# TTP Detail – T1674

## TTP Information

Name: Input Injection

Description: Adversaries may simulate keystrokes on a victim’s computer by various means to perform any type of action on behalf of the user, such as launching the command interpreter using keyboard shortcuts, typing an inline script to be executed, or interacting directly with a GUI-based application. These actions can be preprogrammed into adversary tooling or executed through physical devices such as Human Interface Devices (HIDs).

For example, adversaries have used tooling that monitors the Windows message loop to detect when a user visits bank-specific URLs. If detected, the tool then simulates keystrokes to open the developer console or select the address bar, pastes malicious JavaScript from the clipboard, and executes it - enabling manipulation of content within the browser, such as replacing bank account numbers during transactions.(Citation: BleepingComputer BackSwap)(Citation: welivesecurity BackSwap)

Adversaries have also used malicious USB devices to emulate keystrokes that launch PowerShell, leading to the download and execution of malware from adversary-controlled servers.(Citation: BleepingComputer USB)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## APTs (Intrusion Sets)

* FIN7