Abusing Windows 10 Narrator's 'Feedback-Hub' URI for Fileless Persistence

- October 19, 2019

Novel Accessibility Feature Abuse technique

While investigating Ease of Access options in Windows 10 for new persistence techniques, I have actually found an undocumented one via 'Provide Narrator feedback' functionality.

Behind the scenes the Narrator feedback consists in launching the custom handler via URI scheme ‘feedback-hub’.

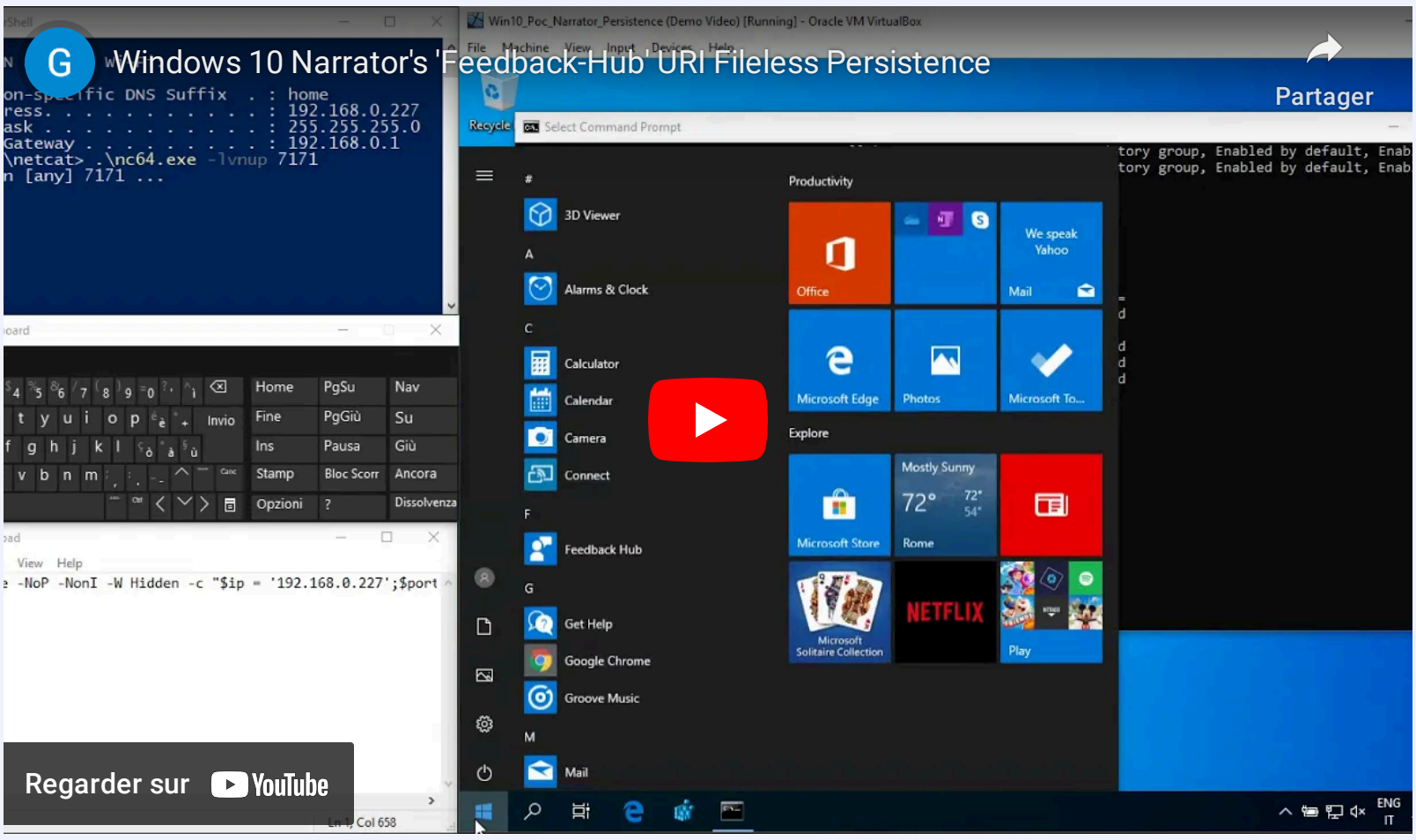
However, in a post exploitation scenario is possible to trivially backdoor this component with fileless payloads hosted in the registry.

Even if there is no security boundary between windows logon screen and the default user desktop (indeed both part of the same window station WinSta0) the possibility of the interaction between the Narrator instance running in the environment of the locked out users and the Windows logon screen opens the chance to trigger the malicious command defined in the registry as soon as the 'Provide Narrator feedback' combination keys are pressed in the latter context.

The novel technique presented in this article has the following advantages in respect to already known Ease of Use abuses (see next paragraph):

- fileless (Living off the Land approach)
- no administrative privileges required (if physical access scenario and victim user is locked out)

Demo video



For the insights, have a look at the documentation for Universal App URI schemes persistence:
https://github.com/giuliocomi/backoori

Quick recap of Accessibility Features for Red Teamers

The Windows Accessibility Features, a set of tools available in the Windows logon screen (like Sticky Keys), are designed to be launched via predefined combination of keys to assist the end users. These Windows features are also quite famous because have been abused by APT groups for backdooring target systems in the past. Having administrative privileges is a requirement in order to replace the genuine Windows binary of the tool ('sethc.exe' or 'narrator.exe', 'magnify.exe', etc.) with an ad-hoc binary.

Overview of the Universal Apps URI schemes persistence

The Accessibility feature is a specific case of the more comprehensive URI persistence technique that affects all Universal Apps URI, which is applicable to every URI protocol listed in the Settings under “Choose default apps by protocol”. Some of these protocols are very interesting, like ‘https’ because in this case it will be possible to trigger the payload from a crafted web pages (with for example an <a> tag link) and the payload will be “MiTM” for the request by executing itself and transparently forwarding the arguments to the legitimate default browser of the unaware victim (for more details have a look at backoori).

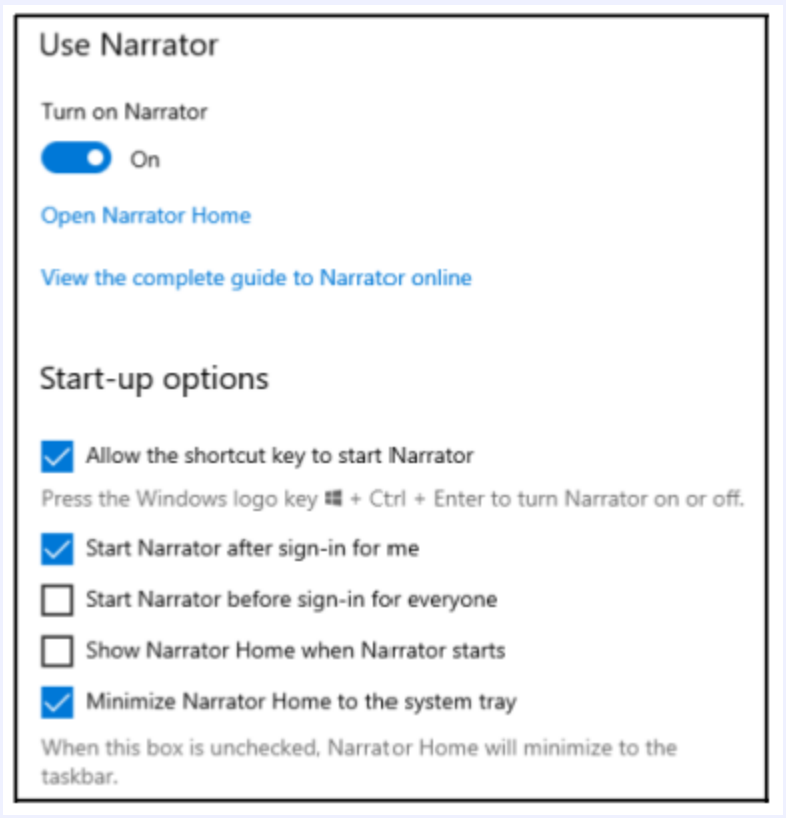
Tweaking Narrator's settings of the compromised user

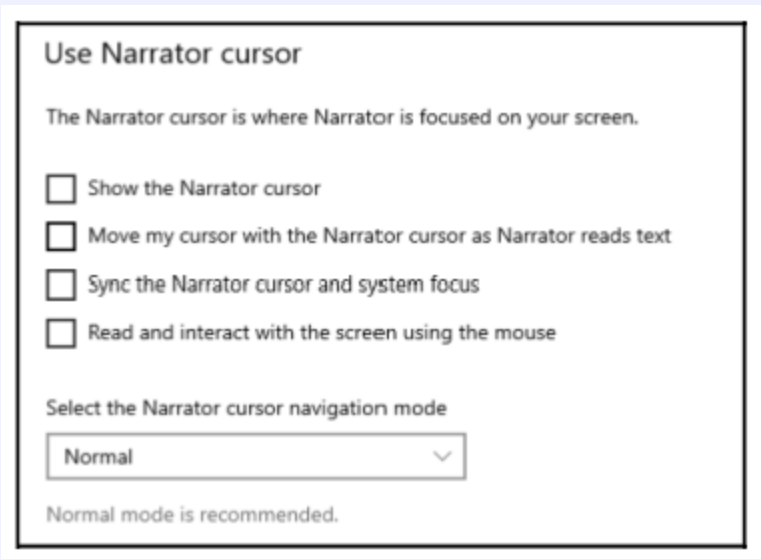
But let’s not digress, the focus of this walk-through is on the Narrator feature abuse.
Every time the ‘feedback-hub’ URI is triggered via:

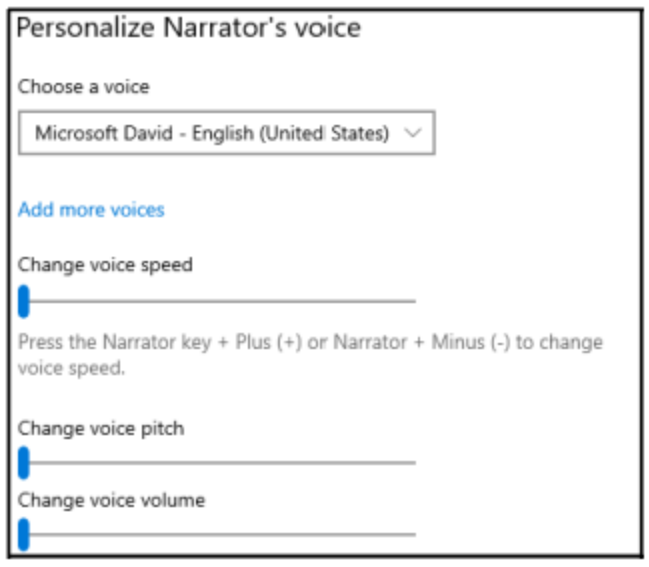
- shortcut key for Feedback Hub in the desktop environment
- the task manager ‘Send feedback’ option
- ‘explorer.exe feedback-hub:’ command
- Narrator Ease of Use feedback in the windows logon desktop

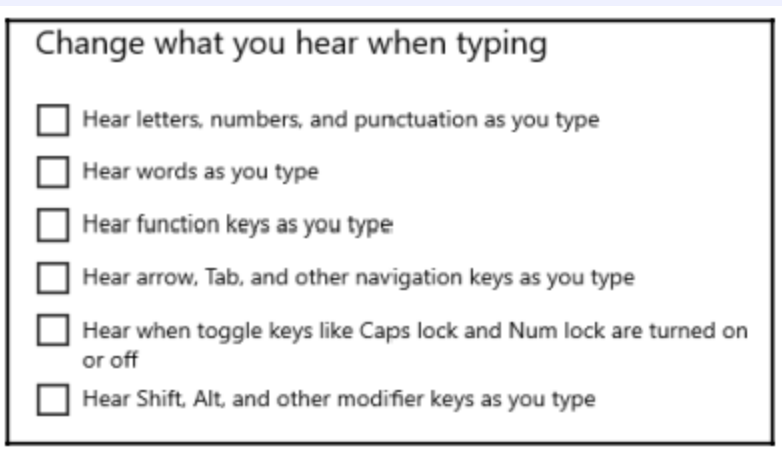
the defined payload will get executed.

For backdooring the last option, the one that involves the Narrator, it is recommended to apply the configuration displayed in the screenshots below. The reason is that the Narrator does not start automatically, it is very loudly and its cursor catches the yes of the victims. Moreover, as said before the Narrator abuse works out of the box for locked out victims (therefore physical persistence), but for signed out users it is necessary to also enable “Start Narrator before sign-in for everyone” with a compromised administrative account.

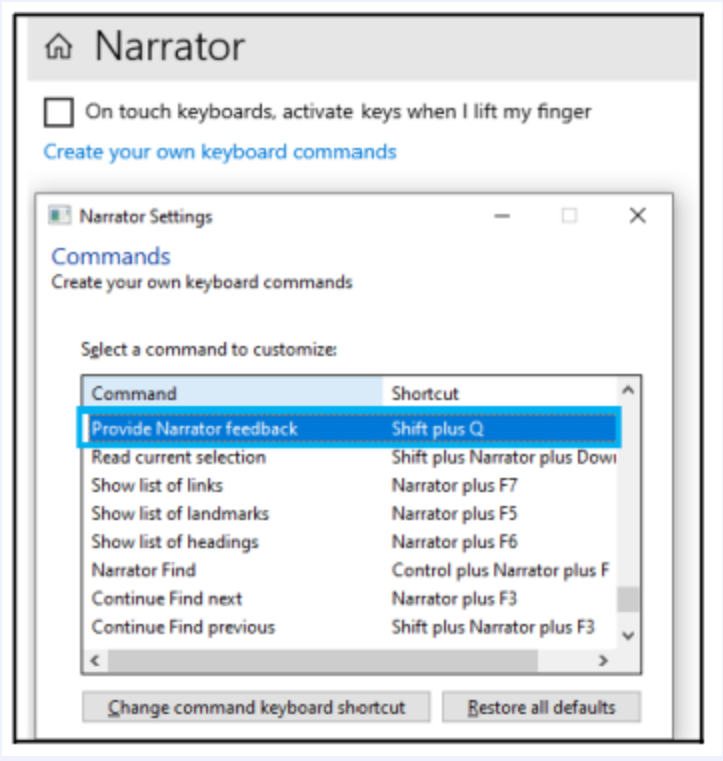








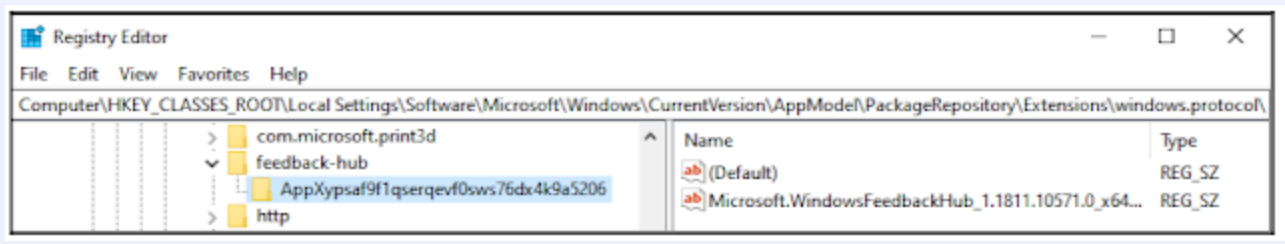
And choose a shortcut key for the ‘Provide Narrator feedback’ setting.



Backdooring ‘Feedback-Hub’ URI functionality

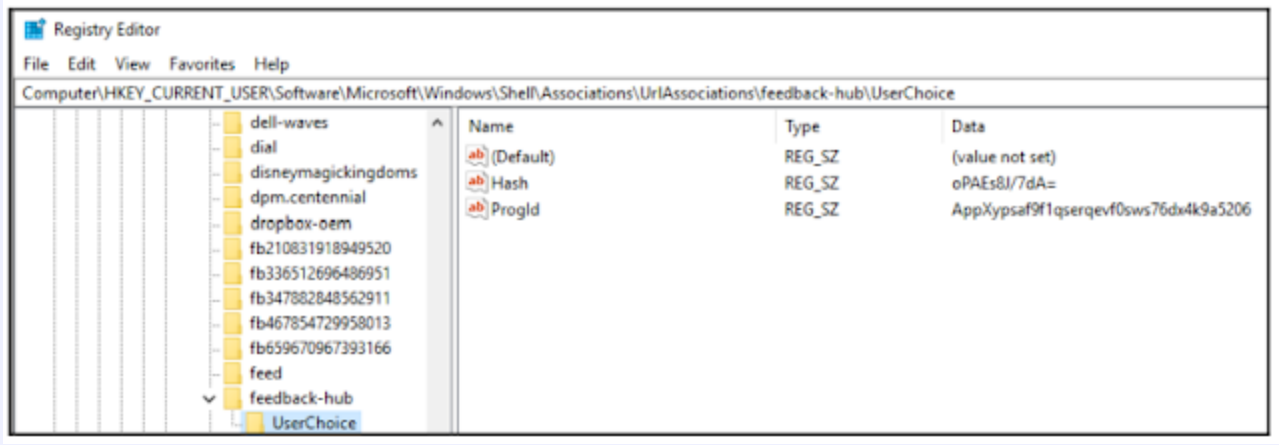
There are two approaches, the expected way is to develop a Universal App and set it as default handler and the more smoothly one based on the editing of registry keys. Let’s focus on the second one.
We need to track down the essential keys to modify in the Registry in order to point the Feedback Hub Microsoft URI scheme to our own payload.
To have a better insights on the few steps involved, have a look at agent_plate.ps1, the agent template part of the tool created as PoC to automate this persistence technique for arbitrary specified URLs.
By looking up the registry for ‘feedback-hub’ key, we find out one registered Universal App Id:

HKCR:Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\windows.protocol\feedback-hub



In case the default handler was already explicitly chosen by the user it will be under key:

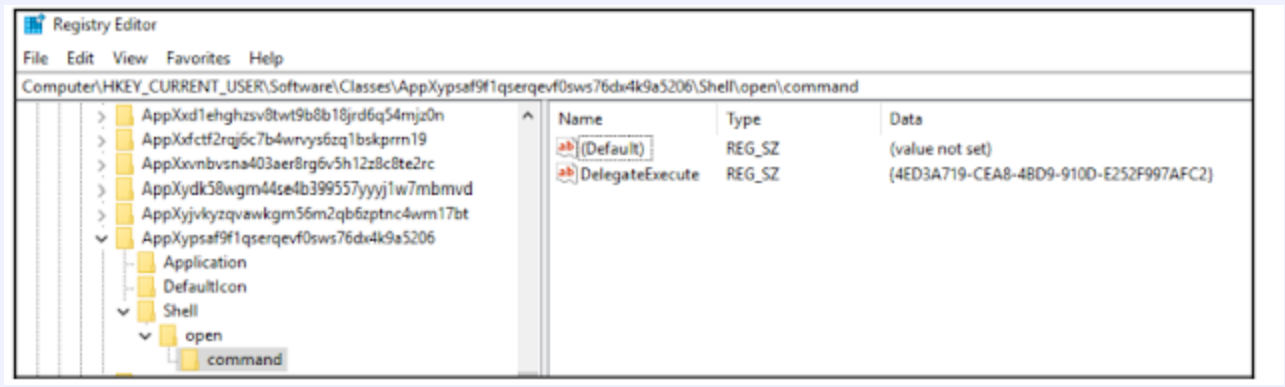
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\feedback-hub\UserChoice



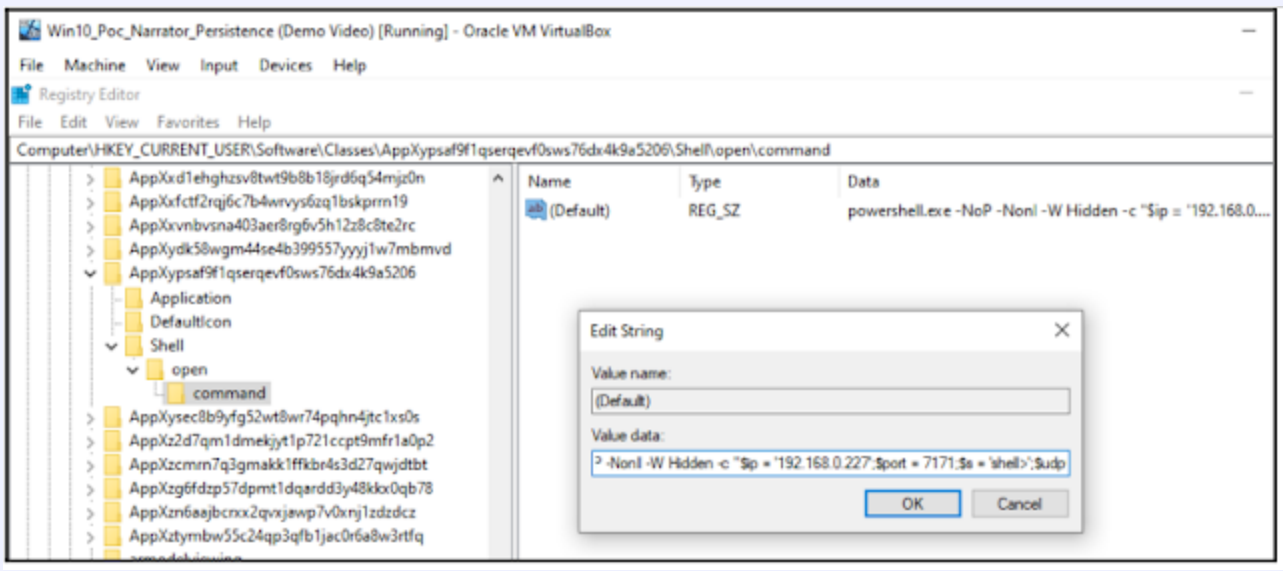
And then again, by looking under

Computer\HKEY_CURRENT_USER\Software\Classes\Appxypsaf9f1qserqevf0sws76dx4k9a5206

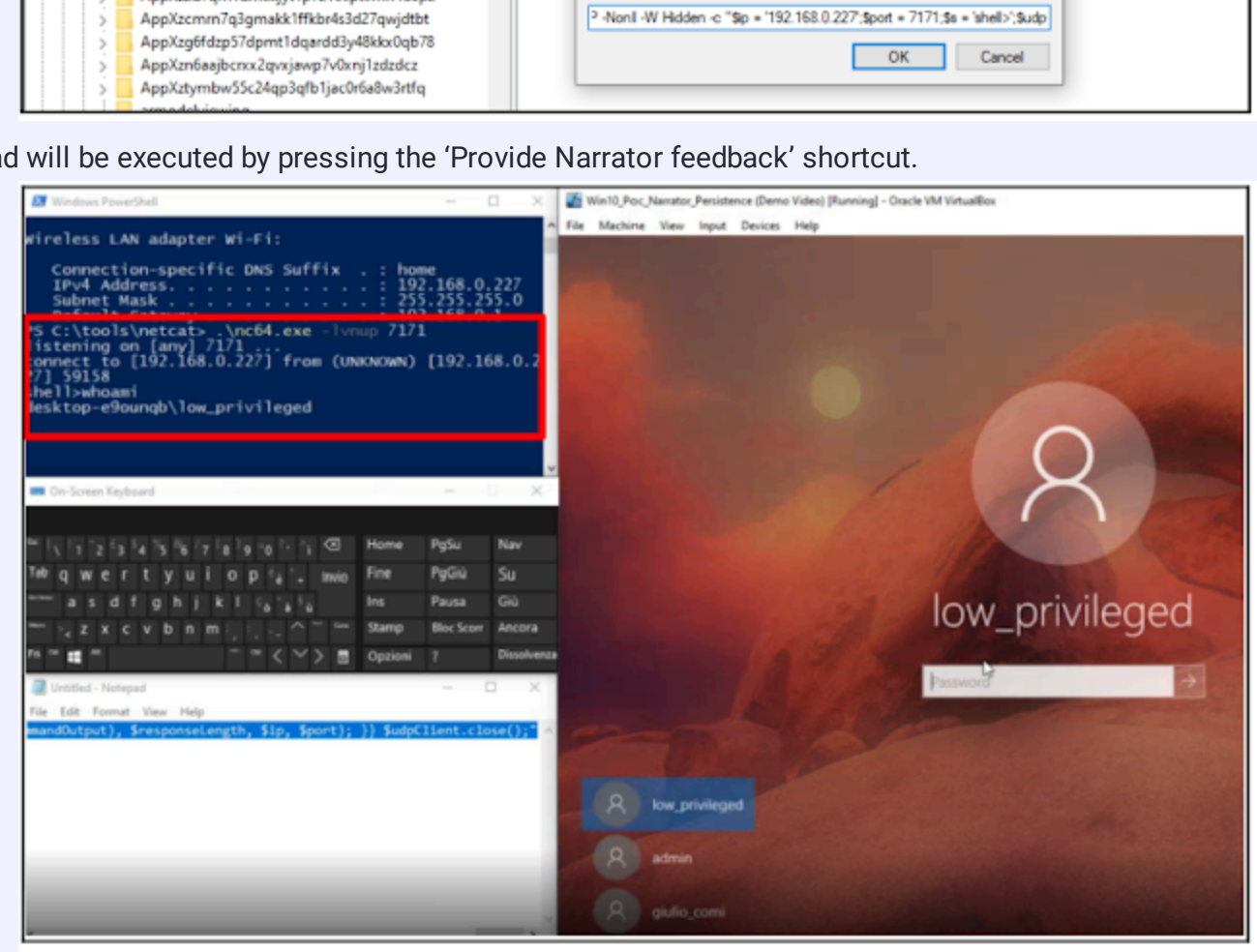
we get the following configuration (by the way it is the standard one for all Universal Apps):



Turned out after a not-so “educated” guess that by getting rid of the "DelegateExecute" entry and then adding a Powershell payload for the ‘Default’ value we will open rooms for this fileless persistence technique:



The payload will be executed by pressing the ‘Provide Narrator feedback’ shortcut.



Full video here: https://youtu.be/oPKnYO9V8-M

Conclusion

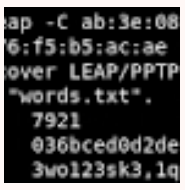
To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Popular posts from this blog

WPA2-PSK vs WPA2-Enterprise: hacking and hardening

- *June 15, 2018*



This post has the aim to summarise the security aspects of WPA2, with a focus on WPA2-Enterprise hacking. At the end, EAP-TLS is presented as a pretty secure implementation. WPA2 in brief The Wi-Fi Protected Access is a wireless technology designed to secure the communiciations between statio ...

READ MORE

Management Frame Protection and its limitations

- *June 03, 2018*

In this article we talk about management frames, their exposure to Denial of Service (DoS) via de-authentication attack, how Management Frames Protection can prevent this and its limitations against other DoS attacks discovered during the years by security researchers. A brief overview of ...

READ MORE

Powered by Blogger

Theme images by merrymoonmary