# TTP Detail – T1218.009

## TTP Information

Name: Regsvcs/Regasm

Description: 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](https://attack.mitre.org/techniques/T1559/001) (COM) assemblies. Both are binaries that may be digitally signed by Microsoft. (Citation: MSDN Regsvcs) (Citation: MSDN Regasm)

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: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> 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. (Citation: LOLBAS Regsvcs)(Citation: LOLBAS Regasm)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Agent Tesla