# TTP Detail – T1586.002

## TTP Information

Name: Email Accounts

Description: Adversaries may compromise email accounts that can be used during targeting. Adversaries can use compromised email accounts to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598), [Phishing](https://attack.mitre.org/techniques/T1566), or large-scale spam email campaigns. Utilizing an existing persona with a compromised email account may engender a level of trust in a potential victim if they have a relationship with, or knowledge of, the compromised persona. Compromised email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).

A variety of methods exist for compromising email accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.(Citation: AnonHBGary)(Citation: Microsoft DEV-0537) Prior to compromising email accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. Adversaries may target compromising well-known email accounts or domains from which malicious spam or [Phishing](https://attack.mitre.org/techniques/T1566) emails may evade reputation-based email filtering rules.

Adversaries can use a compromised email account to hijack existing email threads with targets of interest.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* APT28
* APT29
* HEXANE
* IndigoZebra
* Kimsuky
* LAPSUS$
* Leviathan
* Magic Hound
* OilRig
* Star Blizzard
* TA577