# TTP Detail – T1558.005

## TTP Information

Name: Ccache Files

Description:
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 <code>/etc/krb5.conf</code> configuration file and the <code>KRB5CCNAME</code> 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 <code>kinit</code>, which obtains a Ticket-Granting-Ticket (TGT) for the principal; <code>klist</code>, which lists obtained tickets currently held in the credentials cache; and other built-in binaries.(Citation: Kerberos GNU/Linux)(Citation: Binary Defense Kerberos Linux)

Adversaries can collect tickets from ccache files stored on disk and authenticate as the current user without their password to perform [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003) attacks. Adversaries can also use these tickets to impersonate legitimate users with elevated privileges to perform [Privilege Escalation](https://attack.mitre.org/tactics/TA0004). Tools like Kekeo can also be used by adversaries to convert ccache files to Windows format for further [Lateral Movement](https://attack.mitre.org/tactics/TA0008). 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.(Citation: SpectorOps Bifrost Kerberos macOS 2019)(Citation: Linux Kerberos Tickets)(Citation: Brining MimiKatz to Unix)(Citation: Kekeo)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* Impacket