# TTP Detail – T1048.001

## TTP Information

Name: Exfiltration Over Symmetric Encrypted Non-C2 Protocol

Description: Adversaries may steal data by exfiltrating it over a symmetrically encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Symmetric encryption algorithms are those that use shared or the same keys/secrets on each end of the channel. This requires an exchange or pre-arranged agreement/possession of the value used to encrypt and decrypt data.

Network protocols that use asymmetric encryption often utilize symmetric encryption once keys are exchanged, but adversaries may opt to manually share keys and implement symmetric cryptographic algorithms (ex: RC4, AES) vice using mechanisms that are baked into a protocol. This may result in multiple layers of encryption (in protocols that are natively encrypted such as HTTPS) or encryption in protocols that not typically encrypted (such as HTTP or FTP).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration