Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 5 Actions Wiki Security Insights

Files

f339e7d

Go to file

.github
atomic_red_team
atomics
Indexes
T1003.001
T1003.002
T1003.003
T1003.004
T1003.005
T1003.006
T1003.007
T1003.008
T1003
T1006
T1007
T1010
T1012
T1014
T1016
T1018
T1020
T1021.001
T1021.002
T1021.003
T1021.006
T1027.001
T1027.002
T1027.004
T1027
T1030
T1033
T1036.003
T1036.004
T1036.005
T1036.006
T1036

atomic-red-team / atomics / T1564.003 / T1564.003.md

CircleCI Atomic Red Team doc... Generate docs from job=gener... 36d49de · 3 years ago History

Preview Code Blame 49 lines (23 loc) · 2.14 KB Raw

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

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

T1037.001
T1037.002
T1037.004
T1037.005
T1039
T1040

Attack Commands: Run with `powershell`!

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