# TTP Detail – T1001.001

## TTP Information

Name: Junk Data

Description: Adversaries may add junk data to protocols used for command and control to make detection more difficult.(Citation: FireEye SUNBURST Backdoor December 2020) By adding random or meaningless data to the protocols used for command and control, adversaries can prevent trivial methods for decoding, deciphering, or otherwise analyzing the traffic. Examples may include appending/prepending data with junk characters or writing junk characters between significant characters.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## Malware

* BendyBear
* Downdelph
* GoldMax
* GrimAgent
* Kevin
* Mori
* P2P ZeuS
* P8RAT
* PLEAD
* SUNBURST
* TrailBlazer
* Turian
* UPSTYLE
* Uroburos
* WellMess

## APTs (Intrusion Sets)

* APT28