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 / T1574.009 / T1574.009.md

CircleCI Atomic Red Team doc... Generate docs from job=genera... bc21f59 · 3 years ago History

Preview Code Blame 59 lines (34 loc) · 3.02 KB Raw

T1574.009 - Path Interception by Unquoted Path

Description from ATT&CK

> Adversaries may execute their own malicious payloads by hijacking vulnerable file path references. Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.
> Service paths (Citation: Microsoft CurrentControlSet Services) and shortcut paths may also be vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., `C:\unsafe path with space\program.exe` vs. `"C:\safe path with space\program.exe"`). (Citation: Help eliminate unquoted path) (stored in Windows Registry keys) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is `C:\program files\myapp.exe`, an adversary may create a program at `C:\program.exe` that will be run instead of the intended program. (Citation: Windows Unquoted Services) (Citation: Windows Privilege Escalation Guide)
>
> This technique can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

Atomic Tests

- Atomic Test #1 - Execution of program.exe as service with unquoted service path

Atomic Test #1 - Execution of program.exe as service with unquoted service path

When a service is created whose executable path contains spaces and isn’t enclosed within quotes, leads to a vulnerability known as Unquoted Service Path which allows a user to gain SYSTEM privileges. In this case, if an executable program.exe in C:\ exists, C:\program.exe will be executed instead of test.exe in C:\Program Files\subfolder\test.exe.

Supported Platforms: Windows

auto_generated_guid: 2770dea7-c50f-457b-84c4-c40a47460d9f

Inputs:

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

Name	Description	Type	Default Value
service_executable	Path of the executable used for the service and as the hijacked program.exe	Path	PathToAtomicsFolder\T1574.009\bin\Winc

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
copy #{service_executable} "C:\Program Files\windows_service.exe"
copy #{service_executable} "C:\program.exe"
sc create "Example Service" binpath= "C:\Program Files\windows_service.e
sc start "Example Service"
```

Cleanup Commands:

```
sc stop "Example Service" >nul 2>&1
sc delete "Example Service" >nul 2>&1
del "C:\Program Files\windows_service.exe" >nul 2>&1
del "C:\program.exe" >nul 2>&1
del "C:\Time.log" >nul 2>&1
```