# TTP Detail – T1204.004

## TTP Information

Name: Malicious Copy and Paste

Description: An adversary may rely upon a user copying and pasting code in order to gain execution. Users may be subjected to social engineering to get them to copy and paste code directly into a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059).

Malicious websites, such as those used in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), may present fake error messages or CAPTCHA prompts that instruct users to open a terminal or the Windows Run Dialog box and execute an arbitrary command. These commands may be obfuscated using encoding or other techniques to conceal malicious intent. Once executed, the adversary will typically be able to establish a foothold on the victim's machine.(Citation: CloudSEK Lumma Stealer 2024)(Citation: Sekoia ClickFake 2025)(Citation: Reliaquest CAPTCHA 2024)

Adversaries may also leverage phishing emails for this purpose. When a user attempts to open an attachment, they may be presented with a fake error and offered a malicious command to paste as a solution.(Citation: Proofpoint ClickFix 2024)

Tricking a user into executing a command themselves may help to bypass email filtering, browser sandboxing, or other mitigations designed to protect users against malicious downloaded files.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution