☐ Audio Capture via SoundRecorder

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

Bypass UAC via CMSTP

Bypass UAC via CompMgmtLauncher

Bypass UAC via Fodhelper.exe

Bypass UAC via Fodhelper.exe

Bypass UAC via WSReset.exe

Change Default File Association

Clearing Windows Event Logs with wevtutil

COM Hijack via Script Object

Command-Line Creation of a RAR file

**Control Panel Items** 

Creation of an Archive with Common Archivers

Creation of Kernel Module

Creation of Scheduled Task with schtasks.exe

Creation or Modification of Systemd Service

Credential Enumeration via Credential Vault CLI

Delete Volume USN Journal with fsutil

Disconnecting from Network Shares with net.exe

Discovery and Enumeration of System Information via Rundll32

Discovery of a Remote System's Time

Discovery of Domain Groups

Discovery of Network Environment via Built-in Tools

Discovery of Network Environment via Built-in Tools

DLL Search Order Hijacking with known programs

Domain Trust Discovery

Domain Trust Discovery via NItest.exe

Encoding or Decoding Files via CertUtil

**Enumeration of Local Shares** 

**Enumeration of Mounted Shares** 

**Enumeration of Remote Shares** 

**Enumeration of System Information** 

**Enumeration of System Information** 

Executable Written and Executed by Microsoft Office Applications

Execution of a Command via a SYSTEM Service

Franctice of Evidence Coming via

Docs » Analytics » Audio Capture via SoundRecorder

C Edit on GitHub

# **Audio Capture via SoundRecorder**

Detect audio collection via SoundRecorder application.

id: f72a98cb-7b3d-4100-99c3-a138b6e9ff6e

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

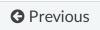
```
process where subtype.create and
process_name == "SoundRecorder.exe" and command_line == "* /FILE*"
```

#### **Detonation**

Atomic Red Team: T1123

#### **Contributors**

• Endgame





© Copyright 2019, Endgame Revision 30243396.

Built with Sphinx using a theme provided by Read the Docs.

