T1070.004 - File Deletion

Description from ATT&CK

> Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.
> There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in Command and Scripting Interpreter functions include `del` on Windows and `rm` or `unlink` on Linux and macOS.

Atomic Tests

- Atomic Test #1 - Delete a single file - Linux/macOS
- Atomic Test #2 - Delete an entire folder - Linux/macOS

Atomic Test #1 - Delete a single file - Linux/macOS

Delete a single file from the temporary directory

Supported Platforms: Linux, macOS

auto_generated_guid: 562d737f-2fc6-4b09-8c2a-7f8ff0828480

Inputs:

Name	Description	Type	Default Value
file_to_delete	Path of file to delete	Path	/tmp/victim-files/a

Attack Commands: Run with `sh`!

```
rm -f #{file_to_delete}
```

Atomic Test #2 - Delete an entire folder - Linux/macOS

Recursively delete the temporary directory and all files contained within it

Supported Platforms: Linux, macOS

auto_generated_guid: a415f17e-ce8d-4ce2-a8b4-83b674e7017e

Inputs:

Name	Description	Type	Default Value
folder_to_delete	Path of folder to delete	Path	/tmp/victim-files

Attack Commands: Run with `sh`!

```
rm -rf #{folder_to_delete}
```

Atomic Test #3 - Overwrite and delete a file with shred

Use the `shred` command to overwrite the temporary file and then delete it

Supported Platforms: Linux

auto_generated_guid: 039b4b10-2900-404b-b67f-4b6d49aa6499

Inputs:

Name	Description	Type	Default Value
file_to_shred	Path of file to shred	Path	/tmp/victim-shred.txt

Attack Commands: Run with `sh`!

```
shred -u #{file_to_shred}
```

Atomic Test #4 - Delete a single file - Windows cmd

Delete a single file from the temporary directory using cmd.exe. Upon execution, no output will be displayed. Use File Explorer to verify the file was deleted.

Supported Platforms: Windows

auto_generated_guid: 861ea0b4-708a-4d17-848d-186c9c7f17e3

Inputs:

Name	Description	Type	Default Value
file_to_delete	File to delete. Run the prereq command to create it if it does not exist.	String	%temp%\deleteme_T1551.004

Attack Commands: Run with `command_prompt`!

```
del /f #{file_to_delete}
```

Dependencies: Run with `command_prompt`!

Description: The file to delete must exist on disk at specified location (#{file_to_delete})

Check Prereq Commands:

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

Get Prereq Commands:

```
echo deleteme_T1551.004 >> #{file_to_delete}
```

Atomic Test #5 - Delete an entire folder - Windows cmd

Recursively delete a folder in the temporary directory using cmd.exe. Upon execution, no output will be displayed. Use File Explorer to verify the folder was deleted.

Supported Platforms: Windows

auto_generated_guid: ded937c4-2add-42f7-9c2c-c742b7a98698

Inputs:

Name	Description	Type	Default Value
folder_to_delete	Folder to delete. Run the prereq command to create it if it does not exist.	String	%temp%\deleteme_T1551.004

Attack Commands: Run with `command_prompt`!

```
rmdir /s /q #{folder_to_delete}
```

Dependencies: Run with `command_prompt`!

Description: The file to delete must exist on disk at specified location (#{folder_to_delete})

Check Prereq Commands:

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

Get Prereq Commands:

```
mkdir #{folder_to_delete}
```

Atomic Test #6 - Delete a single file - Windows PowerShell

Delete a single file from the temporary directory using Powershell. Upon execution, no output will be displayed. Use File Explorer to verify the file was deleted.

Supported Platforms: Windows

auto_generated_guid: 9dee89bd-9a98-4c4f-9e2d-4256690b0e72

Inputs:

Name	Description	Type	Default Value
file_to_delete	File to delete. Run the prereq command to create it if it does not exist.	String	$env:TEMP\deleteme_T1551.004

Attack Commands: Run with `powershell`!

```
Remove-Item -path #{file_to_delete}
```

Dependencies: Run with `powershell`!

Description: The file to delete must exist on disk at specified location (#{file_to_delete})

Check Prereq Commands:

```
if (Test-Path #{file_to_delete}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Path #{file_to_delete} | Out-Null
```

Atomic Test #7 - Delete an entire folder - Windows PowerShell

Recursively delete a folder in the temporary directory using Powershell. Upon execution, no output will be displayed. Use File Explorer to verify the folder was deleted.

Supported Platforms: Windows

auto_generated_guid: edd779e4-a509-4cba-8dfa-a112543dbfb1

Inputs:

Name	Description	Type	Default Value
folder_to_delete	Folder to delete. Run the prereq command to create it if it does not exist.	String	$env:TEMP\deleteme_folder_T1551.004

Attack Commands: Run with `powershell`!

```
Remove-Item -Path #{folder_to_delete} -Recurse
```

Dependencies: Run with `powershell`!

Description: The folder to delete must exist on disk at specified location (#{folder_to_delete})

Check Prereq Commands:

```
if (Test-Path #{folder_to_delete}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Path #{folder_to_delete} -Type Directory | Out-Null
```

Atomic Test #8 - Delete Filesystem - Linux

This test deletes the entire root filesystem of a Linux system. This technique was used by Amnesia IoT malware to avoid analysis. This test is dangerous and destructive, do NOT use on production equipment.

Supported Platforms: Linux

auto_generated_guid: f3aa95fe-4f10-4485-ad26-abf22a764c52

Attack Commands: Run with `bash`!

```
rm -rf / --no-preserve-root > /dev/null 2> /dev/null
```

Atomic Test #9 - Delete Prefetch File

Delete a single prefetch file. Deletion of prefetch files is a known anti-forensic technique. To verify execution, Run "(Get-ChildItem -Path "$Env:SystemRoot\prefetch*.pf" | Measure-Object).Count" before and after the test to verify that the number of prefetch files decreases by 1.

Supported Platforms: Windows

auto_generated_guid: 36f96049-0ad7-4a5f-8418-460acaeb92fb

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

```
Remove-Item -Path (Join-Path "$Env:SystemRoot\prefetch\" (Get-ChildItem -Path "$Env
```

Atomic Test #10 - Delete TeamViewer Log Files

Adversaries may delete TeamViewer log files to hide activity. This should provide a high true-positive alert ration. This test just places the files in a non-TeamViewer folder, a detection would just check for a deletion event matching the TeamViewer log file format of TeamViewer_##.log. Upon execution, no output will be displayed. Use File Explorer to verify the folder was deleted.

https://twitter.com/SBousseaden/status/1197524463304290305?s=20

Supported Platforms: Windows

auto_generated_guid: 69f50a5f-967c-4327-a5bb-e1a9a9983785

Inputs:

Name	Description	Type	Default Value
teamviewer_log_file	Teamviewer log file to delete. Run the prereq command to create it if it does not exist.	String	$env:TEMP\TeamViewer_54.log

Attack Commands: Run with `powershell`!

```
Remove-Item #{teamviewer_log_file}
```

Dependencies: Run with `powershell`!

Description: The folder to delete must exist on disk at specified location (#{teamviewer_log_file})

Check Prereq Commands:

```
if (Test-Path #{teamviewer_log_file}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Path #{teamviewer_log_file} | Out-Null
```