Simple Obfuscation with PowerShell using Base64 Encoding

Jun 15, 2017 · POWERSHELL · Share on:

I recently received a question from someone wanting to know how I encoded a string of text on my blog site. Back in January of 2013, I competed in Jeff Hicks PowerShell Challenge that was held by TrainSignal. One of the questions had an encoded command which you were to decode. I figured out that the `EncodedCommand` parameter of `PowerShell.exe` could not only be used to run commands that are encoded with Base64, that it could also be used to easily decode a string of text that was encoded with Base64.

```batch
powershell.exe /?
```

```
...
-EncodedCommand
    Accepts a base-64-encoded string version of a command. Use t
    to submit commands to Windows PowerShell that require compl
    marks or curly braces.
...
```

The help for `PowerShell.exe` also shows you how to encode a command with Base64:

Mike F. Robbins

Scripting | Automation | Efficiency

READ MORE

Disclaimer

All information and code on this site is for informational purposes only and provided as-is. This site does not provide any warranty, either express or implied. All thoughts and opinions are my own.

Recent Posts

- How to install PowerShell 7 and

```
...
    # To use the -EncodedCommand parameter:
    $command = 'dir "c:\program files" '
    $bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
    $encodedCommand = [Convert]::ToBase64String($bytes)
    powershell.exe -encodedCommand $encodedCommand
```

Encoding something like the domain name for this blog site is easy enough:

POWERSHELL
```
[Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBy
```

```
JwBtAGkAawBlAGYAcgBvAGIAYgBpAG4AcwAuAGMAbwBtACcA
```

While it could be decoded within PowerShell:

POWERSHELL
```
[System.Text.Encoding]::Unicode.GetString([System.Convert]::Fro
```

```
'mikefrobbins.com'
```

Adding quotes around the domain name also allows it to be decoded with `PowerShell.exe` using the `EncodedCommand` parameter without having to encode it with a command such as `Write-Output`:

BATCH
```
powershell.exe -encodedCommand JwBtAGkAawBlAGYAcgBvAGIAYgBpAG4AC
```

essential tools on Linux

- How to install PowerShell 7 and essential tools on Windows 11
- Find paired Azure region locations with Azure PowerShell
- Understanding the Clean block in PowerShell
- Detecting Windows Terminal with PowerShell
- How to resolve winget is unable to find or install packages
- Check out someone else's pull request using the GitHub CLI
- Generating PowerShell module documentation with platyPS

Categories

POWERSHELL 347

ACTIVE DIRECTORY 34

SCRIPTING GAMES 32

```
mikefrobbins.com
```

The code shown in the previous example specifies the `NoProfile` parameter but it's not required.

µ

SQL SERVER 20
DESIRED STATE CONFIGURATION 18
AZURE 13
HYPER-V 10
LINUX 9
VSCODE 9
POWERSHELL SUMMIT 8
GIT 6
IIS 6
OFFICE 365 6
PESTER 6
AZURE POWERSHELL 5
WINDOWS 10 5
ARCOLINUX 4
AST 4
ALL CATEGORIES

Tags

POWERSHELL 340
ACTIVE DIRECTORY 32

SCRIPTING GAMES 30

SQL SERVER 21

DSC 19

DESIRED STATE CONFIGURATION 18

AZURE 13

HYPER-V 11

VIDEO 11

PESTER 10

LINUX 9

VSCODE 9

AST 8

POWERSHELL VERSION 5 8

GIT 7

IIS 6

OFFICE 365 6

POWERSHELL SCRIPT MODULE DESIGN 6

ALL TAGS