What is DCOM lateral movement?

DCOM (Distributed Component Object Model) lets a program on one Windows machine instantiate and call COM objects on another. Some exposed objects, such as MMC20.Application, ShellWindows, and ShellBrowserWindow, have methods that execute shell commands, so an attacker with admin rights can run code on a remote host through DCOM. It is a less-monitored lateral-movement path than PsExec or WMI, driven from PowerShell with the target's ProgID/CLSID.

HOW IT WORKS

01 The abuse and payload

From a machine with admin rights to the target, the attacker instantiates a command-capable DCOM object remotely:

- MMC20.Application:
  `$c=[activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","10.0.0.5"));`
  `$c.Document.ActiveView.ExecuteShellCommand("cmd.exe",$null,"/c calc.exe","7")`
- ShellWindows / ShellBrowserWindow expose similar `Document.Application.ShellExecute` paths via their CLSID.

No new service is created and execution comes through DCOM, so it evades detections focused on PsExec or WMI. Documented techniques shown for defenders.

> LESS WATCHED
>
> *DCOM execution is chosen precisely because many defenders watch PsExec and WMI but not DCOM object instantiation. Detection should include remote DCOM activity for command-capable objects.*

HOW TO DEFEND

- Restrict DCOM with the firewall and DCOM/COM security settings so only management hosts can reach it.
- Limit local-administrator rights and use LAPS, since DCOM execution still needs admin on the target.
- Harden or disable risky DCOM objects where feasible.
- Monitor for remote instantiation of command-capable DCOM objects (MMC20.Application, ShellWindows) and child processes spawned by them.
- Reduce NTLM and enforce strong authentication.

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] Microsoft: Distributed COM (DCOM)

[3] NIST SP 800-115 Technical Guide to Security Testing

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/what-is-dcom-lateral-movement

Open online