# TTP Detail – T1071.005

## TTP Information

Name: Publish/Subscribe Protocols

Description: Adversaries may communicate using publish/subscribe (pub/sub) application layer protocols 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 <code>MQTT</code>, <code>XMPP</code>, <code>AMQP</code>, and <code>STOMP</code> use a publish/subscribe design, with message distribution managed by a centralized broker.(Citation: wailing crab sub/pub)(Citation: Mandiant APT1 Appendix) Publishers categorize their messages by topics, while subscribers receive messages according to their subscribed topics.(Citation: wailing crab sub/pub) An adversary may abuse publish/subscribe protocols to communicate with systems under their control from behind a message broker while also mimicking normal, expected traffic.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* GLOOXMAIL