.. /Infdefaultinstall.exe

Execute

Binary used to perform installation based on content inside inf files

Paths:
C:\Windows\System32\Infdefaultinstall.exe
C:\Windows\SysWOW64\Infdefaultinstall.exe

Resources:
- https://twitter.com/KyleHanslovan/status/911997635455852544
- https://blog.conscioushacker.io/index.php/2017/10/25/evading-microsofts-autoruns/
- https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/

Acknowledgements:
- Kyle Hanslovan (@kylehanslovan)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_infdefaultinstall_execute_sct_scripts.yml
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Execute

Executes SCT script using scrobj.dll from a command in entered into a specially prepared INF file.

```
InfDefaultInstall.exe Infdefaultinstall.inf
```

Use case: Code execution
Privileges required: Admin
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218