T1030 - Data Transfer Size Limits

Description from ATT&CK

> An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

Atomic Tests

- Atomic Test #1 - Data Transfer Size Limits

Atomic Test #1 - Data Transfer Size Limits

Take a file/directory, split it into 5Mb chunks

Supported Platforms: macOS, Linux

auto_generated_guid: ab936c51-10f4-46ce-9144-e02137b2016a

Inputs:

Name	Description	Type	Default Value
file_name	File name	Path	T1030_urandom
folder_path	Path where the test creates artifacts	Path	/tmp/T1030

Attack Commands: Run with `sh`!

```
cd #{folder_path}; split -b 5000000 #{file_name}
ls -l #{folder_path}
```

Cleanup Commands:

```
if [ -f #{folder_path}/safe_to_delete ]; then rm -rf #{folder_path}; fi;
```

Dependencies: Run with `sh`!

Description: The file must exist for the test to run.

Check Prereq Commands:

```
if [ ! -f #{folder_path}/#{file_name} ]; then exit 1; else exit 0; fi;
```

Get Prereq Commands:

```
if [ ! -d #{folder_path} ]; then mkdir -p #{folder_path}; touch #{folder_path}/safe
```