Access Token Manipulation: SID-History Injection, Sub-technique T1134.005 - Enterprise

Archived: 2026-04-05 13:18:16 UTC

Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. [1] An account can hold additional SIDs in the SID-History Active Directory attribute [2], allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

With Domain Administrator (or equivalent) rights, harvested or well-known SID values [3] may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as Remote Services, SMB/Windows Admin Shares, or Windows Remote Management.

Source: https://attack.mitre.org/techniques/T1134/005