# TTP Detail – T1056

## TTP Information

Name: Input Capture

Description: Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

**•** mitre-attack: credential-access

## Malware

* Chaes
* FlawedAmmyy
* Kobalos
* Mafalda
* metaMain

## Tools

* NPPSPY

## APTs (Intrusion Sets)

* APT39
* APT42
* Storm-1811