

Detection Strategy for Hidden User Accounts, Detection Strategy DET0353

Archived: 2026-04-05 17:27:21 UTC

AN1001

Registry modifications to HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList setting user visibility to 0, or creation of user accounts not shown on login screen. Defender view: correlation of account creation with registry edits that mark users hidden.

Log Sources

Mutable Elements

| Field | Description |
|---------------------|---|
| AccountScope | Restrict monitoring to privileged or unexpected accounts. |
| BaselineHiddenUsers | Whitelist accounts that are intentionally hidden by administrators. |

AN1002

Use of gsettings or direct Display Manager modifications to hide users from greeter login screen. Defender view: anomalous command execution modifying org.gnome.login-screen or other greeter configurations.

Log Sources

| Data Component | Name | Channel |
|---|---------------|---|
| Command Execution (DC0064) | auditd:EXECVE | Execution of gsettings set org.gnome.login-screen disable-user-list true |
| File Modification (DC0061) | auditd:FILE | Modification of Display Manager configuration files (/etc/gdm3/*, /etc/lightdm/*) |

Mutable Elements

| Field | Description |
|---------------------|--|
| DisplayManagerScope | Specify which Display Managers are in use to minimize noise. |

AN1003

User creation or modification via dscl with IsHidden=1, UID<500, or plist edits to com.apple.loginwindow Hide500Users flag. Defender view: correlation of hidden account attributes with login screen exclusion.

Log Sources

Mutable Elements

| Field | Description |
|--------------|---|
| UIDThreshold | Tune detection based on acceptable UID ranges for hidden/system accounts. |
| PlistScope | Restrict plist monitoring to com.apple.loginwindow to reduce false positives. |

Source: <https://attack.mitre.org/detectionstrategies/DET0353>