Remote Services: Distributed Component Object Model, Sub-technique T1021.003 - Enterprise

Archived: 2026-04-05 13:31:53 UTC

Adversaries may use Valid Accounts to interact with remote machines by taking advantage of Distributed Component Object Model (DCOM). The adversary may then perform actions as the logged-on user.

The Windows Component Object Model (COM) is a component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE). Distributed COM (DCOM) is transparent middleware that extends the functionality of COM beyond a local computer using remote procedure call (RPC) technology.[1][2]

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry.[3] By default, only Administrators may remotely activate and launch COM objects through DCOM.[4]

Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications[5] as well as other Windows objects that contain insecure methods.[6][7] DCOM can also execute macros in existing documents[8] and may also invoke Dynamic Data Exchange (DDE) execution directly through a COM created instance of a Microsoft Office application[9], bypassing the need for a malicious document. DCOM can be used as a method of remotely interacting with Windows Management Instrumentation. [10]

Source: https://attack.mitre.org/techniques/T1021/003