Behavior-chain detection for T1135 Network Share Discovery across Windows, Linux, and macOS, Detection Strategy DET0182

Archived: 2026-04-05 16:03:00 UTC

AN0513

Process or script enumerates network shares via CLI (net view/net share, PowerShell Get-SmbShare/WMI) or OS APIs (NetShareEnum/ srvsvc.NetShareEnumAll RPC) → bursts of outbound SMB/RPC connections (445/139, \host\IPC$ / srvsvc) to many hosts inside a short window → optional follow-on file listing or copy operations.

Log Sources

Mutable Elements

Field	Description
BurstHostThreshold	Minimum number of unique destination hosts over SMB within TimeWindow to treat as scanning (e.g., ≥5).
TimeWindow	Correlation window between the discovery process start and SMB fan-out (default 10m).
AllowedDiscoveryAccounts	Service/admin accounts legitimately running inventory scripts.
PipeNameAllowList	Pipes (e.g., \PIPE\spoolss) normally accessed by management agents; exclude from alerts.

AN0514

CLI tools (smbclient -L, smbmap, rpcclient, nmblookup) or custom scripts enumerate SMB shares on many internal hosts → corresponding SMB connections (445/139) captured by Zeek/Netflow within a short window.

Log Sources

Mutable Elements

Field	Description
BurstHostThreshold	Minimum unique hosts to flag (e.g., ≥5).
TimeWindow	Correlation window between tool exec and SMB fan-out (default 10m).
ApprovedInventoryHosts	IPs of vulnerability scanners or config mgmt systems.

AN0515

Use of native/mac tools (sharing -l, smbutil view, mount_smbfs) or scripts to enumerate SMB shares across many hosts, followed by outbound SMB connections observed in PF/Zeek logs.

Log Sources

Mutable Elements

Field	Description
BurstHostThreshold	Minimum unique SMB destinations (e.g., ≥3–5 in smaller mac fleets).
TimeWindow	Correlation window between exec and SMB connections (default 10m).
AllowedMgmtTools	Jamf/IT scripts legitimately running smbutil/mount_smbfs.
