# TTP Detail – T1113

## TTP Information

Name: Screen Capture

Description: Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as <code>CopyFromScreen</code>, <code>xwd</code>, or <code>screencapture</code>.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* Agent Tesla
* AppleSeed
* Aria-body
* Attor
* Azorult
* BADHATCH
* BADNEWS
* BISCUIT
* BLUELIGHT
* BadPatch
* Bandook
* BlackEnergy
* CHIMNEYSWEEP
* CHOPSTICK
* Cadelspy
* Cannon
* Carbanak
* Carberp
* Cardinal RAT
* Catchamas
* Chaes
* CharmPower
* Chrommme
* Clambling
* Cobalt Strike
* Cobian RAT
* CosmicDuke
* Crimson
* CrossRAT
* Cuckoo Stealer
* DOGCALL
* DUSTTRAP
* Daserf
* Derusbi
* DustySky
* ECCENTRICBANDWAGON
* EvilGrab
* FinFisher
* Flame
* FlawedAmmyy
* FruitFly
* FunnyDream
* GRIFFON
* HALFBAKED
* HotCroissant
* Hydraq
* HyperBro
* InvisiMole
* JHUHUGIT
* Janicab
* KEYMARBLE
* KONNI
* Kasidet
* Kazuar
* KeyBoy
* Kivars
* LightSpy
* LitePower
* Lizar
* LookBack
* Lumma Stealer
* LunarMail
* MacMa
* MacSpy
* Machete
* Mafalda
* Manjusaka
* MarkiRAT
* Matryoshka
* Metamorfo
* Micropsia
* Mispadu
* NETWIRE
* NKAbuse
* NightClub
* ObliqueRAT
* Octopus
* POORAIM
* POWERSTATS
* POWRUNER
* Peppy
* PlugX
* PoetRAT
* Prikormka
* Proton
* Pteranodon
* QuietSieve
* RCSession
* RDAT
* ROKRAT
* RTM
* Raccoon Stealer
* RainyDay
* Ramsay
* RedLeaves
* Remexi
* Revenge RAT
* RogueRobin
* Rover
* SHUTTERSPEED
* SLOTHFULMEDIA
* SMOKEDHAM
* SVCReady
* SharpStage
* Socksbot
* StoneDrill
* StrifeWater
* SysUpdate
* T9000
* TRANSLATEXT
* TURNEDUP
* TajMahal
* TinyZBot
* Trojan.Karagany
* Troll Stealer
* Turian
* UPPERCUT
* Ursnif
* VERMIN
* Valak
* Woody RAT
* XAgentOSX
* XCSSET
* XLoader
* ZLib
* Zebrocy
* Zeus Panda
* ZxShell
* gh0st RAT
* jRAT
* metaMain
* njRAT
* yty

## Tools

* AsyncRAT
* Brute Ratel C4
* ConnectWise
* Empire
* PcShare
* PowerSploit
* Pupy
* Quick Assist
* Remcos
* RemoteUtilities
* SILENTTRINITY
* Sliver

## APTs (Intrusion Sets)

* APT28
* APT39
* APT42
* BRONZE BUTLER
* Dark Caracal
* Dragonfly
* FIN7
* GOLD SOUTHFIELD
* Gamaredon Group
* Group5
* Kimsuky
* Magic Hound
* MoustachedBouncer
* MuddyWater
* OilRig
* Silence
* Volt Typhoon
* Winter Vivern