# TTP Detail – T1048.003

## TTP Information

Name: Exfiltration Over Unencrypted Non-C2 Protocol

Description: Adversaries may steal data by exfiltrating it over an un-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.(Citation: copy\_cmd\_cisco)

Adversaries may opt to obfuscate this data, without the use of encryption, within network protocols that are natively unencrypted (such as HTTP, FTP, or DNS). This may include custom or publicly available encoding/compression algorithms (such as base64) as well as embedding data within protocol headers and fields.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration

## Malware

* Agent Tesla
* Brave Prince
* CORALDECK
* Carbon
* CharmPower
* Cherry Picker
* CookieMiner
* CosmicDuke
* Dok
* KONNI
* Kessel
* PoetRAT
* Remsec
* SocGholish
* WARPWIRE
* WindTail
* ccf32

## Tools

* BITSAdmin
* Rclone
* ftp

## APTs (Intrusion Sets)

* APT32
* APT33
* FIN6
* FIN8
* Lazarus Group
* OilRig
* Salt Typhoon
* Thrip
* Wizard Spider