Pre-OS Boot: TFTP Boot, Sub-technique T1542.005 - Enterprise

Archived: 2026-04-05 18:41:48 UTC

Adversaries may abuse netbooting to load an unauthorized network device operating system from a Trivial File Transfer Protocol (TFTP) server. TFTP boot (netbooting) is commonly used by network administrators to load configuration-controlled network device images from a centralized management server. Netbooting is one option in the boot sequence and can be used to centralize, manage, and control device images.

Adversaries may manipulate the configuration on the network device specifying use of a malicious TFTP server, which may be used in conjunction with Modify System Image to load a modified image on device startup or reset. The unauthorized image allows adversaries to modify device configuration, add malicious capabilities to the device, and introduce backdoors to maintain control of the network device while minimizing detection through use of a standard functionality. This technique is similar to ROMMONkit and may result in the network device running a modified image. [1]

Source: https://attack.mitre.org/techniques/T1542/005