Boot or Logon Autostart Execution: Kernel Modules and Extensions, Sub-technique T1547.006 - Enterprise

Archived: 2026-04-05 13:15:43 UTC

Adversaries may modify the kernel to automatically execute programs on system boot. Loadable Kernel Modules (LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system.[1]

When used maliciously, LKMs can be a type of kernel-mode Rootkit that run with the highest operating system privilege (Ring 0).[2] Common features of LKM based rootkits include: hiding itself, selective hiding of files, processes and network activity, as well as log tampering, providing authenticated backdoors, and enabling root access to non-privileged users.[3]

Kernel extensions, also called kext, are used in macOS to load functionality onto a system similar to LKMs for Linux. Since the kernel is responsible for enforcing security and the kernel extensions run as apart of the kernel, kexts are not governed by macOS security policies. Kexts are loaded and unloaded through `kextload` and `kextunload` commands. Kexts need to be signed with a developer ID that is granted privileges by Apple allowing it to sign Kernel extensions. Developers without these privileges may still sign kexts but they will not load unless SIP is disabled. If SIP is enabled, the kext signature is verified before being added to the AuxKC.[4]

Since macOS Catalina 10.15, kernel extensions have been deprecated in favor of System Extensions. However, kexts are still allowed as "Legacy System Extensions" since there is no System Extension for Kernel Programming Interfaces.[5]

Adversaries can use LKMs and kexts to conduct Persistence and/or Privilege Escalation on a system. Examples have been found in the wild, and there are some relevant open source projects as well.[6][7][8][9][10][11][12][13]

Source: https://attack.mitre.org/techniques/T1547/006