Credentials from Password Stores: Keychain, Sub-technique T1555.001 - Enterprise

Archived: 2026-04-05 18:30:23 UTC

Adversaries may acquire credentials from Keychain. Keychain (or Keychain Services) is the macOS credential management system that stores account names, passwords, private keys, certificates, sensitive application data, payment data, and secure notes. There are three types of Keychains: Login Keychain, System Keychain, and Local Items (iCloud) Keychain. The default Keychain is the Login Keychain, which stores user passwords and information. The System Keychain stores items accessed by the operating system, such as items shared among users on a host. The Local Items (iCloud) Keychain is used for items synced with Apple's iCloud service.

Keychains can be viewed and edited through the Keychain Access application or using the command-line utility `security`. Keychain files are located in `~/Library/Keychains/`, `/Library/Keychains/`, and `/Network/Library/Keychains/`.[1][2][3]

Adversaries may gather user credentials from Keychain storage/memory. For example, the command `security dump-keychain -d` will dump all Login Keychain credentials from `~/Library/Keychains/login.keychain-db`. Adversaries may also directly read Login Keychain credentials from the `~/Library/Keychains/login.keychain` file. Both methods require a password, where the default password for the Login Keychain is the current user's password to login to the macOS host.[4][5]

Source: https://attack.mitre.org/techniques/T1555/001