Can you track processes accessing the camera and microphone?

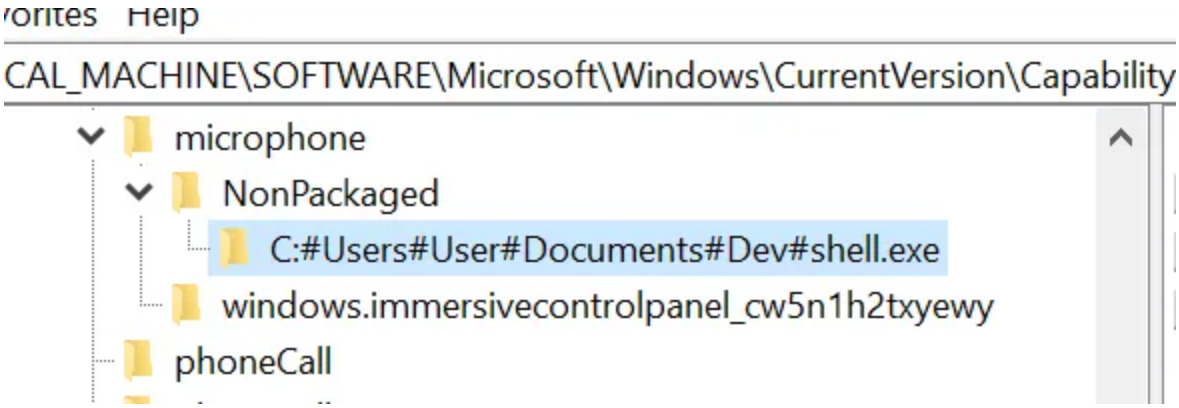
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Capab
ilityAccessManager\ConsentStore\webcam\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Capab
ilityAccessManager\ConsentStore\microphone\

HKEY_USERS\*\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityA
ccessManager\ConsentStore\webcam\

HKEY_USERS\*\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityA
ccessManager\ConsentStore\microphone\
```

> *EDIT 2022/01/08: Some further testing was done by Phill Moore and observed the*

Within the `NonPackaged` directory, you can see that the name of the keys are the full path of an executable with `#` replacing `\`.

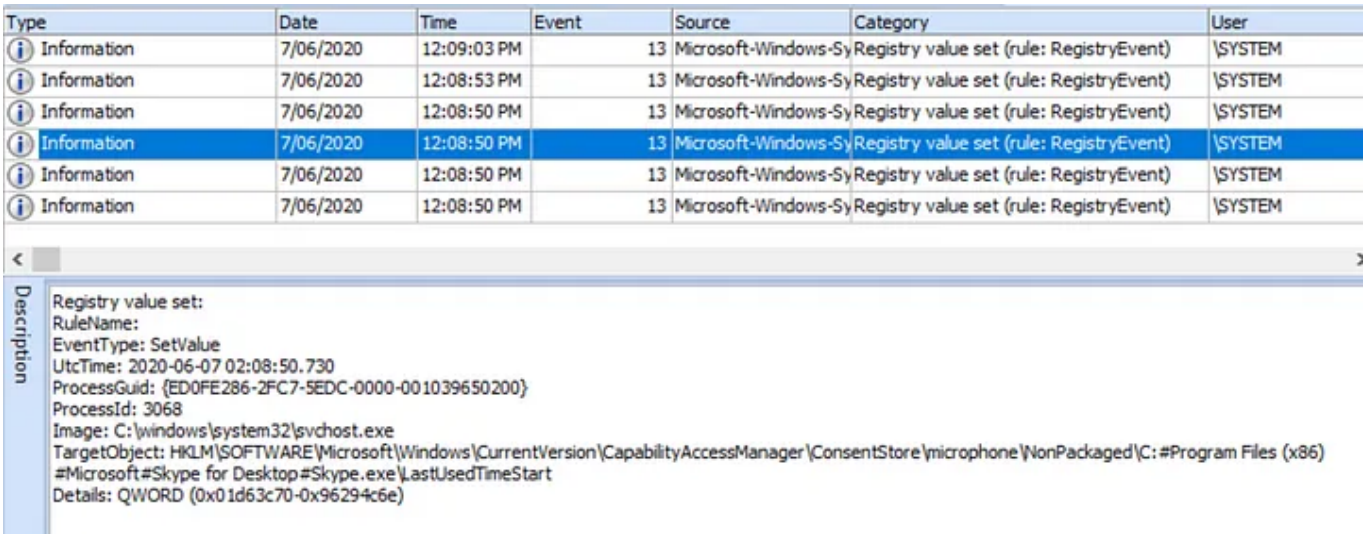
Each entry has two values, **LastUsedTimeStart** and **LastUsedTimeStop**, with the timestamps in FILETIME format.

From the example above, you are able to determine**, Zoom.exe** had **access to my webcam for 27.2 minutes** (between 2020/06/01 04:30:52 UTC and 2020/06/01 04:58:04 UTC).



Monitoring

If we wanted to track all sessions (not just the last), it is easy with Sysmon. If



Type	Date	Time	Event	Source	Category	User
Information	7/06/2020	12:09:03 PM	13	Microsoft-Windows-Sy	Registry value set (rule: RegistryEvent)	\SYSTEM
Information	7/06/2020	12:08:53 PM	13	Microsoft-Windows-Sy	Registry value set (rule: RegistryEvent)	\SYSTEM
Information	7/06/2020	12:08:50 PM	13	Microsoft-Windows-Sy	Registry value set (rule: RegistryEvent)	\SYSTEM
Information	7/06/2020	12:08:50 PM	13	Microsoft-Windows-Sy	Registry value set (rule: RegistryEvent)	\SYSTEM
Information	7/06/2020	12:08:50 PM	13	Microsoft-Windows-Sy	Registry value set (rule: RegistryEvent)	\SYSTEM
Information	7/06/2020	12:08:50 PM	13	Microsoft-Windows-Sy	Registry value set (rule: RegistryEvent)	\SYSTEM

Description

Registry value set:
RuleName:
EventType: SetValue
UtcTime: 2020-06-07 02:08:50.730
ProcessGuid: {ED0FE286-2FC7-5EDC-0000-001039650200}
ProcessId: 3068
Image: C:\windows\system32\svchost.exe
TargetObject: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\microphone\NonPackaged\C:#Program Files (x86)#Microsoft#Skype for Desktop#Skype.exe\LastUsedTimeStart
Details: QWORD (0x01d63c70-0x96294c6e)

Zach

Forensics Dfir Incident Response

-- 2