# TTP Detail – T1566

## TTP Information

Name: Phishing

Description: Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by [Email Spoofing](https://attack.mitre.org/techniques/T1672)(Citation: Proofpoint-spoof) the identity of the sender, which can be used to fool both the human recipient as well as automated security tools,(Citation: cyberproof-double-bounce) or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").(Citation: phishing-krebs)

Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* Hikit
* INC Ransomware
* Royal

## APTs (Intrusion Sets)

* Axiom
* GOLD SOUTHFIELD
* INC Ransom
* Kimsuky
* Sea Turtle