado, sólo sobran vestigios inactivos (2)
c. Fue detectado algo y parcialmente eliminado, pero los vestigios del malware se mantienen todavía activos (1)
d. Malware no fue detectado y no fue elimiado nada (0)

En la valoración no debia ser considerado cual de las técnicas disponibles era necesaria para eliminar el malware. No obstante debieron ser aplicadas todas las técnicas. Si un producto elimine en el archivo host todas las entradas correspondientes a este producto, limpie el ordenador de infecciones y deje el producto en un estado de funcionamiento y actualizable, debe recibir la puntuación completa, aún cuando queden entradas en el archivo host para otros proveedores de sistemas de seguridad

Muestra

El conjunto consistía en 12 archivos dañinos que tenían la capacidad de infectar Windows 10 (RS3, 64 Bit).

Resultados del ensayo

EnigmaSoft Limited alcanzó en ambas partes del ensayo un resultado perfecto de 100 %.
Los resultados de las dos partes del ensayo se muestran en la figura 2.

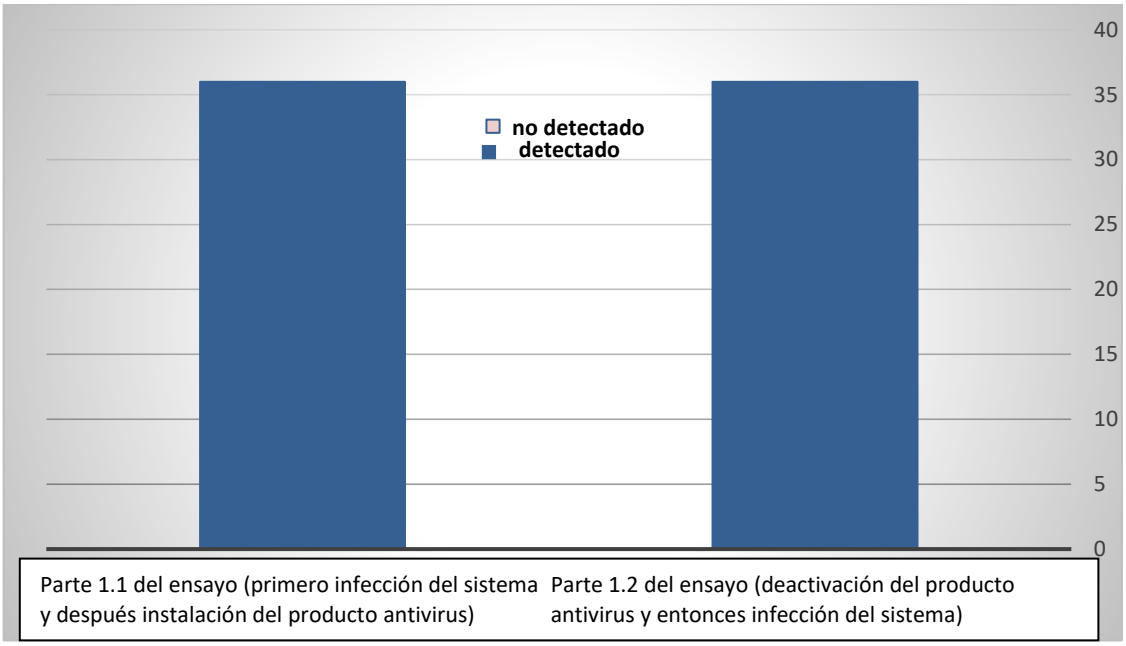
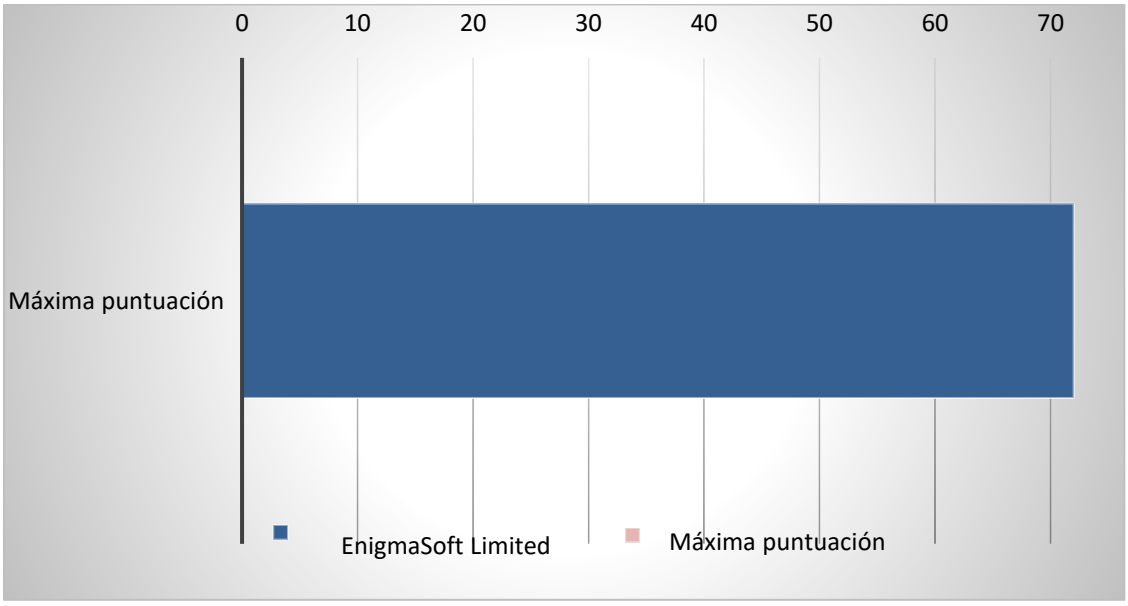


Figura 2: Resultado de la reparación – Partes 1.1 +1.2 del ensayo

En lo que se refiera a la capacidad de limpieza, SpyHunter pudo limpiar el sistema de todos los 12 muestras ensayadas. Además fueron eliminados perfectamente todos los artefactos y elementos de registro.

La puntuación máxima fue 72. Como se ve en la figura 3, la EnigmaSoft Limited alcanzó el resultado sorprendente de 72 puntos.



Anexo

Versión del software ensayado

Diseñador, Distribuidor	Denominación	Versión
EnigmaSoft Limited	SpyHunter 5	5.0.30.51

Relación de las muestras utilizadas para el ensayo de reparación

(SHA256)
0x0bf737607d46bfa4434a8d62b2376b9fdd4b013bb1614bd5f089fa332feef0b2
0x179cb0ba8030ee09e2e7d5be3a9d0f1b20663a5e1f49e8d1d876b3f76e088476
0x3c5fc8acd9a0ef88795d2592fee6a20be800a3874a40f672700bf23707ca9f82
0x4ff747afb05bc711742f3617d92735a8435eb16c8954dbfe1e558cb7b5de7c3d
0x5400e496f79ad8d09b6be069ca680af2e359f81625993e15fa52a09b1444f78b
0x6287b31e3681973ecfc969ce082cc195badd8f571ce057695a021c9227ee63d4
0x6abef4b7e1d91fc80c7f83cfebffa1ac129333c4acb8e7779bd646a1e66129c3
0x7e8a7fd6bb805f8bd42d30c17490b9bd0a9602485efcb708abfca3e1d5b16c01
0xa058357700d6bbec06232492c40a88487f57e343f7a7c6180582b4d83714f1bd
0xc3519c9fc77812b3ad088174729fc3f712de69505659f73e4d277af6b4ba31ab
0xe67ddfdfdca394eb8a4ebf7fe64c7dc7459df1b3b050e680ce94ab51a2e54c0c
0xf4e496f3a1d094eddf13a93e92e22dbc6a224aa8e8e8664fdf7fdbb4b456485c