Audio Capture, Technique T1123 - Enterprise

Archived: 2026-04-05 17:50:58 UTC

G0067 APT37

APT37 has used an audio capturing utility known as SOUNDWAVE that captures microphone input.[2]

S0438 Attor

Attor's has a plugin that is capable of recording audio using available input sound devices.[1]

S0234 Bandook

Bandook has modules that are capable of capturing audio.[3]

S0454 Cadelspy

Cadelspy has the ability to record audio from the compromised host.[4]

S0338 Cobian RAT

Cobian RAT has a feature to perform voice recording on the victim’s machine.[5]

S0115 Crimson

Crimson can perform audio surveillance using microphones.[6]

S0334 DarkComet

DarkComet can listen in to victims' conversations through the system’s microphone.[7][8]

S0021 Derusbi

Derusbi is capable of performing audio captures.[9]

S0213 DOGCALL

DOGCALL can capture microphone data from the victim's machine.[10]

S0152 EvilGrab

EvilGrab has the capability to capture audio from a victim machine.[11]

S0143 Flame

Flame can record audio using any existing hardware recording devices.[12][13]

S0434 Imminent Monitor

Imminent Monitor has a remote microphone monitoring capability.[14][15]

S0260 InvisiMole

InvisiMole can record sound using input audio devices.[16][17]

S0163 Janicab

Janicab captured audio and sent it out to a C2 server.[18][19]

S0283 jRAT

jRAT can capture microphone recordings.[20]

S1185 LightSpy

LightSpy uses Apple's built-in AVFoundation Framework library to capture and manage audio recordings then transform them to JSON blobs for exfiltration.[21]

S0409 Machete

Machete captures audio from the computer’s microphone.[22][23][24]

S1016 MacMa

MacMa has the ability to record audio.[25]

S0282 MacSpy

MacSpy can record the sounds from microphones on a computer.[26]

S1146 MgBot

MgBot can capture input and output audio streams from infected devices.[27][28]

S0339 Micropsia

Micropsia can perform microphone recording.[29]

S0336 NanoCore

NanoCore can capture audio feeds from the system.[30][31]

S1090 NightClub

NightClub can load a module to leverage the LAME encoder and `mciSendStringW` to control and capture audio.[32]

S0194 PowerSploit

PowerSploit's `Get-MicrophoneAudio` Exfiltration module can record system microphone audio.[33][34]

S0192 Pupy

Pupy can record sound with the microphone.[35]

S0332 Remcos

Remcos can capture data from the system's microphone.[36]

S0379 Revenge RAT

Revenge RAT has a plugin for microphone interception.[37][38]

S0240 ROKRAT

ROKRAT has an audio capture and eavesdropping module.[39]

S0098 T9000

T9000 uses the Skype API to record audio and video calls. It writes encrypted data to `%APPDATA%\Intel\Skype`.[40]

S0467 TajMahal

TajMahal has the ability to capture VoiceIP application audio on an infected host.[41]

S0257 VERMIN

VERMIN can perform audio capture.[42]
