# TTP Detail – T1090.001

## TTP Information

Name: Internal Proxy

Description: Adversaries may use an internal proxy to direct command and control traffic between two or more systems in a compromised environment. 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 internal proxies to manage command and control communications inside a compromised environment, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between infected systems to avoid suspicion. Internal proxy connections may use common peer-to-peer (p2p) networking protocols, such as SMB, to better blend in with the environment.

By using a compromised internal system as a proxy, adversaries may conceal the true destination of C2 traffic while reducing the need for numerous connections to external systems.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* BACKSPACE
* CHOPSTICK
* Cobalt Strike
* Drovorub
* Duqu
* FatDuke
* Gomir
* Hikit
* InvisiMole
* Kazuar
* Mafalda
* MiniDuke
* Ninja
* Pay2Key
* Stuxnet
* Winnti for Windows
* metaMain

## Tools

* Mythic
* Sliver

## APTs (Intrusion Sets)

* APT39
* FIN13
* Higaisa
* Lazarus Group
* Lotus Blossom
* Strider
* Turla
* Velvet Ant
* Volt Typhoon