AV Evasion with Shellter

What is Shellter?

Shelter is an open-source tool that allows us to create and execute malicious payloads while evading detection by AV software. It works by leveraging various techniques, such as process hollowing, DLL injection, and reflective DLL injection, to execute code in memory without writing it to disk.

Lets start by installing shelter

```
sudo apt install shellter
```

Now lets install the required dependencies

```
sudo apt install wine

dpkg --add-architecture i386

sudo apt update

sudo apt install wine32
```

- Now that we are done with the installation. Lets execute the shellter command, it will provide us with a new console running under wine.

```
shellter
```

Shellter can run in either *Auto* or *Manual* mode. In Manual mode, the tool will launch the PE we want to use for injection and allow us to manipulate it on a more granular level. We can use this mode to highly customize the injection process in case the automatically selected options fail.

For the purposes of this example however, we will run Shellter in Auto mode by selecting **A** at the prompt.

Next, we must select a target PE. Shellter will analyze and alter the execution flow to inject and execute our payload.

For this example, we are taking VLC media player 32 bit executable installer.

You can get it from here - https://www.videolan.org/vlc/download-windows.html

As soon as Shellter finds a suitable place to inject our payload, it will ask us if we want to enable *Stealth Mode*. which will attempt to restore the execution flow of the PE after our payload has been executed.

At this point, we are presented with the list of available payloads. These include popular selections such as Meterpreter, but Shellter also supports custom payloads.

Let choose the meterpreter reverse TCP payload.

With all of the parameters set, Shellter will inject the payload into the VLC installer and attempt to reach the first instruction of the payload.

Now that we have successful injection our shellcode into the VLC installer. Lets check our create payload in Virustotal

VirusTotal is a free online tool that helps you check if a file or website is safe from viruses, malware, and other harmful content.
