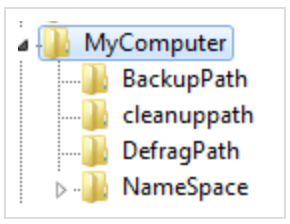
Beyond good ol' Run key, Part 55

The flexibility offered by the Registry comes with a price. Whoever is in a position to change the Registry keys or its values can affect not only the way OS works, but also adjust the functionality of many programs relying on some particular settings. If we talk about persistence, there is yet another location that may be abused for this purpose. The trick I am going to describe is actually very old, but with the intention to document as many persistence mechanisms as possible nothing should be omitted. Plus, it still works on win 10.

Looking at the following location:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer

we can quickly guess that the keys listed underneath refer to a couple of utility tools that Windows occasionally runs:

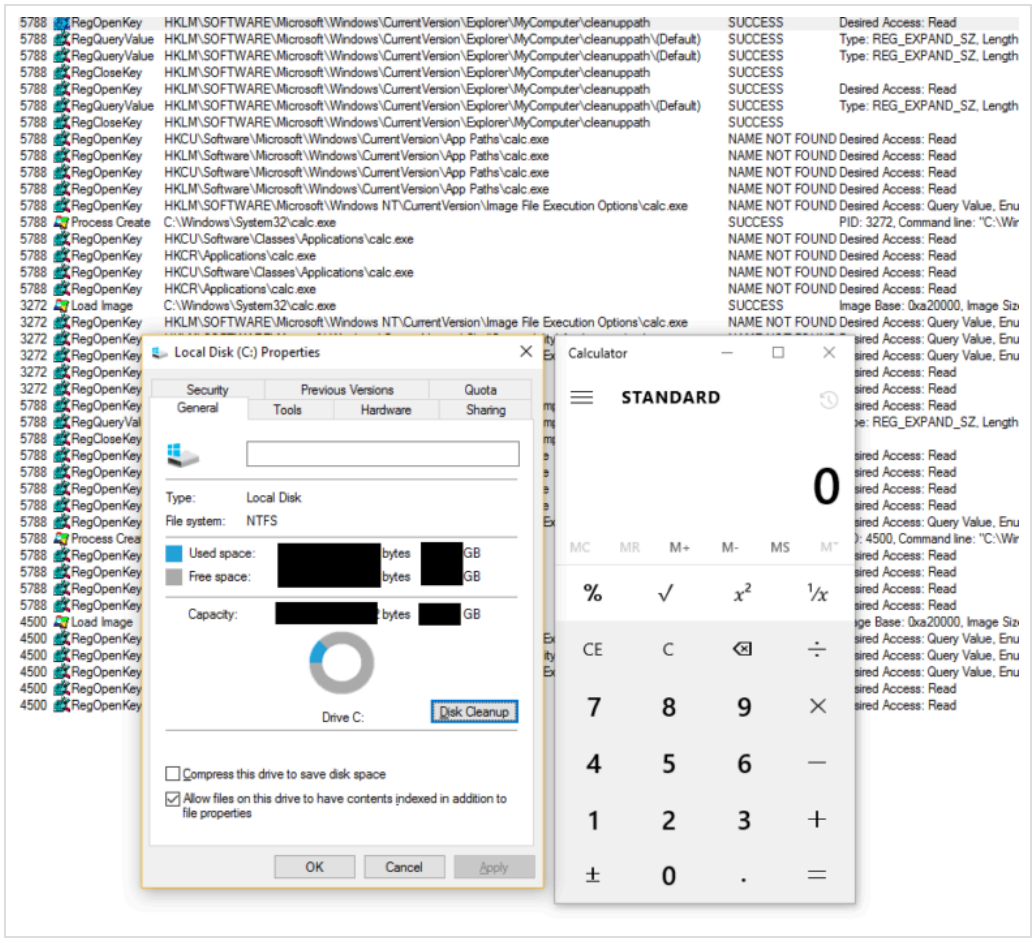


Exploring them we can find out that the settings are mapped to the following locations:

- BackupPath = %SystemRoot%\system32\sdclt.exe
- cleanuppath = %SystemRoot%\System32\cleanmgr.exe /D %c
- DefragPath = %systemroot%\system32\dfrgui.exe

Obviously, replacing these settings with your own (read: malware) will end up with the replacement programs being executed at the time OS will decide to kick off the respective activity (or, the user triggers it – see example below).

The easiest way to test this particular persistence mechanism is by replacing the entry for the CleanupPath; since this is a path pointing to the tool that will be executed when you click the Disk Cleanup on a drive, the replacement tool will be executed immediately after clicking the button (in my case it's just a calculator):



This entry was posted in **Anti-Forensics**, **Autostart (Persistence)**, **Compromise Detection**, **Incident Response**, **Malware Analysis** by **adam**. Bookmark the **permalink**.