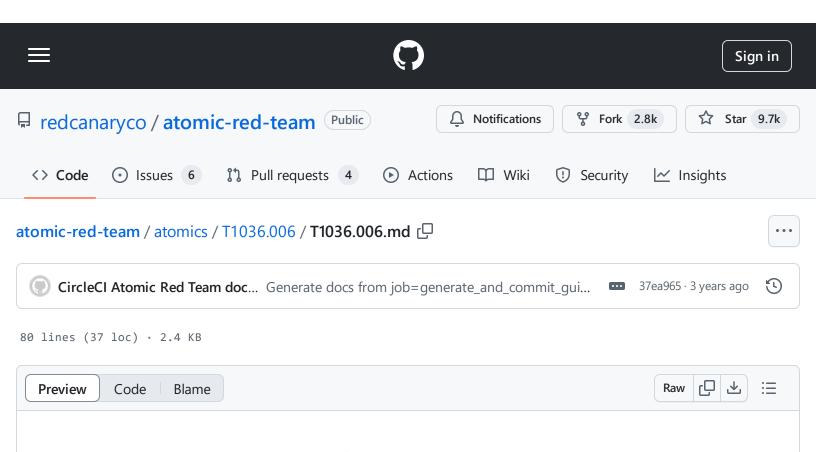
atomic-red-team/atomics/T1036.006/T1036.006.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 15:14 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1036.006/T1036.006.md



# 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\

## 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 space aftomatical space aftomati
```

 $atomic-red-team/atomics/T1036.006/T1036.006.md\ at\ f339e7da7d05f6057fdfcdd3742bfcf365fee2a9\cdot redcanaryco/atomic-red-team\cdot GitHub$  - 31/10/2024 15:14 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1036.006/T1036.006.md

chmod +x 'testdirwithspaceend /init '
'./testdirwithspaceend /init '

Cleanup Commands:

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