# TTP Detail – T1090

## TTP Information

Name: Proxy

Description: 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](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) 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.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## Malware

* Aria-body
* AuditCred
* BADCALL
* BADHATCH
* Bisonal
* Cardinal RAT
* Dridex
* FunnyDream
* GoBear
* Green Lambert
* HARDRAIN
* HOPLIGHT
* KEYPLUG
* KOCTOPUS
* Kapeka
* Kessel
* LITTLELAMB.WOOLTEA
* LunarWeb
* NETWIRE
* Neo-reGeorg
* PLEAD
* RainyDay
* RansomHub
* SDBbot
* Sagerunex
* Samurai
* Socksbot
* SombRAT
* TSCookie
* TYPEFRAME
* Ursnif
* Vasport
* WarzoneRAT
* XTunnel
* ZIPLINE
* ZxShell
* jRAT
* reGeorg

## Tools

* FRP
* HTRAN
* PoshC2
* QuasarRAT
* Remcos
* netsh
* ngrok

## APTs (Intrusion Sets)

* APT41
* Blue Mockingbird
* Cinnamon Tempest
* CopyKittens
* Earth Lusca
* Fox Kitten
* LAPSUS$
* Magic Hound
* MoustachedBouncer
* POLONIUM
* Sandworm Team
* Turla
* Volt Typhoon
* Windigo