Pre-OS Boot: Bootkit, Sub-technique T1542.003 - Enterprise

Archived: 2026-04-05 14:38:59 UTC

Adversaries may use bootkits to persist on systems. A bootkit is a malware variant that modifies the boot sectors of a hard drive, allowing malicious code to execute before a computer's operating system has loaded. Bootkits reside at a layer below the operating system and may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

In BIOS systems, a bootkit may modify the Master Boot Record (MBR) and/or Volume Boot Record (VBR).[1] 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.[2]

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.

In UEFI (Unified Extensible Firmware Interface) systems, a bootkit may instead create or modify files in the EFI system partition (ESP). The ESP is a partition on data storage used by devices containing UEFI that allows the system to boot the OS and other utilities used by the system. An adversary can use the newly created or patched files in the ESP to run malicious kernel code.[3][4]
