# TTP Detail – T1573

## TTP Information

Name: Encrypted Channel

Description: Adversaries may employ an encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* Chaes
* Cryptoistic
* Emotet
* Gomir
* Lizar
* MacMa
* NETWIRE
* PowGoop
* PowerLess
* RCSession
* gh0st RAT

## APTs (Intrusion Sets)

* APT29
* BITTER
* Magic Hound
* Tropic Trooper