Behavior-chain detection for T1134.001 Access Token Manipulation: Token Impersonation/Theft on Windows, Detection Strategy DET0482

Archived: 2026-04-05 16:36:17 UTC

AN1324

Detection of token duplication and impersonation attempts by correlating suspicious command-line executions (e.g., runas) with API calls to DuplicateToken, DuplicateTokenEx, ImpersonateLoggedOnUser, or SetThreadToken. The chain includes the initial command execution or in-memory API invocation → token handle duplication or thread token assignment → a new or existing process assuming the impersonated user's context.

Log Sources

Mutable Elements

Field	Description
AllowedSystemProcesses	Whitelist of known processes that legitimately duplicate tokens (e.g., services.exe).
TimeWindow	Time interval between API call and subsequent impersonated process (e.g., 5m).
UserContextFilter	Filter for service accounts or known administrative accounts that perform legitimate impersonation.
ParentProcessAnomalyThreshold	Threshold for parent-child process lineage anomalies indicating token theft.
