Lab - How to Disable Microsoft's new UCPD Driver

Overview

Microsoft recently introduced the User Choice Protection Driver (UCPD) into Windows 10 and 11 systems. This driver blocks access to UserChoice Registry keys. The primary purpose of the driver is to force users to use the Microsoft Edge Browser, which is set as the default browser for Windows 10 and 11.

How UCPD Works

The UCPD driver blocks access to certain UserChoice Registry keys by returning access denied.

Microsoft still allows access, but only for processes that pass the following verification:

1. Is the process signed by Microsoft?
2. Is the process on the deny list?

In other words, any third-party program that tries to change default apps, file extension handlines, or protocols on Windows is blocked from doing so.

Lab Requirements:

- One installation of VirtualBox with the extension pack
- One virtual install of Windows 10 Pro

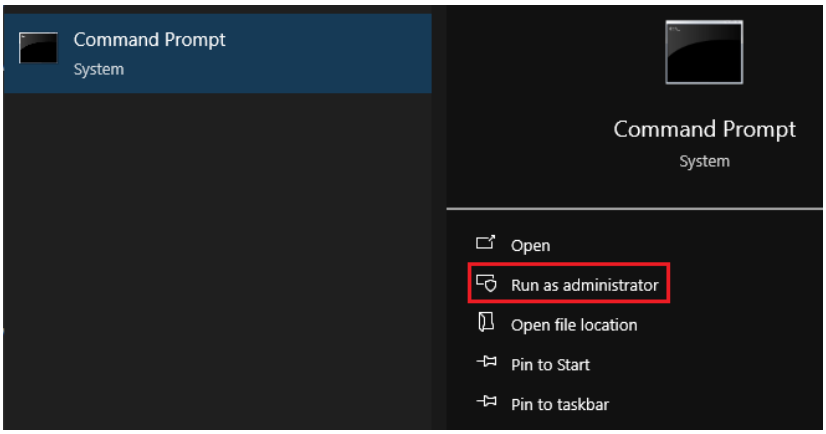
Lab Steps:

1. **Open PowerShell:**

   In the Windows search bar, type `cmd`.

   Select `Command Prompt (Admin)`.



2. Query to see if the UCPD driver is running. At the terminal prompt type:
   `sc query ucpd`

```
C:\Windows\system32>sc query ucpd

SERVICE_NAME: ucpd
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Disable UCDP - sc config ucpd start=disabled

```
C:\Windows\system32>sc config ucpd start=disabled
[SC] ChangeServiceConfig SUCCESS
```

schtasks /change /disable /tn "\microsoft\windows\appxdeploymentclient\ucpd velocity

```
C:\Windows\system32>schtasks /change /disable /tn "\microsoft\windows\appxdeploymentclient\ucpd velocity
SUCCESS: The parameters of scheduled task "\microsoft\windows\appxdeploymentclient\ucpd velocity" have been changed.

C:\Windows\system32>
```

Disable the scheduled task from running

```
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc query ucpd

SERVICE_NAME: ucpd
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Windows\system32>sc config ucpd start=disabled
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>schtasks /change /disable /tn "\microsoft\windows\appxdeploymentclient\ucpd velocity
SUCCESS: The parameters of scheduled task "\microsoft\windows\appxdeploymentclient\ucpd velocity" have been changed.

C:\Windows\system32>
```

End of The lab!