

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
```

Cleanup Commands:

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

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 00 40 00
```

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	Type	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}
```

Cleanup Commands:

```
del /A:S #{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 #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	Type	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

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

Inputs:

Name	Description	Type	Default Value
filename	path of file to hide	Path	/tmp/evil

Attack Commands: Run with `sh` !

```
setfile -a V #{filename}
```

Atomic Test #6 - Hide a Directory

Hide a directory on MacOS

Supported Platforms: macOS

auto_generated_guid: b115ecaf-3b24-4ed2-ae2e-2fcb9db913d3

Attack Commands: Run with `sh` !

```
touch /var/tmp/T1564.001_mac.txt
chflags hidden /var/tmp/T1564.001_mac.txt
```

Cleanup Commands:

```
rm /var/tmp/T1564.001_mac.txt
```

Atomic Test #7 - Show all hidden files

Show all hidden files on MacOS

Supported Platforms: macOS

atomic-red-team / atomics / T1564.001 / T1564.001.md ↑ Top

Preview

Code

Blame

323 lines (158 loc) · 7.7 KB

Raw

```
defaults write com.apple.finder AppleShowAllFiles YES
```































Cleanup Commands:

```
defaults write com.apple.finder AppleShowAllFiles NO
```

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 - <https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Tiotua-P/detailed-analysis.aspx>

Supported Platforms: Windows

- >  T1000
- >  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
- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

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
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
```

Cleanup Commands:

```
reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Adva
reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Adva
```