Steal or Forge Kerberos Tickets: Ccache Files, Sub-technique T1558.005 - Enterprise

Archived: 2026-04-05 17:04:33 UTC

Adversaries may attempt to steal Kerberos tickets stored in credential cache files (or ccache). These files are used for short term storage of a user's active session credentials. The ccache file is created upon user authentication and allows for access to multiple services without the user having to re-enter credentials.

The `/etc/krb5.conf` configuration file and the `KRB5CCNAME` environment variable are used to set the storage location for ccache entries. On Linux, credentials are typically stored in the `/tmp` directory with a naming format of `krb5cc_%UID%` or `krb5.ccache`. On macOS, ccache entries are stored by default in memory with an `API:{uuid}` naming scheme. Typically, users interact with ticket storage using `kinit`, which obtains a Ticket-Granting-Ticket (TGT) for the principal; `klist`, which lists obtained tickets currently held in the credentials cache; and other built-in binaries.[1][2]

Adversaries can collect tickets from ccache files stored on disk and authenticate as the current user without their password to perform Pass the Ticket attacks. Adversaries can also use these tickets to impersonate legitimate users with elevated privileges to perform Privilege Escalation. Tools like Kekeo can also be used by adversaries to convert ccache files to Windows format for further Lateral Movement. On macOS, adversaries may use open-source tools or the Kerberos framework to interact with ccache files and extract TGTs or Service Tickets via lower-level APIs.[3][4][5][6]

Source: https://attack.mitre.org/techniques/T1558/005