T1564.003 - Hidden Window

Description from ATT&CK

> Adversaries may use 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.
> On Windows, there are a variety of features in scripting languages in Windows, such as PowerShell, Jscript, and Visual Basic to make windows hidden. One example of this is `powershell.exe -WindowStyle Hidden`. (Citation: PowerShell About 2019)
>
> Similarly, on macOS the configurations for how applications run are listed in property list (plist) files. One of the tags in these files can be `apple.awt.UIElement`, 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.
>
> Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.(Citation: Antiquated Mac Malware)

Atomic Tests

Atomic Test #1 - Hidden Window

Launch PowerShell with the "-WindowStyle Hidden" argument to conceal PowerShell windows by setting the WindowStyle parameter to hidden. Upon execution a hidden PowerShell window will launch calc.exe

Supported Platforms: Windows

auto_generated_guid: f151ee37-9e2b-47e6-80e4-550b9f999b7a

Inputs:

Name	Description	Type	Default Value
powershell_command	Command to launch calc.exe from a hidden PowerShell Window	String	powershell.exe -WindowStyle hidden calc.exe

Attack Commands: Run with `powershell`!

```
Start-Process #{powershell_command}
```