# TTP Detail – T1572

## TTP Information

Name: Protocol Tunneling

Description: Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.   
  
There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel.(Citation: SSH Tunneling)(Citation: Sygnia Abyss Locker 2025)   
  
[Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19)   
  
Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol or Service Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* Cobalt Strike
* Cyclops Blink
* Duqu
* FLIPSIDE
* FunnyDream
* Heyoka Backdoor
* Industroyer
* Kevin
* LunarWeb
* Milan
* Neo-reGeorg
* QakBot
* Uroburos
* reGeorg

## Tools

* Brute Ratel C4
* FRP
* Mythic
* ngrok

## APTs (Intrusion Sets)

* Chimera
* Cinnamon Tempest
* Cobalt Group
* Ember Bear
* FIN13
* FIN6
* Fox Kitten
* Leviathan
* Magic Hound
* OilRig
* Salt Typhoon