# TTP Detail – T1071.003

## TTP Information

Name: Mail Protocols

Description: Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as SMTP/S, POP3/S, and IMAP that carry electronic mail may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the email messages themselves. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.(Citation: FireEye APT28)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* Agent Tesla
* BadPatch
* CHOPSTICK
* CORESHELL
* Cannon
* ComRAT
* Goopy
* IMAPLoader
* JPIN
* LightNeuron
* LunarMail
* NavRAT
* NightClub
* OLDBAIT
* PowerExchange
* RDAT
* Remsec
* SUGARDUMP
* Uroburos
* Zebrocy

## APTs (Intrusion Sets)

* APT28
* APT32
* Kimsuky
* SilverTerrier
* Turla