# TTP Detail – T1552.008

## TTP Information

Name: Chat Messages

Description: Adversaries may directly collect unsecured credentials stored or passed through user communication services. Credentials may be sent and stored in user chat communication applications such as email, chat services like Slack or Teams, collaboration tools like Jira or Trello, and any other services that support user communication. Users may share various forms of credentials (such as usernames and passwords, API keys, or authentication tokens) on private or public corporate internal communications channels.

Rather than accessing the stored chat logs (i.e., [Credentials In Files](https://attack.mitre.org/techniques/T1552/001)), adversaries may directly access credentials within these services on the user endpoint, through servers hosting the services, or through administrator portals for cloud hosted services. Adversaries may also compromise integration tools like Slack Workflows to automatically search through messages to extract user credentials. These credentials may then be abused to perform follow-on activities such as lateral movement or privilege escalation (Citation: Slack Security Risks).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

## APTs (Intrusion Sets)

* LAPSUS$