# TTP Detail – T1559

## TTP Information

Name: Inter-Process Communication

Description: Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.

Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Cyclops Blink
* HyperStack
* LunarWeb
* Ninja
* OilBooster
* PITSTOP
* ROADSWEEP
* Raspberry Robin
* RotaJakiro
* StealBit
* Uroburos