# TTP Detail – T1480.002

## TTP Information

Name: Mutual Exclusion

Description: Adversaries may constrain execution or actions based on the presence of a mutex associated with malware. A mutex is a locking mechanism used to synchronize access to a resource. Only one thread or process can acquire a mutex at a given time.(Citation: Microsoft Mutexes)

While local mutexes only exist within a given process, allowing multiple threads to synchronize access to a resource, system mutexes can be used to synchronize the activities of multiple processes.(Citation: Microsoft Mutexes) By creating a unique system mutex associated with a particular malware, adversaries can verify whether or not a system has already been compromised.(Citation: Sans Mutexes 2012)

In Linux environments, malware may instead attempt to acquire a lock on a mutex file. If the malware is able to acquire the lock, it continues to execute; if it fails, it exits to avoid creating a second instance of itself.(Citation: Intezer RedXOR 2021)(Citation: Deep Instinct BPFDoor 2023)

Mutex names may be hard-coded or dynamically generated using a predictable algorithm.(Citation: ICS Mutexes 2015)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BPFDoor
* Black Basta
* Gazer
* GrimAgent
* LockBit 3.0
* PoisonIvy
* REvil
* SUNSPOT
* StrelaStealer
* Troll Stealer

## APTs (Intrusion Sets)

* APT38