

Write-HijackDll

SYNOPSIS

Patches in the path to a specified .bat (containing the specified command) into a pre-compiled hijackable C++ DLL writes the DLL out to the specified ServicePath location.

Author: Will Schroeder (@harmj0y)

License: BSD 3-Clause

Required Dependencies: None

SYNTAX

```
Write-HijackDll [-DllPath] <String> [[-Architecture] <String>] [[-BatPath] <String>] [[-Password] <String>] [[-LocalGroup] <String>] [[-Credential] <PSCredential>]
```

DESCRIPTION

First builds a self-deleting .bat file that executes the specified -Command or local user, to add and writes the .bat out to -BatPath. The BatPath is then patched into a pre-compiled C++ DLL that is built to be hijackable by the IKEEXT service. There are two DLLs, one for x86 and one for x64, and both are contained as base64-encoded strings. The DLL is then written out to the specified OutputFile.

EXAMPLES

Example 1

```
PS C:\> {{ Add example code here }}
```

{{ Add example description here }}

Home

Recon

About

Functions

Export-PowerViewCSV

Resolve-IPAddress

ConvertTo-SID

ConvertFrom-SID

Convert-ADName

ConvertFrom-UACValue

Add-RemoteConnection

Remove-RemoteConnection

Invoke-UserImpersonation

Invoke-RevertToSelf

Get-DomainSPNTicket

Invoke-Kerberoast

Get-PathAcl

Get-DomainDNSZone

Get-DomainDNSRecord

Get-Domain

Get-DomainController

Get-Forest

Get-ForestDomain

Get-ForestGlobalCatalog

Find-DomainObjectPropertyOutlier

Get-DomainUser

New-DomainUser

Set-DomainUserPassword

Get-DomainUserEvent

PARAMETERS

-DllPath

File name to write the generated DLL out to.

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **True**
Position: **1**
Default value: **None**
Accept pipeline input: **False**
Accept wildcard characters: **False**

-Architecture

The Architecture to generate for the DLL, x86 or x64. If not specified, PowerUp will try to automatically determine the correct architecture.

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **2**
Default value: **None**
Accept pipeline input: **False**
Accept wildcard characters: **False**

-BatPath

Path to the .bat for the DLL to launch.

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **3**
Default value: **None**
Accept pipeline input: **False**
Accept wildcard characters: **False**

-UserName

The [domain\]username to add. If not given, it defaults to "john". Domain users are not created, only added to the specified localgroup.

Home

Recon

About

Functions

Export-PowerViewCSV

Resolve-IPAddress

ConvertTo-SID

ConvertFrom-SID

Convert-ADName

ConvertFrom-UACValue

Add-RemoteConnection

Remove-RemoteConnection

Invoke-UserImpersonation

Invoke-RevertToSelf

Get-DomainSPNTicket

Invoke-Kerberoast

Get-PathAcl

Get-DomainDNSZone

Get-DomainDNSRecord

Get-Domain

Get-DomainController

Get-Forest

Get-ForestDomain

Get-ForestGlobalCatalog

Find-DomainObjectPropertyOutlier

Get-DomainUser

New-DomainUser

Set-DomainUserPassword

Get-DomainUserEvent

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **4**
Default value: John
Accept pipeline input: **False**
Accept wildcard characters: **False**

-Password

The password to set for the added user. If not given, it defaults to "Password123!"

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **5**
Default value: Password123!
Accept pipeline input: **False**
Accept wildcard characters: **False**

-LocalGroup

Local group name to add the user to (default of 'Administrators').

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **6**
Default value: Administrators
Accept pipeline input: **False**
Accept wildcard characters: **False**

-Credential

A [Management.Automation.PSCredential] object specifying the user/password to add.

Type: **PSCredential**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **7**
Default value: [Management.Automation.PSCredential]::Empty
Accept pipeline input: **False**
Accept wildcard characters: **False**

- Home
- Recon
- About
- Functions
 - Export-PowerViewCSV
 - Resolve-IPAddress
 - ConvertTo-SID
 - ConvertFrom-SID
 - Convert-ADName
 - ConvertFrom-UACValue
 - Add-RemoteConnection
 - Remove-RemoteConnection
 - Invoke-UserImpersonation
 - Invoke-RevertToSelf
 - Get-DomainSPNTicket
 - Invoke-Kerberoast
 - Get-PathAcl
 - Get-DomainDNSZone
 - Get-DomainDNSRecord
 - Get-Domain
 - Get-DomainController
 - Get-Forest
 - Get-ForestDomain
 - Get-ForestGlobalCatalog
 - Find-DomainObjectPropertyOutlier
 - Get-DomainUser
 - New-DomainUser
 - Set-DomainUserPassword
 - Get-DomainUserEvent

-Command

Custom command to execute instead of user creation.

Type: **String**
Parameter Sets: (All)
Aliases:

Required: **False**
Position: **8**
Default value: **None**
Accept pipeline input: **False**
Accept wildcard characters: **False**

INPUTS

OUTPUTS

[PowerUp.HijackableDLL](#)

NOTES

RELATED LINKS

[⬅ Previous](#)

[Next ➡](#)

Built with [MkDocs](#) using a [theme](#) provided by [Read the Docs](#).