Informe sobre la prueba comparativa Remediation

AV-TEST GmbH realizó la prueba comparativa por encargo de Enigma Software Group
Informe del 10 de mayo; actualizado el 24 de mayo de 2017

Resumen

En marzo de 2017, AV-TEST comprobó en una prueba comparativa las funciones y capacidades 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 21 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.

En la primera fase de la prueba, SpyHunter consiguió un resultado casi perfecto del 98% y fue capaz de eliminar todos los componentes activos del malware. Solo en una ocasión permaneció en el sistema la aplicación generada por un malware. Los siguientes tres productos sometidos a la prueba, Emsisoft Anti-Malware, Malwarebytes Free y Malwarebytes Premium, también la superaron con éxito, obteniendo resultados del 92-93%, mientras que Spybot Search & Destroy y IObit Malware Fighter se quedaron muy atrás con un 40% y un 10% respectivamente.

Tras la evaluación de la segunda fase de la prueba se obtuvo una imagen muy semejante a la de la primera parte en cuanto a la valoración de los productos: SpyHunter volvió a alcanzar un resultado muy bueno de un 97%, neutralizando todos los componentes activos del malware y dejando solo una entrada de inicio en el registro, así como las aplicaciones creadas en el sistema. Emsisoft Anti-Malware, Malwarebytes Free y Malwarebytes Premium volvieron a obtener una buena valoración del 92-93%. A la cola quedaron de nuevo Spybot Search & Destroy y IObit con magnitudes del 40% y el 10%.

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.

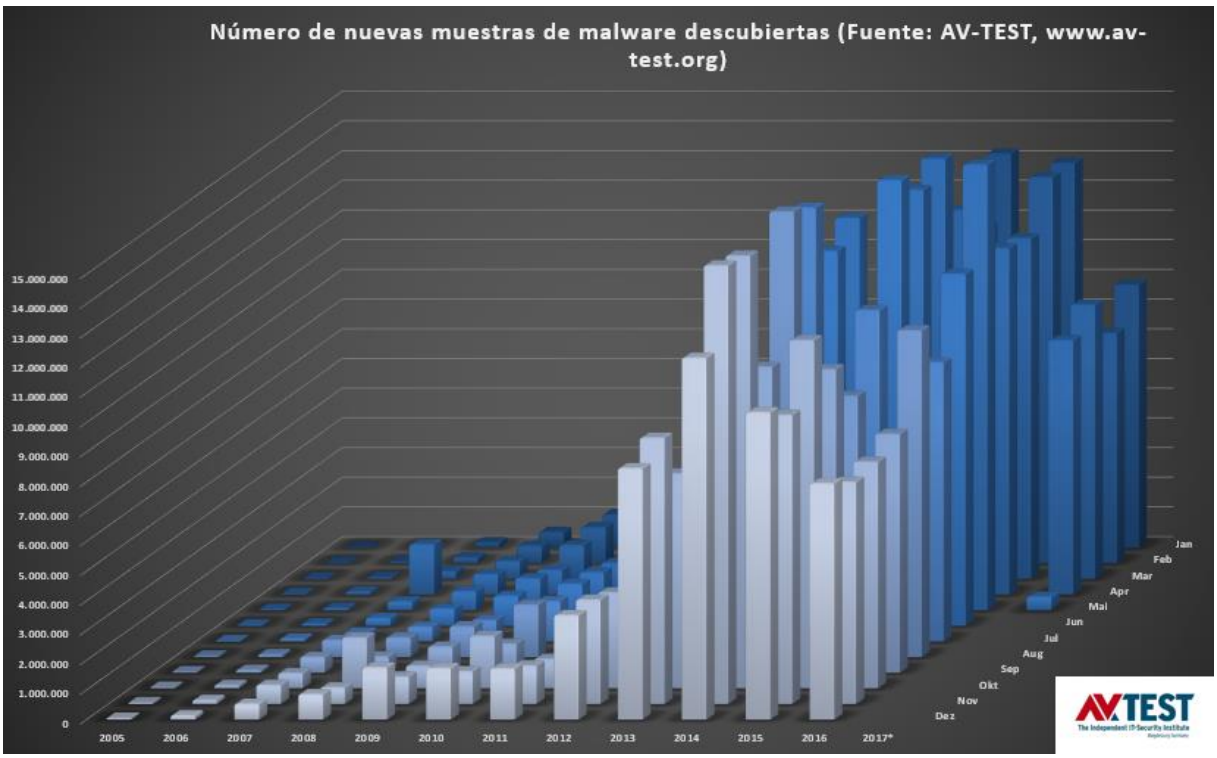

Gráfico 1: Nuevas muestras de malware al año

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 630 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 marzo 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, 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 prueba abarcaba 21 programas maliciosos capaces de infectar Windows 7 (SP1, 64 bits).

Resultados de la prueba

SpyHunter obtuvo la mejor puntuación en esta prueba comparativa con 123 de los 126 puntos posibles, seguido de los dos productos de Malwarebytes, que también consiguieron un buen resultado con 118 puntos, asegurándose el segundo puesto.

Emsisoft Anti-Malware les siguió de cerca con una puntuación también buena de 116 puntos. Con un total de 50 puntos, Spybot Search & Destroy obtuvo un flojo resultado, mientras que la puntuación de IObit Malware con apenas 12 de los 126 puntos posibles solo puede calificarse de pésima.

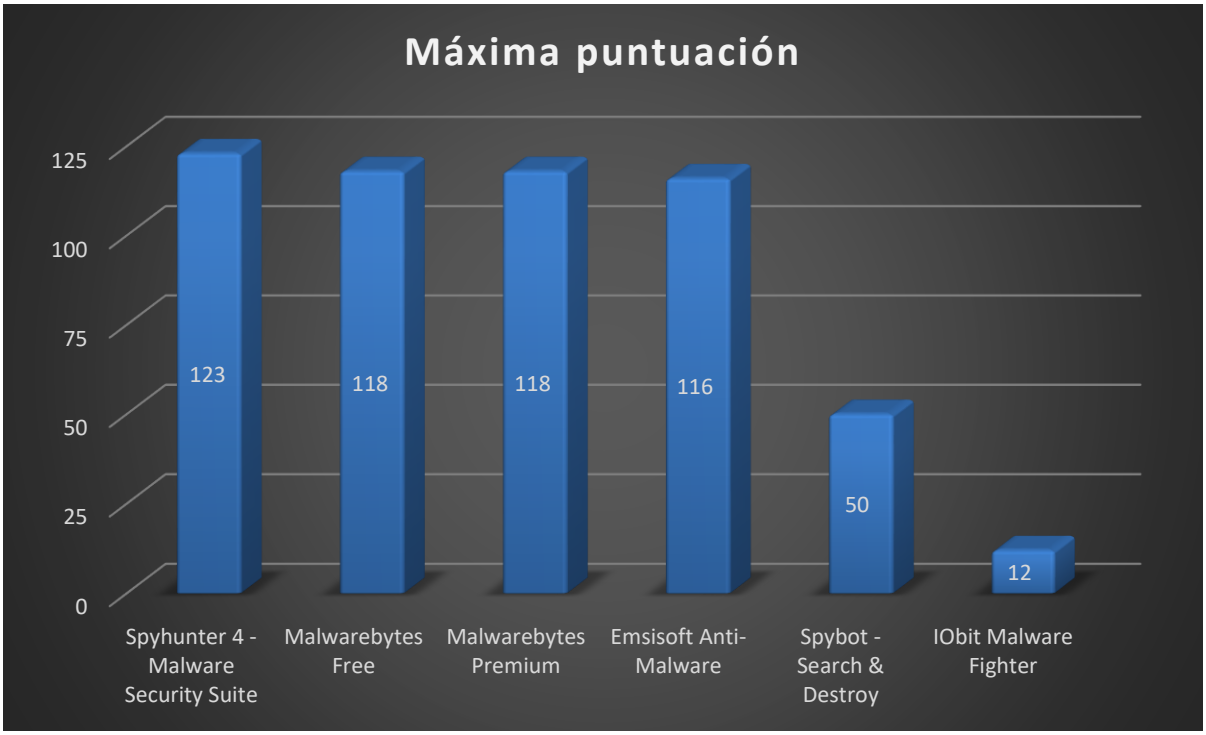

Gráfico 2: Resultado conjunto de la prueba de Remediation: fases 1.1 y 1.2

Grafiktext: Resultado conjunto
x-Achse (korrigieren): SpyHunter Spybot Search & Destroy

En los gráficos 3 y 4 se ve claramente que los resultados de las fases 1 y 2 son prácticamente idénticos. La puntuación máxima que podía conseguirse en cada una de las etapas de la prueba era de 63 puntos.

SpyHunter obtuvo en la primera y la segunda fase de la prueba 62 y 61 puntos respectivamente y, por tanto, un excelente resultado. En ambas pruebas, el programa dejó en el sistema una aplicación y en la segunda fase además una entrada en el registro.

Con 59 puntos por prueba, las dos versiones de Malwarebytes obtuvieron un buen resultado total, a pesar de que en una ocasión no consiguieran eliminar el malware y dejaran componentes activos del malware en el sistema. Emsisoft Anti-Malware se aseguró el tercer puesto con 58 puntos en cada prueba; el programa borró todos los componentes activos de las 21 muestras de la prueba y solo dejó en el sistema una aplicación y entradas en el registro.

Spybot Search & Destroy fue capaz de eliminar menos de la mitad de las muestras de malware y por ello solo obtuvo 25 puntos tanto en la fase 1 como en la 2.

La peor puntuación fue la obtenida por IObit con solo 6 puntos por prueba; el programa no pudo eliminar a 18 de las 21 muestras de malware.

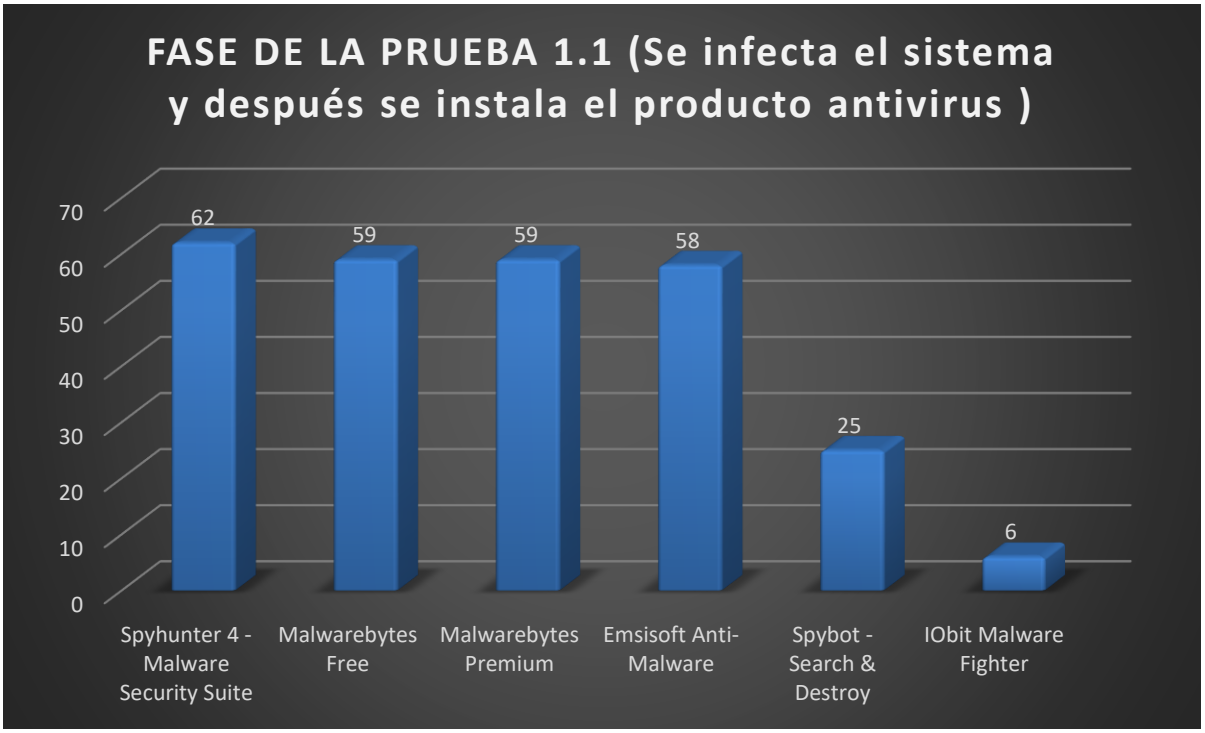

Gráfico 3: Resultado de la prueba de Remediation: fases 1.1 y 1.2

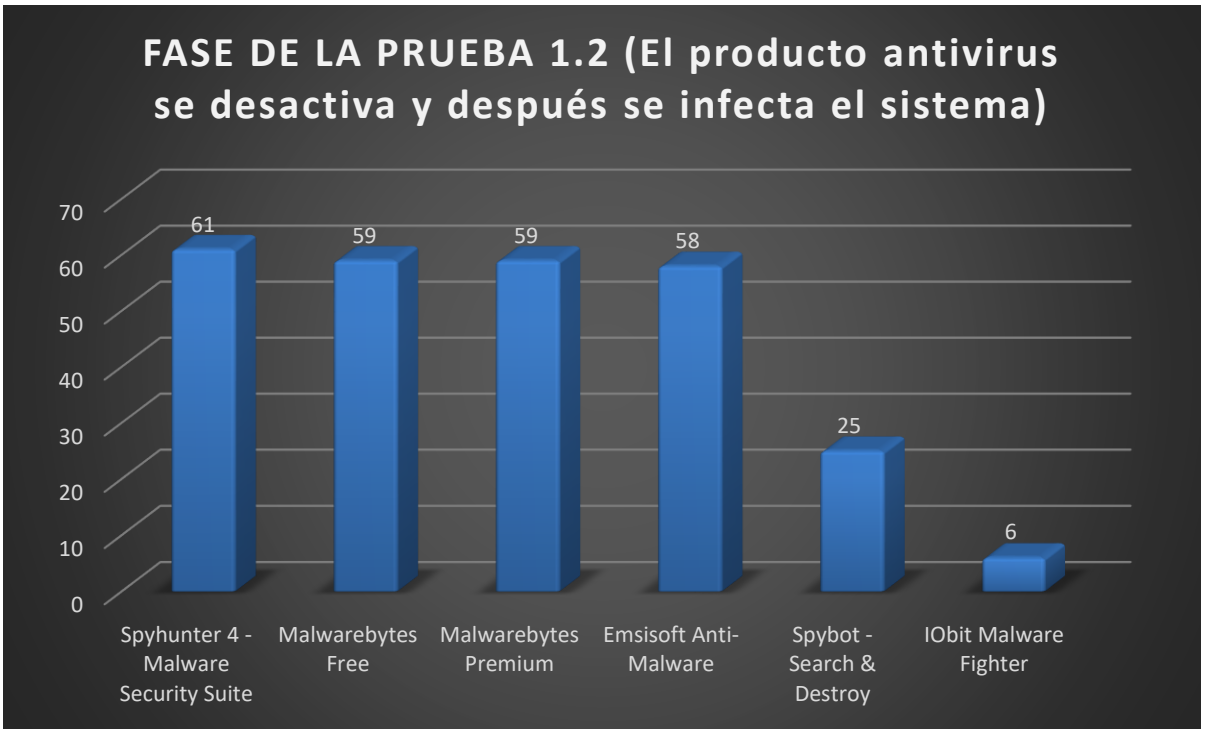

Gráfico 4: Resultado de la prueba de Remediation: fases 1.2 y 1.2

Anexo

Información sobre la versión del software sometido a la prueba

Desarrollador, fabricante	Denominación del producto	Versión del programa	Motor/versión de la firma
Emsisoft	Anti-Malware	2017.2.1.7260	4.0.1.856/20170324
Enigma Software Group	SpyHunter 4	4.24.3.4750	2017.01.17v01
IObit	Malware Fighter	4.5.0.3457	1634
Malwarebytes	Malwarebytes Free	3.0.6.1469	n/a
Malwarebytes	Malwarebytes Premium	3.0.6.1469	n/a
Safer Networking	Spybot Search & Destroy	1.6.2.46	n/a

Lista de las muestras de malware utilizadas en la prueba Remediation

(SHA256)
* 0x0101d4a72a3685aaf8a7baa4408223914ba7f1c8d193628fabbe98cd377536cd
* 0x01168762ca9a57ffe5b69371b85d7d60339a3a95091554e87750715fc146313d
* 0x0bf7ab1fd378c78ea8206c84dfa780c472d84c5357238d78df369881f762ad99
* 0x246082bd340133a0b634ef874a20f9823336fc3e65baddaddc57c3af5588a35a
* 0x369fab397bbc2ca10601c3ca89f77b24eecf485b080f07d820daf8a6487554a2
* 0x3b56fcb59462dac54bee27b85bc8e29af286d0349909aa9a313868e8be5c96bd
* 0x453442bc8fd9e0fec64febb1c7c81cc1daecc151faa0aa30041b25296b906423
* 0x454ecf8d9846abae025fa57f097fa6bc11b3ac7bd68b9a1c2eb55bc6861b3d4c
* 0x4b91c4e2f69697a888b56147f69d4c96ca13095a2aaf640a48e68994c7228565
* 0x4da0d3e569ceeced62b7128ed35c55cfb48236be628ba64411f066a9a38a5aff
* 0x4e59b6263b5b3a5ce4ea5054dc48cca37945ca930ad1a5aa300029539d8042a3
* 0x6a9936983ee1bc49d5fff7e2ae6435462667c7f62547a710297b8f9c86a36873
* 0x7021df3d38a24a1de948ef5c820b60d8e61c95ed3409c255680eba79e4221123
* 0x7a1e9db7fe1bc6341b1e1a002c19ca6f32224aa0c4eb6582d984d66bb44f339e
* 0x8f995f37b1aee61018742c35ab410820b02982fe2ac0b9a2554d02909f2590a2
* 0x9643447291f6e468611c8acb6e58f8e3b3c40a3394e4f7d5c20489a9af0e0750
* 0xc0d110efbd58448c8fed7e249a3e5503185cd3f2fc4a13339874646256877f9e
* 0xda3458870afb6487c435129bd1ac4c8b994c2133d3790ca505949cc2644293bf
* 0xee7e9a572dd14739aaf6cc16f1d52e66b62347f1902a2c93a9145ab9c0f29d83
* 0xf6c186da15892176e8f8cd31e9dd637024a4e4e08510315011d6d735a32f2c93