# TTP Detail – T1071.004

## TTP Information

Name: DNS

Description: Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.(Citation: PAN DNS Tunneling)(Citation: Medium DnsTunneling)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* Anchor
* BONDUPDATER
* Cobalt Strike
* Cobian RAT
* DanBot
* DarkGate
* Denis
* DnsSystem
* Ebury
* Gelsemium
* Goopy
* Green Lambert
* HTTPBrowser
* Helminth
* Heyoka Backdoor
* InvisiMole
* Kevin
* Matryoshka
* Milan
* Mori
* NanHaiShu
* NightClub
* POWERSOURCE
* POWRUNER
* Pisloader
* PlugX
* QUADAGENT
* RDAT
* Remsec
* SOUNDBITE
* SUNBURST
* ShadowPad
* Shark
* SombRAT
* SysUpdate
* TEXTMATE
* Uroburos
* WellMess

## Tools

* Brute Ratel C4
* Mythic
* Sliver

## APTs (Intrusion Sets)

* APT18
* APT39
* APT41
* Chimera
* Cobalt Group
* Ember Bear
* FIN7
* Ke3chang
* LazyScripter
* OilRig
* Tropic Trooper