# TTP Detail – T1114.002

## TTP Information

Name: Remote Email Collection

Description: Adversaries may target an Exchange server, Office 365, or Google Workspace to collect sensitive information. Adversaries may leverage a user's credentials and interact directly with the Exchange server to acquire information from within a network. Adversaries may also access externally facing Exchange services, Office 365, or Google Workspace to access email using credentials or access tokens. Tools such as [MailSniper](https://attack.mitre.org/software/S0413) can be used to automate searches for specific keywords.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* LightNeuron
* SeaDuke
* Valak

## Tools

* MailSniper

## APTs (Intrusion Sets)

* APT1
* APT28
* APT29
* Chimera
* Dragonfly
* FIN4
* HAFNIUM
* Ke3chang
* Kimsuky
* Leafminer
* Magic Hound
* Star Blizzard