What is GPO abuse?

GPO abuse is the exploitation of write access to a Group Policy Object (or its SYSVOL files) to push a malicious policy across everything the GPO applies to. A single editable GPO linked to many machines becomes mass code execution, an immediate scheduled task that adds a local admin or runs a payload on every target. Because GPO permissions are often over-granted, this is a common escalation and lateral-movement path. Defend by auditing GPO write access and monitoring SYSVOL changes.

HOW IT WORKS

01 How the attack works

With write access to a target GPO the attacker uses `SharpGPOAbuse` (or pyGPOAbuse) to add an immediate scheduled task, a startup script, or a new local administrator that applies to every machine in scope. On the next policy refresh, the payload runs across all of them. Finding the writable GPO is usually the recon step; the push itself is a single command. Payloads are shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Group Policy overview

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/gpo-abuse

Open online