# TTP Detail – T1143

## TTP Information

Name: Hidden Window

Description: Adversaries may implement hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. Adversaries may abuse operating system functionality to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.

### Windows
There are a variety of features in scripting languages in Windows, such as [PowerShell](https://attack.mitre.org/techniques/T1086), Jscript, and VBScript to make windows hidden. One example of this is <code>powershell.exe -WindowStyle Hidden</code>. (Citation: PowerShell About 2019)

### Mac
The configurations for how applications run on macOS are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. However, adversaries can abuse this feature and hide their running window.(Citation: Antiquated Mac Malware)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion