System Binary Proxy Execution: Regsvr32, Sub-technique T1218.010 - Enterprise

Archived: 2026-04-05 12:48:49 UTC

Adversaries may abuse Regsvr32.exe to proxy execution of malicious code. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. The Regsvr32.exe binary may also be signed by Microsoft. [1]

Malicious usage of Regsvr32.exe may avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of allowlists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe can also be used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions. Since Regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. [2] This variation of the technique is often referred to as a "Squiblydoo" and has been used in campaigns targeting governments. [3] [4]

Regsvr32.exe can also be leveraged to register a COM Object used to establish persistence via Component Object Model Hijacking. [3]

Source: https://attack.mitre.org/techniques/T1218/010