# TTP Detail – T1213.005

## TTP Information

Name: Messaging Applications

Description: Adversaries may leverage chat and messaging applications, such as Microsoft Teams, Google Chat, and Slack, to mine valuable information.

The following is a brief list of example information that may hold potential value to an adversary and may also be found on messaging applications:

\* Testing / development credentials (i.e., [Chat Messages](https://attack.mitre.org/techniques/T1552/008))
\* Source code snippets
\* Links to network shares and other internal resources
\* Proprietary data(Citation: Guardian Grand Theft Auto Leak 2022)
\* Discussions about ongoing incident response efforts(Citation: SC Magazine Ragnar Locker 2021)(Citation: Microsoft DEV-0537)

In addition to exfiltrating data from messaging applications, adversaries may leverage data from chat messages in order to improve their targeting - for example, by learning more about an environment or evading ongoing incident response efforts.(Citation: Sentinel Labs NullBulge 2024)(Citation: Permiso Scattered Spider 2023)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: collection

## APTs (Intrusion Sets)

* Fox Kitten
* LAPSUS$
* Scattered Spider