.. /Msdeploy.exe

Execute | AWL bypass | Copy

Microsoft tool used to deploy Web Applications.

Paths:
C:\Program Files\IIS\Microsoft Web Deploy V2\msdeploy.exe
C:\Program Files (x86)\IIS\Microsoft Web Deploy V2\msdeploy.exe
C:\Program Files\IIS\Microsoft Web Deploy V3\msdeploy.exe
C:\Program Files (x86)\IIS\Microsoft Web Deploy V3\msdeploy.exe
C:\Program Files\IIS\Microsoft Web Deploy V4\msdeploy.exe
C:\Program Files (x86)\IIS\Microsoft Web Deploy V4\msdeploy.exe
C:\Program Files\IIS\Microsoft Web Deploy V5\msdeploy.exe
C:\Program Files (x86)\IIS\Microsoft Web Deploy V5\msdeploy.exe

Resources:
- https://twitter.com/pabraeken/status/995837734379032576
- https://twitter.com/pabraeken/status/999090532839313408

Acknowledgements:
- Pierre-Alexandre Braeken (@pabraeken)
- Avihay Eldad (@AvihayEldad)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_msdeploy.yml

Execute

Launch calc.bat via msdeploy.exe.

```
msdeploy.exe -verb:sync -source:RunCommand -dest:runCommand="c:\temp\calc.bat"
```

Use case: Local execution of batch file using msdeploy.exe.
Privileges required: User
Operating systems: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server
ATT&CK® technique: T1218

AWL bypass

Launch calc.bat via msdeploy.exe.

```
msdeploy.exe -verb:sync -source:RunCommand -dest:runCommand="c:\temp\calc.bat"
```

Use case: Local execution of batch file using msdeploy.exe.
Privileges required: User
Operating systems: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server
ATT&CK® technique: T1218

Copy

Copy file from source to destination.

```
msdeploy.exe -verb:sync -source:filePath=C:\windows\system32\calc.exe -dest:filePath=C:\Users\Public\calc.exe
```

Use case: Copy file.
Privileges required: User
Operating systems: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server
ATT&CK® technique: T1105