.. /Tar.exe

Alternate data streams (Compression) | Copy (Compression)

Used by Windows to extract and create archives.

Paths:
C:\Windows\System32\tar.exe
C:\Windows\SysWOW64\tar.exe

Resources:
- https://twitter.com/Cyber_Sorcery/status/1619819249886969856

Acknowledgements:
- Brian Lucero (@Cyber_Sorcery)
- Avester Fahimipour

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/e1a713d264ac072bb76b5c4e5f41315a015d3f41/rules/windows/process_creation/proc_creation_win_tar_compression.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/e1a713d264ac072bb76b5c4e5f41315a015d3f41/rules/windows/process_creation/proc_creation_win_tar_extraction.yml
- IOC: tar.exe extracting files from a remote host within the environment
- IOC: Abnormal processes spawning tar.exe
- IOC: tar.exe interacting with alternate data streams (ADS)

Alternate data streams

. Compress one or more files to an alternate data stream (ADS).

```
tar -cf compressedfilename:ads C:\folder\file
```

Use case:	Can be used to evade defensive countermeasures, or to hide as part of a persistence mechanism
Privileges required:	User
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1564.004
Tags:	Type: Compression

. Decompress a compressed file from an alternate data stream (ADS).

```
tar -xf compressedfilename:ads
```

Use case: Can be used to evade defensive countermeasures, or to hide as part of a persistence mechanism
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1564.004
Tags: Type: Compression

Copy

Extracts archive.tar from the remote (internal) host (host1) to the current host.

```
tar -xf \\host1\archive.tar
```

Use case: Copy files
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1105
Tags: Type: Compression