

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Search

Sign in

Sign up

redcanaryco / atomic-red-team

Public

Notifications

Fork

2.8k

Star

9.7k

<> Code

Issues

6

Pull requests

5

Actions

Wiki

Security

Insights

Files

f339e7d

▼

Search

Go to file

>  .github

>  atomic\_red\_team

>  atomics

>  Indexes

>  T1003.001

>  T1003.002

>  T1003.003

>  T1003.004

>  T1003.005

>  T1003.006

>  T1003.007

>  T1003.008

>  T1003

>  T1006

>  T1007

>  T1010

>  T1012

>  T1014

>  T1016

>  T1018

>  T1020

>  T1021.001

>  T1021.002

>  T1021.003

>  T1021.006

>  T1027.001

>  T1027.002

>  T1027.004

>  T1027

>  T1030

>  T1033

>  T1036.003

>  T1036.004

>  T1036.005

>  T1036.006

>  T1036

atomic-red-team / atomics / T1123 / T1123.md

CircleCI Atomic Red Team doc...

Generate docs from job=gener...

6bacc32 · 2 years ago

History

Preview

Code

Blame

74 lines (32 loc) · 2.2 KB

Raw

# 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 !

Page 1 of 2

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessM   
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessM
```

Cleanup Commands:

```
reg DELETE HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAcce 
```