# TTP Detail – T1542

## TTP Information

Name: Pre-OS Boot

Description: Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.(Citation: Wikipedia Booting)

Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence