# TTP Detail – T1562.009

## TTP Information

Name: Safe Mode Boot

Description: Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.(Citation: Microsoft Safe Mode)(Citation: Sophos Snatch Ransomware 2019)

Adversaries may abuse safe mode to disable endpoint defenses that may not start with a limited boot. Hosts can be forced into safe mode after the next reboot via modifications to Boot Configuration Data (BCD) stores, which are files that manage boot application settings.(Citation: Microsoft bcdedit 2021)

Adversaries may also add their malicious applications to the list of minimal services that start in safe mode by modifying relevant Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)). Malicious [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) objects may also be registered and loaded in safe mode.(Citation: Sophos Snatch Ransomware 2019)(Citation: CyberArk Labs Safe Mode 2016)(Citation: Cybereason Nocturnus MedusaLocker 2020)(Citation: BleepingComputer REvil 2021)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* AvosLocker
* Black Basta
* LockBit 3.0
* REvil
* RansomHub