System Binary Proxy Execution: Regsvcs/Regasm, Sub-technique T1218.009 - Enterprise

Archived: 2026-04-02 11:19:19 UTC

Adversaries may abuse Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are binaries that may be digitally signed by Microsoft. [1] [2]

Both utilities may be used to bypass application control through use of attributes within the binary to specify code that should be run before registration or unregistration: `[ComRegisterFunction]` or `[ComUnregisterFunction]` respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute. [3][4]
