.. /coregen.exe

Execute (DLL) | AWL bypass (DLL)

Binary coregen.exe (Microsoft CoreCLR Native Image Generator) loads exported function GetCLRRuntimeHost from coreclr.dll or from .DLL in arbitrary path. Coregen is located within "C:\Program Files (x86)\Microsoft Silverlight\5.1.50918.0" or another version of Silverlight. Coregen is signed by Microsoft and bundled with Microsoft Silverlight.

Paths:
C:\Program Files\Microsoft Silverlight\5.1.50918.0\coregen.exe
C:\Program Files (x86)\Microsoft Silverlight\5.1.50918.0\coregen.exe

Resources:
- https://www.youtube.com/watch?v=75XlmxOOlnU
- https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html

Acknowledgements:
- Nicky Tyrer
- Evan Pena
- Casey Erikson

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/image_load/image_load_side_load_coregen.yml
- IOC: coregen.exe loading .dll file not in "C:\Program Files (x86)\Microsoft Silverlight\5.1.50918.0\"
- IOC: coregen.exe loading .dll file not named coreclr.dll
- IOC: coregen.exe command line containing -L or -l
- IOC: coregen.exe command line containing unexpected/invald assembly name
- IOC: coregen.exe application crash by invalid assembly name

Execute

. Loads the target .DLL in arbitrary path specified with /L.

```
coregen.exe /L C:\folder\evil.dll dummy_assembly_name
```

Use case:	Execute DLL code
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1055
Tags:	Execute: DLL

. Loads the coreclr.dll in the corgen.exe directory (e.g. C:\Program Files\Microsoft Silverlight\5.1.50918.0).

```
coregen.exe dummy_assembly_name
```

Use case: Execute DLL code
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1055

AWL bypass

Loads the target .DLL in arbitrary path specified with /L. Since binary is signed it can also be used to bypass application whitelisting solutions.

```
coregen.exe /L C:\folder\evil.dll dummy_assembly_name
```

Use case: Execute DLL code
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218
Tags: Execute: DLL