Execution Guardrails: Mutual Exclusion, Sub-technique T1480.002 - Enterprise

Archived: 2026-04-05 15:27:05 UTC

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.[1]

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.[1] By creating a unique system mutex associated with a particular malware, adversaries can verify whether or not a system has already been compromised.[2]

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.[3][4]

Mutex names may be hard-coded or dynamically generated using a predictable algorithm.[5]

Source: https://attack.mitre.org/techniques/T1480/002