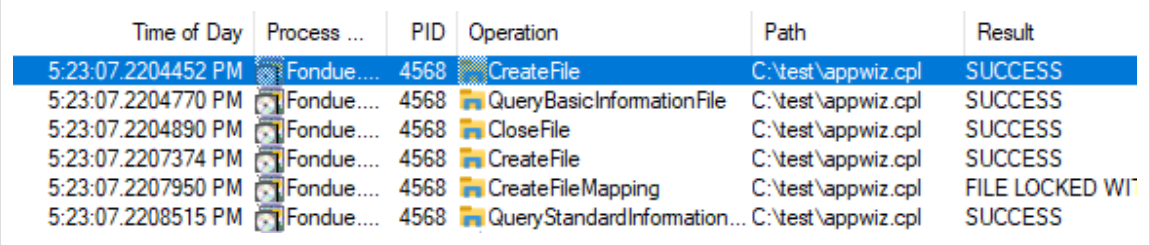
Posted on **2024-01-06** ← Previous Next →

1 little known secret of fondue.exe

Same as in the previous case, we can copy the main executable *fondue.exe* to a different folder f.ex. *c:\test* and start it from there, loading the c:\test*appwiz.cpl* we control in the process.



Time of Day	Process ...	PID	Operation	Path	Result
5:23:07.2204452 PM	Fondue....	4568	CreateFile	C:\test\appwiz.cpl	SUCCESS
5:23:07.2204770 PM	Fondue....	4568	QueryBasicInformationFile	C:\test\appwiz.cpl	SUCCESS
5:23:07.2204890 PM	Fondue....	4568	CloseFile	C:\test\appwiz.cpl	SUCCESS
5:23:07.2207374 PM	Fondue....	4568	CreateFile	C:\test\appwiz.cpl	SUCCESS
5:23:07.2207950 PM	Fondue....	4568	CreateFileMapping	C:\test\appwiz.cpl	FILE LOCKED WI
5:23:07.2208515 PM	Fondue....	4568	QueryStandardInformation...	C:\test\appwiz.cpl	SUCCESS

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