SettingSyncHost.exe as a LolBin

This native OS binary has two interesting options:

- -LoadAndRunDiagScript <name>
- -LoadAndRunDiagScriptNoCab <name>

When executed with these options, it will extract the .bat file stored inside its resources, save it as %TEMP%\RoamDiag.cmd, and then it will execute it.

There are at least two ways we can exploit it.

We can create our own %TEMP%\RoamDiag.cmd and make the SettingSyncHost.exe execute it, but there is a caveat. The .cmd file is always deleted and issues with that will stop program from working. Still, we could try a race condition approach i.e. run SettingSyncHost.exe with the parameters specified while at the same time we could run a batch file that overwrites %TEMP%\RoamDiag.cmd with a content of our choice in a never ending loop. This could work, but I have not tested it.

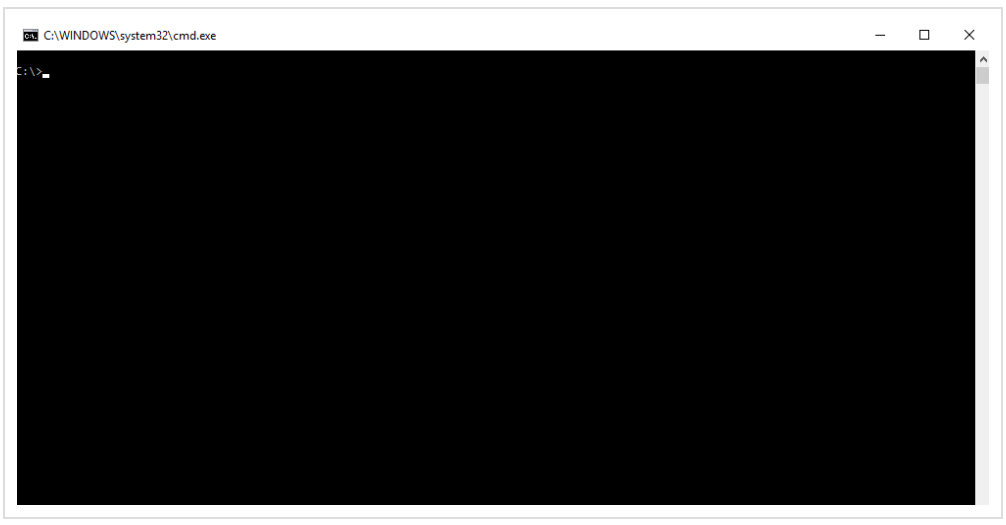
Why?

Because there is an easier way. The batch file extracted from resources of SettingSyncHost.exe and saved as %TEMP%\RoamDiag.cmd executes a number of OS programs including:

- wevtutil
- makecab
- reg
- ipconfig
- settingsynchost.exe
- tracelog

These programs are executed w/o specifying a full path, and in most of cases – not even file extensions. So… we can literally create a malicious file named like any of these 6, drop them inside the %TEMP% directory (including settingsynchost.exe !) and launch them using the following syntax:

cd %TEMP% & c:\windows\system32\SettingSyncHost.exe -LoadAndRunDiagScript foo



This entry was posted in **Living off the land**, **LOLBins**, **Uncategorized** by **adam**. Bookmark the **permalink**.