# TTP Detail – T1656

## TTP Information

Name: Impersonation

Description: Adversaries may impersonate a trusted person or organization in order to persuade and trick a target into performing some action on their behalf. For example, adversaries may communicate with victims (via [Phishing for Information](https://attack.mitre.org/techniques/T1598), [Phishing](https://attack.mitre.org/techniques/T1566), or [Internal Spearphishing](https://attack.mitre.org/techniques/T1534)) while impersonating a known sender such as an executive, colleague, or third-party vendor. Established trust can then be leveraged to accomplish an adversary’s ultimate goals, possibly against multiple victims.

In many cases of business email compromise or email fraud campaigns, adversaries use impersonation to defraud victims -- deceiving them into sending money or divulging information that ultimately enables [Financial Theft](https://attack.mitre.org/techniques/T1657).

Adversaries will often also use social engineering techniques such as manipulative and persuasive language in email subject lines and body text such as `payment`, `request`, or `urgent` to push the victim to act quickly before malicious activity is detected. These campaigns are often specifically targeted against people who, due to job roles and/or accesses, can carry out the adversary’s goal.

Impersonation is typically preceded by reconnaissance techniques such as [Gather Victim Identity Information](https://attack.mitre.org/techniques/T1589) and [Gather Victim Org Information](https://attack.mitre.org/techniques/T1591) as well as acquiring infrastructure such as email domains (i.e. [Domains](https://attack.mitre.org/techniques/T1583/001)) to substantiate their false identity.(Citation: CrowdStrike-BEC)

There is the potential for multiple victims in campaigns involving impersonation. For example, an adversary may [Compromise Accounts](https://attack.mitre.org/techniques/T1586) targeting one organization which can then be used to support impersonation against other entities.(Citation: VEC)

## Threat-Mapped Scoring

Score: 2.9

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Tools

* NPPSPY

## APTs (Intrusion Sets)

* APT41
* APT42
* Kimsuky
* LAPSUS$
* Saint Bear
* Scattered Spider
* Storm-1811