# TTP Detail – T1056.003

## TTP Information

Name: Web Portal Capture

Description: Adversaries may install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. For example, a compromised login page may log provided user credentials before logging the user in to the service.

This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through [External Remote Services](https://attack.mitre.org/techniques/T1133) and [Valid Accounts](https://attack.mitre.org/techniques/T1078) or as part of the initial compromise by exploitation of the externally facing web service.(Citation: Volexity Virtual Private Keylogging)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

**•** mitre-attack: credential-access

## Malware

* IceApple
* WARPWIRE

## APTs (Intrusion Sets)

* Winter Vivern