Firmware Corruption, Technique T1495 - Enterprise

Archived: 2026-04-05 15:13:39 UTC

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.[1] Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices may include the motherboard, hard drive, or video cards.

In general, adversaries may manipulate, overwrite, or corrupt firmware in order to deny the use of the system or devices. For example, corruption of firmware responsible for loading the operating system for network devices may render the network devices inoperable.[2][3] Depending on the device, this attack may also result in Data Destruction.

Source: https://attack.mitre.org/techniques/T1495