Content Injection, Technique T1659 - Enterprise

Archived: 2026-04-05 12:38:16 UTC

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 followed by Drive-by Compromise), 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) and other data to already compromised systems.[1]

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, which describes AiTM activity solely within an enterprise environment) [2]
- From the side, where malicious content is injected and races to the client as a fake response to requests of a legitimate online server [3]

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."[3][1][4]

Source: https://attack.mitre.org/techniques/T1659