# TTP Detail – T1585.002

## TTP Information

Name: Email Accounts

Description: Adversaries may create email accounts that can be used during targeting. Adversaries can use accounts created with email providers to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1) Establishing email accounts may also allow adversaries to abuse free services – such as trial periods – to [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) for follow-on purposes.(Citation: Free Trial PurpleUrchin)

Adversaries may also take steps to cultivate a persona around the email account, such as through use of [Social Media Accounts](https://attack.mitre.org/techniques/T1585/001), to increase the chance of success of follow-on behaviors. Created email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).(Citation: Mandiant APT1)

To decrease the chance of physically tying back operations to themselves, adversaries may make use of disposable email services.(Citation: Trend Micro R980 2016)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* APT1
* APT42
* CURIUM
* EXOTIC LILY
* HEXANE
* Indrik Spider
* Kimsuky
* Lazarus Group
* Leviathan
* Magic Hound
* Moonstone Sleet
* Mustang Panda
* Sandworm Team
* Silent Librarian
* Star Blizzard
* Wizard Spider