# TTP Detail – T1001.002

## TTP Information

Name: Steganography

Description: Adversaries may use steganographic techniques to hide command and control traffic to make detection efforts more difficult. Steganographic techniques can be used to hide data in digital messages that are transferred between systems. This hidden information can be used for command and control of compromised systems. In some cases, the passing of files embedded using steganography, such as image or document files, can be used for command and control.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* Daserf
* Duqu
* HAMMERTOSS
* LightNeuron
* LunarMail
* LunarWeb
* RDAT
* SUNBURST
* ZeroT
* Zox

## Tools

* Sliver

## APTs (Intrusion Sets)

* Axiom