

Challenge Name: Phantom Persistence

Challenge_Descriptions

Spectr Corp's SOC received reports of unusual behaviour on an employee workstation. A memory dump was acquired post-reboot and is provided to you for forensic investigation. You are given a memory image `memory.raw` from a Windows system. Your goal is to determine the persistence mechanism used by the attacker.

Submit the flag in this format:

`flag{method_name}`

In this challenge:

- `method`= type of persistence
- `name`= name of the registry value used by the attacker

File provided:

- `memory.raw`

Step 1: Validate the Memory Dump

We start by verifying that the memory image can be parsed by Volatility. We use Volatility because it is a powerful memory forensics framework that allows investigators, incident responders, and malware analysts to analyse volatile memory (RAM) dumps from compromised systems.

Commands:

- `python3 vol.py -f memory.raw windows.info`

What it does:

- **python3 vol.py**: Runs the `vol.py` script using Python 3, this is the main entry point for Volatility 3.
- **-f memory.raw**: Specifies the input **memory dump file** (`memory.raw`) to analyze.
- **windows.info**: Tells Volatility to run the **windows.info plugin**, which extracts basic OS information from the Windows memory image.

```
L$ python3 vol.py -f [redacted] /memory.raw windows.info
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf8054c000000
DTB 0x1aa000
Symbols file:///home/creed/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D9424FC4861E47C10FAD1B35DEC6DCC8-1.json.xz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf8054cc0f400
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 2
SystemTime 2025-06-25 18:06:56+00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Mon Dec 9 11:07:51 2019
```

This confirms the dumped memory is from a Windows 10 x64 system and allows Volatility to identify relevant plugins.

Step 2: Investigate for Persistence

In cybersecurity, persistence refers to techniques attackers use to maintain access to a compromised system even after reboots, user logoffs, or other interruptions.

Once attackers gain access to a system, they don't want to lose it, so they install backdoors or re-launch malware automatically. One common method for this is modifying the **Windows Registry Run Keys**.

What is Windows Registry Run Keys?

The Windows Registry is a central database that stores system settings, configurations, and startup programs.

Within it, there are specific keys like:

[“HKCU\Software\Microsoft\Windows\CurrentVersion\Run”](#)

These keys tell Windows to automatically launch specific programs when a user logs in. This makes it a prime target for attackers who want their malware to persist every time the machine boots or a user logs in.

Since the attacker may have used Registry Run Keys for persistence, we check the HKCU\Software\Microsoft\Windows\CurrentVersion\Run path:

Commands:

- `python3 vol.py -f memory.raw windows.registry.printkey --key "Software\\Microsoft\\Windows\\CurrentVersion\\Run"`

What it does:

- **python3 vol.py**: Runs the **Volatility 3** framework using Python 3.
- **-f memory.raw**: Specifies the **memory dump file** to analyze (in this case, memory.raw).
- **windows.registry.printkey**: Invokes the **Volatility plugin** that prints the content of a specific Windows **Registry key**.
- **--key "Software\\Microsoft\\Windows\\CurrentVersion\\Run"**: Provides the exact **registry path** to inspect. Double backslashes (\\) are used to **escape** backslashes in the Windows registry path.

```
l--$ python3 vol.py -f /memory.raw windows.registry.printkey --key "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
Volatility 3 Framework 2.26.2
Progress: 100.00% PDB scanning finished
Last Write Time Hive Offset Type Key Name Data Volatile
-
0x850ec4454000 Key [NONAME] Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec4460000 Key \REGISTRY\MACHINE\SYSTEM\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec4497000 Key \REGISTRY\MACHINE\HARDWARE\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec4481000 Key \Device\HarddiskVolume1\Boot\BCD\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec4483000 Key \SystemRoot\System32\Config\SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec7b20000 Key \SystemRoot\System32\Config\SECURITY\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec7b98000 Key \SystemRoot\System32\Config\SAM\Software\Microsoft\Windows\CurrentVersion\Run - - -
2025-06-26 00:32:13.000000 UTC 0x850ec7c40000 REG_SZ \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run OneDriveSetup C:\Windows\SysWOW64\OneDriveSetup.exe
0x850ec7e3d000 Key \SystemRoot\System32\Config\BB1\Software\Microsoft\Windows\CurrentVersion\Run - - -
2025-06-26 00:32:17.000000 UTC 0x850ec7e43000 REG_SZ \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run OneDriveSetup C:\Windows\SysWOW64\OneDriveSetup.exe
2025-06-25 17:59:44.000000 UTC 0x850ec965e000 REG_SZ \??\C:\Users\creed\ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Run MicrosoftEdgeAutoLaunch_917988B932E692AF3FF59BAE22104D64
ge\Application\msedge.exe" --no-startup-window --win-session-start False
2025-06-25 17:59:44.000000 UTC 0x850ec965e000 REG_SZ \??\C:\Users\creed\ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Run OneDrive "C:\Users\creed\AppData\Local\Microsoft\OneDrive\OneDrive.exe"
2025-06-25 17:59:44.000000 UTC 0x850ec965e000 REG_SZ \??\C:\Users\creed\ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Updater C:\Users\creed\AppData\Roaming\updater.exe False
0x850ec9660000 Key \??\C:\Users\creed\AppData\Local\Microsoft\Windows\UsrClass.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec9e7d000 Key \??\C:\Windows\AppCompat\Programs\Amcache.hve\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca3b2000 Key \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.19041.3636_neutral_neutral_cw5nh2txyewy\ActivationStore.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca3f1000 Key \??\C:\Users\creed\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5nh2txyewy\Settings\settings.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca7d9000 Key \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Search_1.14.10.19041_neutral_neutral_cw5nh2txyewy\ActivationStore.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca7db000 Key \??\C:\Users\creed\AppData\Local\Packages\Microsoft.Windows.Search_cw5nh2txyewy\Settings\settings.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca9ec000 Key \??\C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\State\dosvcState.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca4a0000 Key \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Client_CBS_1000.19053.1000.0_x64_cw5nh2txyewy\ActivationStore.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850eca235000 Key \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_kzf8qxf38zgc\ActivationStore.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ecb388000 Key \??\C:\Users\creed\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zgc\Settings\settings.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec8d7f000 Key \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.WindowsStore_11910.1002.5.0_x64_8wekyb3d8bbwe\ActivationStore.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
0x850ec4a41000 Key \??\C:\Users\creed\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat\Software\Microsoft\Windows\CurrentVersion\Run - - -
```

Step 3: Analyze the Output

Volatility returns the following key entry:

```
Key: \??\C:\Users\████████ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Name: Updater
Data: C:\Users\████████\AppData\Roaming\updater.exe
```

This indicates a classic attacker technique:

- The malware was copied to a hidden path in the user profile (AppData\Roaming)
- A Run key named Updater was added to launch the malware on every login

Step 4: Extract the Flag

Based on the format and findings:

- Method = run_key
- Name = updater

Final Flag:

WARZONE{run_key_updater}