# TTP Detail – T1010

## TTP Information

Name: Application Window Discovery

Description: Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.(Citation: Prevailion DarkWatchman 2021) For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) to evade.(Citation: ESET Grandoreiro April 2020)

Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) commands and [Native API](https://attack.mitre.org/techniques/T1106) functions.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Aria-body
* Attor
* Cadelspy
* Catchamas
* DUSTTRAP
* DarkGate
* DarkWatchman
* Duqu
* Flagpro
* FunnyDream
* Grandoreiro
* HotCroissant
* InvisiMole
* Kazuar
* Machete
* Metamorfo
* NETWIRE
* NetTraveler
* NightClub
* PLEAD
* PoisonIvy
* PowerDuke
* QakBot
* ROKRAT
* Remexi
* SOUNDBITE
* Trojan.Karagany
* WINERACK
* njRAT

## Tools

* SILENTTRINITY

## APTs (Intrusion Sets)

* HEXANE
* Lazarus Group
* Volt Typhoon