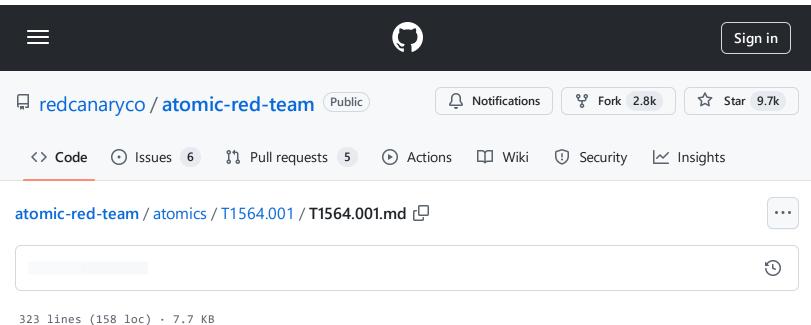
atomic-red-team/atomics/T1564.001/T1564.001.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 20:07 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md#atomic-test-8---hide-files-through-registry



#### ,

# T1564.001 - Hidden Files and Directories

# **Description from ATT&CK**

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a 'hidden' file. These files don't show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (dir /a for Windows and 1s -a for Linux and macOS).

On Linux and Mac, users can mark specific files as hidden simply by putting a "." as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folders that start with a period, '.', are by default hidden from being viewed in the Finder application and standard command-line utilities like "Is". Users must specifically change settings to have these files viewable.

Files on macOS can also be marked with the UF\_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications

atomic-red-team/atomics/T1564.001/T1564.001.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 20:07 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md#atomic-test-8---hide-files-through-registry

create these hidden files and folders to store information so that it doesn't clutter up the user's workspace. For example, SSH utilities create a .ssh folder that's hidden and contains the user's known hosts and keys.

Adversaries can use this to their advantage to hide files and folders anywhere on the system and evading a typical user or system analysis that does not incorporate investigation of hidden files.

### **Atomic Tests**

- Atomic Test #1 Create a hidden file in a hidden directory
- Atomic Test #2 Mac Hidden file
- Atomic Test #3 Create Windows System File with Attrib
- Atomic Test #4 Create Windows Hidden File with Attrib
- Atomic Test #5 Hidden files
- Atomic Test #6 Hide a Directory
- Atomic Test #7 Show all hidden files
- Atomic Test #8 Hide Files Through Registry

## Atomic Test #1 - Create a hidden file in a hidden directory

Creates a hidden file inside a hidden directory

Supported Platforms: Linux, macOS

auto\_generated\_guid: 61a782e5-9a19-40b5-8ba4-69a4b9f3d7be

Attack Commands: Run with sh!

mkdir /var/tmp/.hidden-directory
echo "T1564.001" > /var/tmp/.hidden-directory/.hidden-file

Q

#### **Cleanup Commands:**

rm -rf /var/tmp/.hidden-directory/

ᄆ

## Atomic Test #2 - Mac Hidden file

Hide a file on MacOS

Supported Platforms: macOS

auto\_generated\_guid: cddb9098-3b47-4e01-9d3b-6f5f323288a9

Attack Commands: Run with sh!

xattr -lr \* / 2>&1 /dev/null | grep -C 2 "00 00 00 00 00 00 00 40 00 FF FF FF FI  $\Box$ 

## Atomic Test #3 - Create Windows System File with Attrib

Creates a file and marks it as a system file using the attrib.exe utility. Upon execution, open the file in file explorer then open Properties > Details and observe that the Attributes are "SA" for System and Archive.

Supported Platforms: Windows

auto\_generated\_guid: f70974c8-c094-4574-b542-2c545af95a32

#### Inputs:

Name	Description	Туре	Default Value
file_to_modify	File to modify using Attrib command	String	%temp%\T1564.001.txt

#### Attack Commands: Run with command\_prompt! Elevation Required (e.g. root or admin)

attrib.exe +s #{file\_to\_modify}

0

#### **Cleanup Commands:**

```
del /A:S #{file_to_modify} >nul 2>&1
```

Q

Dependencies: Run with command\_prompt!

Description: The file must exist on disk at specified location (#{file\_to\_modify})

**Check Prereq Commands:** 

```
IF EXIST #{file_to_modify} ( EXIT 0 ) ELSE ( EXIT 1 )
```

O

#### **Get Prereq Commands:**

```
echo system_Attrib_T1564.001 >> #{file_to_modify}
```

rΦ

## Atomic Test #4 - Create Windows Hidden File with Attrib

Creates a file and marks it as hidden using the attrib.exe utility. Upon execution, open File Epxplorer and enable View > Hidden Items. Then, open Properties > Details on the file and observe that the Attributes are "SH" for System and Hidden.

Supported Platforms: Windows

auto\_generated\_guid: dadb792e-4358-4d8d-9207-b771faa0daa5

Inputs:

Name	Description	Туре	Default Value
------	-------------	------	---------------

file_to_modify File to modify using Attrib command String %	%temp%\T1564.001.txt
---	----------------------

#### Attack Commands: Run with command\_prompt! Elevation Required (e.g. root or admin)

```
attrib.exe +h #{file_to_modify}
```

#### **Cleanup Commands:**

```
del /A:H #{file_to_modify} >nul 2>&1
```

Dependencies: Run with command\_prompt!

Description: The file must exist on disk at specified location (#{file\_to\_modify})

**Check Prereq Commands:** 

```
IF EXIST #{file_to_modify} ( EXIT 0 ) ELSE ( EXIT 1 )
```

#### **Get Prereq Commands:**

```
echo system_Attrib_T1564.001 >> #{file_to_modify}
```

### Atomic Test #5 - Hidden files

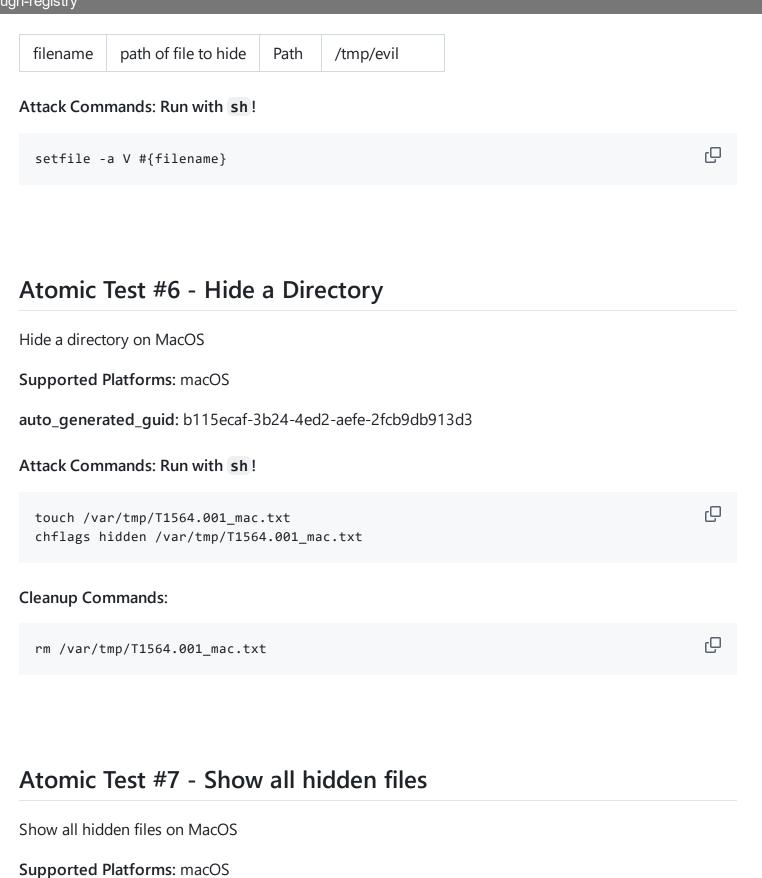
Requires Apple Dev Tools

Supported Platforms: macOS

auto\_generated\_guid: 3b7015f2-3144-4205-b799-b05580621379

Inputs:

Name	Description	Туре	Default Value
------	-------------	------	---------------



 $\equiv$ 

Preview

Code

Blame

atomic-red-team/atomics/T1564.001/T1564.001.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 20:07 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md#atomic-test-8---hide-files-through-registry

Attack Commands: Run with sh!	
defaults write com.apple.finder AppleShowAllFiles YES	C
Cleanup Commands:	
defaults write com.apple.finder AppleShowAllFiles NO	<sub>C</sub>

# Atomic Test #8 - Hide Files Through Registry

Disable Show Hidden files switch in registry. This technique was abused by several malware to hide their files from normal user. See how this trojan abuses this technique - <a href="https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Tiotua-P/detailed-analysis.aspx">https://www.sophos.com/en-us/threat-analyses/viruses-and-spyware/W32~Tiotua-P/detailed-analysis.aspx</a>

Supported Platforms: Windows

auto\_generated\_guid: f650456b-bd49-4bc1-ae9d-271b5b9581e7

Attack Commands: Run with command\_prompt! Elevation Required (e.g. root or admin)

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowSu| Creg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Hidden

### **Cleanup Commands:**

reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v SI reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v H: