# TTP Detail – T1090.002

## TTP Information

Name: External Proxy

Description: Adversaries may use an external proxy to 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, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths to avoid suspicion.  
  
External connection proxies are used to mask the destination of C2 traffic and are typically implemented with port redirectors. Compromised systems outside of the victim environment may be used for these purposes, as well as purchased infrastructure such as cloud-based resources or virtual private servers. Proxies may be chosen based on the low likelihood that a connection to them from a compromised system would be investigated. Victim systems would communicate directly with the external proxy on the Internet and then the proxy would forward communications to the C2 server.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## Malware

* InvisiMole
* Okrum
* POWERSTATS
* QUIETEXIT
* QakBot
* Regin
* ShimRat
* TrickBot
* Winnti for Windows

## Tools

* Mythic

## APTs (Intrusion Sets)

* APT28
* APT29
* APT3
* APT39
* FIN5
* GALLIUM
* Lazarus Group
* MuddyWater
* Silence
* Tonto Team
* menuPass