# TTP Detail – T1067

## TTP Information

Name: Bootkit

Description: A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). (Citation: MTrends 2016)

Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

### Master Boot Record
The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code. (Citation: Lau 2011)

### Volume Boot Record
The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to adversary code.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence