Credentials from Password Stores: Password Managers, Sub-technique T1555.005 - Enterprise

Archived: 2026-04-05 18:31:52 UTC

Adversaries may acquire user credentials from third-party password managers.[1] Password managers are applications designed to store user credentials, normally in an encrypted database. Credentials are typically accessible after a user provides a master password that unlocks the database. After the database is unlocked, these credentials may be copied to memory. These databases can be stored as files on disk.[1]

Adversaries may acquire user credentials from password managers by extracting the master password and/or plain-text credentials from memory.[2][3] Adversaries may extract credentials from memory via Exploitation for Credential Access.[4]
Adversaries may also try brute forcing via Password Guessing to obtain the master password of a password manager.[5]

Source: https://attack.mitre.org/techniques/T1555/005