T1123 - Audio Capture

Description from ATT&CK

> An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.
> Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Atomic Tests

- Atomic Test #1 - using device audio capture commandlet
- Atomic Test #2 - Registry artefact when application use microphone

Atomic Test #1 - using device audio capture commandlet

AudioDeviceCmdlets

Supported Platforms: Windows

auto_generated_guid: 9c3ad250-b185-4444-b5a9-d69218a10c95

Attack Commands: Run with `powershell`!

```
powershell.exe -Command WindowsAudioDevice-Powershell-Cmdlet
```

Atomic Test #2 - Registry artefact when application use microphone

can-you-track-processes-accessing-the-camera-and-microphone

Supported Platforms: Windows

auto_generated_guid: 7a21cce2-6ada-4f7c-afd9-e1e9c481e44a

Attack Commands: Run with `command_prompt`!

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\Cons
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\Cons
```

Cleanup Commands:

```
reg DELETE HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\(
```