Detection fo Remote Service Session Hijacking for RDP., Detection Strategy DET0588

Archived: 2026-04-05 15:42:12 UTC

Analytics

- Windows

AN1620

Detection of suspicious use of `tscon.exe` or equivalent methods to hijack legitimate RDP sessions. Defenders can observe anomalies such as session reassignments without corresponding authentication, processes spawned in the context of hijacked sessions, or unusual RDP network traffic flows that deviate from expected baselines.

Log Sources

Mutable Elements

Field	Description
ExpectedRDPHosts	Whitelist of systems and accounts authorized to use RDP; deviations indicate possible hijacking.
TimeWindow	Time threshold for correlating logon events with session reassignment and process execution.
SessionIDMapping	Environment-specific mapping of user accounts to session IDs; inconsistencies may reveal hijacking.
