# TTP Detail – T1659

## TTP Information

Name: Content Injection

Description: Adversaries may gain access and continuously communicate with victims by injecting malicious content into systems through online network traffic. Rather than luring victims to malicious payloads hosted on a compromised website (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004) followed by [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)), adversaries may initially access victims through compromised data-transfer channels where they can manipulate traffic and/or inject their own content. These compromised online network channels may also be used to deliver additional payloads (i.e., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) and other data to already compromised systems.(Citation: ESET MoustachedBouncer)

Adversaries may inject content to victim systems in various ways, including:

\* From the middle, where the adversary is in-between legitimate online client-server communications (\*\*Note:\*\* this is similar but distinct from [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557), which describes AiTM activity solely within an enterprise environment) (Citation: Kaspersky Encyclopedia MiTM)
\* From the side, where malicious content is injected and races to the client as a fake response to requests of a legitimate online server (Citation: Kaspersky ManOnTheSide)

Content injection is often the result of compromised upstream communication channels, for example at the level of an internet service provider (ISP) as is the case with "lawful interception."(Citation: Kaspersky ManOnTheSide)(Citation: ESET MoustachedBouncer)(Citation: EFF China GitHub Attack)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

**•** mitre-attack: command-and-control

## Malware

* Disco

## APTs (Intrusion Sets)

* MoustachedBouncer