# TTP Detail – T1001

## TTP Information

Name: Data Obfuscation

Description: Adversaries may obfuscate command and control traffic to make it more difficult to detect.(Citation: Bitdefender FunnyDream Campaign November 2020) Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* DarkGate
* FRAMESTING
* FlawedAmmyy
* FunnyDream
* Ninja
* Okrum
* RDAT
* SLOTHFULMEDIA
* SideTwist
* StrelaStealer
* TrailBlazer

## APTs (Intrusion Sets)

* Gamaredon Group