# TTP Detail – T1125

## TTP Information

Name: Video Capture

Description: An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.

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 video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1113) due to use of specific devices or applications for video recording rather than capturing the victim's screen.

In macOS, there are a few different malware samples that record the user's webcam such as FruitFly and Proton. (Citation: objective-see 2017 review)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* Agent Tesla
* Bandook
* Clambling
* Cobian RAT
* Crimson
* DarkComet
* Derusbi
* EvilGrab
* InvisiMole
* Kazuar
* Machete
* NanoCore
* ObliqueRAT
* PoetRAT
* Revenge RAT
* SDBbot
* T9000
* TajMahal
* WarzoneRAT
* ZxShell
* jRAT
* njRAT

## Tools

* AsyncRAT
* ConnectWise
* Empire
* Imminent Monitor
* PcShare
* Pupy
* QuasarRAT
* Quick Assist
* Remcos

## APTs (Intrusion Sets)

* Ember Bear
* FIN7
* Silence