# TTP Detail – T1598.002

## TTP Information

Name: Spearphishing Attachment

Description: Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email. In some cases, they may rely upon the recipient populating information, then returning the file.(Citation: Sophos Attachment)(Citation: GitHub Phishery) The text of the spearphishing email usually tries to give a plausible reason why the file should be filled-in, such as a request for information from a business associate. In other cases, adversaries may leverage techniques such as [HTML Smuggling](https://attack.mitre.org/techniques/T1027/006) to harvest user credentials via fake login portals.(Citation: Huntress HTML Smuggling 2024)

Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## APTs (Intrusion Sets)

* Dragonfly
* SideCopy
* Sidewinder
* Star Blizzard