The attacker can pass SKEL Protection on the macOS High Sierra

The new security feature on macOS High Siera (10.13), named Secure Kernel Extension Loading, can be bypassed, allowing downloading of kernel kernel extensions.

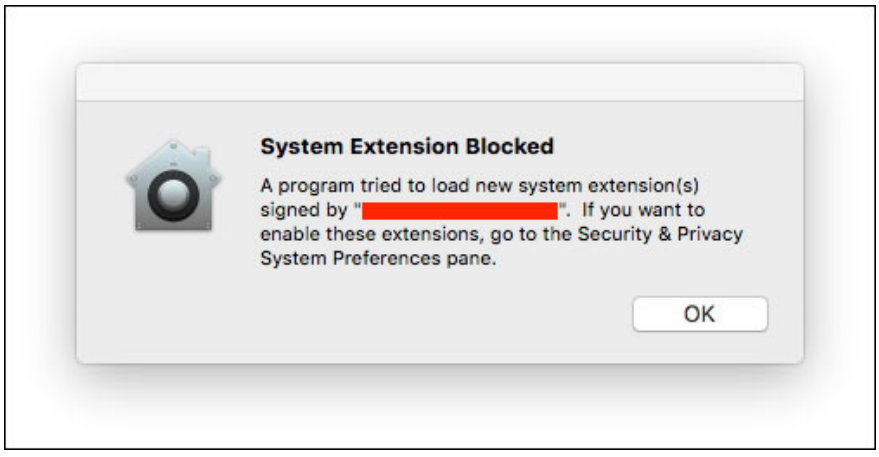
The new security feature on macOS High Siera (10.13), named Secure Kernel Extension Loading, can be bypassed, allowing downloading of kernel kernel extensions.

Like Linux and Windows, macOS allows applications to run third-party kernel extensions when running low-level OS requests.

SKEL improves the process of loading kernel extensions

Developers who want to download the kernel extension (KEXT file) during application installation need to register for that extension a kernel registration certificate, carefully selected by Apple when licensing.

MacOS High Sierra is about to release Apple to introduce SKEL, a tool to improve the security of KEXT download process. SKEL works by displaying a popup as shown below when the application tries to load the kernel extension.



Popup displays when trying to load kernel extensions

This popup window will not appear when opening a few apps from reputable developers and a few other cases are detailed in the Apple SKEL page. *https://developer.apple.com/library/content/technotes/tn2459/_index.html#//apple_ref/doc/uid/DTS40017658*

SKEL was overcome before the release of High Sierra

At first glance, macOS users will be pleased when Apple attempts to improve security on the OS with SKEL. But Patrick Wardle, an Apple security researcher and head of security research at Synack, doesn't think so.

Wardle said that Apple 's SKEL system "only prevents efforts of good intentions" (third party macOS developers such as security software designers).

He thought that 'due to the error in doing so, those who have bad intentions may not be affected' by the protection method of SKEL.

Disclosure of details on how to pass SKEL

To prove what they said, Wardle pointed out how an attacker could bypass the SKEL protection on macOS High Sierra via the Synack website *https://www.synack.com/2017/09/08/high- sierras-secure-kernel-extension-loading-is-broken /* and my personal blog. *https://objective-see.com/blog/blog_0x21.html*

'Unfortunately, when such security features are offered, even with the most attention, it only makes it difficult for third-party developers and users, while not affecting bad guys (those who are not 'playing by law.' Wardle said. 'SKEL of High Sierra is a perfect example.'

Passing SKEL is only part of the study of Wardle's techniques for overcoming KEXT downloads starting last year and was introduced in detail at the DEF CON 2016 security conference.

MacOS High Sierra will be released on September 25.