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
    - T1036.006.md

atomic-red-team / atomics / T1036.006 / T1036.006.md

CircleCI Atomic Red Team doc... Generate docs from job=genera... 37ea965 · 3 years ago History

Preview Code Blame 80 lines (37 loc) · 2.4 KB Raw

T1036.006 - Space after Filename

Description from ATT&CK

> Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system.
> For example, if there is a Mach-O executable file called `evil.bin`, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to `evil.txt`, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to `evil.txt ` (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed (Citation: Mac Backdoors are back).
>
> Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

Atomic Tests

- Atomic Test #1 - Space After Filename (Manual)
- Atomic Test #2 - Space After Filename

Atomic Test #1 - Space After Filename (Manual)

Space After Filename

Supported Platforms: macOS

auto_generated_guid: 89a7dd26-e510-4c9f-9b15-f3bae333360f

Run it with these steps!

1. echo '#!/bin/bash\necho "print "hello, world!"" | /usr/bin/python\nexit' > execute.txt && chmod +x execute.txt
2. mv execute.txt "execute.txt "
3. ./execute.txt\

T1036.006.yaml
T1036
T1037.001
T1037.002
T1037.004
T1037.005

Atomic Test #2 - Space After Filename

Space after filename.

Supported Platforms: macOS, Linux

auto_generated_guid: b95ce2eb-a093-4cd8-938d-5258cef656ea

Attack Commands: Run with `bash`!

```
mkdir -p /tmp/atomic-test-T1036.006
cd /tmp/atomic-test-T1036.006
mkdir -p 'testdirwithspaceend '
/usr/bin/echo -e "%d\na\n#!/usr/bin/perl\nprint \"running T1035.006 with
chmod +x 'testdirwithspaceend /init '
'./testdirwithspaceend /init '
```

Cleanup Commands:

```
rm -rf /tmp/atomic-test-T1036.006
```