Erledigt Problem bei Combo-Update

Beitrag von „griven“ vom 13. Oktober 2018, 00:27

Solange alle OS fremden Extensions über den Booter injected werden kann man die SIP vollständig aktivieren. Die Injects der Bootloader laufen an der SIP vorbei will meinen das alles was vom Booter kommt ins System gemogelt wird bevor die SIP überhaupt greifen kann. Hier mal eine vermutlich eher laienhafte Darstellung dessen was da passiert:

-> Bootlaoader -> boot.efi -> decrompress Prelinked Kernel -> Erfolg -> Loader hängt sich ein und platziert alle zusätzlichen Extensions im Speicherbereich des entpackten Kernels und eweitert diesen sofern nötig und möglich -> Erfolg -> übergabe and boot.efi -> System start

Das System startet in dem Fall mit allen Extensions denn für macOS sieht es so aus als käme das alles aus dem prelinked Kernel und ist somit auch vertrauenswürdig denn din den prelinked Kernel können nur Extensions gelagen die gemäß SIP signiert und erlaubt sind. Eine weitere Prüfung ob das für jede Extension die im prelinkted Kernel vorhanden ist zutrifft findet nicht statt.