


[Home](#) > [Techniques](#) > [Enterprise](#) > [Proxy](#)

Proxy

Sub-techniques (4) 

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](#), [ZXProxy](#), and [ZXPortMap](#).^[1] Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

ID: T1090

Sub-techniques:
[T1090.001](#), [T1090.002](#),
[T1090.003](#), [T1090.004](#)

 **Tactic:** [Command and Control](#)

 **Platforms:** Linux, Network, Windows, macOS

Contributors: Heather Linn; Jon Sheedy; Walker Johnson

Version: 3.1

Created: 31 May 2017

Last Modified: 30 August 2021

[Version](#) [Permalink](#)

Procedure Examples

ID	Name	Description
G0096	APT41	APT41 used a tool called CLASSFON to covertly proxy network communications. ^[2]