# TTP Detail – T1021.003

## TTP Information

Name: Distributed Component Object Model

Description: Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) 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.(Citation: Fireeye Hunting COM June 2019)(Citation: Microsoft COM)

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry.(Citation: Microsoft Process Wide Com Keys) By default, only Administrators may remotely activate and launch COM objects through DCOM.(Citation: Microsoft COM ACL)

Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications(Citation: Enigma Outlook DCOM Lateral Movement Nov 2017) as well as other Windows objects that contain insecure methods.(Citation: Enigma MMC20 COM Jan 2017)(Citation: Enigma DCOM Lateral Movement Jan 2017) DCOM can also execute macros in existing documents(Citation: Enigma Excel DCOM Sept 2017) and may also invoke [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) (DDE) execution directly through a COM created instance of a Microsoft Office application(Citation: Cyberreason DCOM DDE Lateral Movement Nov 2017), bypassing the need for a malicious document. DCOM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). (Citation: MSDN WMI)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: lateral-movement

## Malware

* Cobalt Strike

## Tools

* Empire
* SILENTTRINITY