# TTP Detail – T1589.002

## TTP Information

Name: Email Addresses

Description: Adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.  
  
Adversaries may easily gather email addresses, since they may be readily available and exposed via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: HackersArise Email)(Citation: CNET Leaks) Email addresses could also be enumerated via more active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)), such as probing and analyzing responses from authentication services that may reveal valid usernames in a system.(Citation: GrimBlog UsernameEnum) For example, adversaries may be able to enumerate email addresses in Office 365 environments by querying a variety of publicly available API endpoints, such as autodiscover and GetCredentialType.(Citation: GitHub Office 365 User Enumeration)(Citation: Azure Active Directory Reconnaisance)  
  
Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Email Accounts](https://attack.mitre.org/techniques/T1586/002)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Brute Force](https://attack.mitre.org/techniques/T1110) via [External Remote Services](https://attack.mitre.org/techniques/T1133)).

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## Tools

* AADInternals

## APTs (Intrusion Sets)

* APT32
* EXOTIC LILY
* HAFNIUM
* HEXANE
* Kimsuky
* LAPSUS$
* Lazarus Group
* Magic Hound
* Moonstone Sleet
* Saint Bear
* Sandworm Team
* Silent Librarian
* TA551
* Volt Typhoon