Audio Capture via PowerShell

Detect attacker collecting audio via PowerShell Cmdlet.

id:	ab7a6ef4-0983-4275-a4f1-5c6bd3c31c23
categories:	detect
confidence:	medium
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Collection
techniques:	T1123 Audio Capture

Query

```
process where subtype.create and
  process_name == "powershell.exe" and command_line == "* WindowsAudioDevice-Powershell-Cmd
```

Detonation

Atomic Red Team: T1123

Contributors

- Endgame

Previous Next