# TTP Detail – T1114

## TTP Information

Name: Email Collection

Description: Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Emails may also contain details of ongoing incident response operations, which may allow adversaries to adjust their techniques in order to maintain persistence or evade defenses.(Citation: TrustedSec OOB Communications)(Citation: CISA AA20-352A 2021) Adversaries can collect or forward email from mail servers or clients.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* Emotet
* TRANSLATEXT

## APTs (Intrusion Sets)

* Ember Bear
* Magic Hound
* Scattered Spider
* Silent Librarian