Dylib Hijack Scanner

download

Dylib Hijack Scanner or DHS, is a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked.

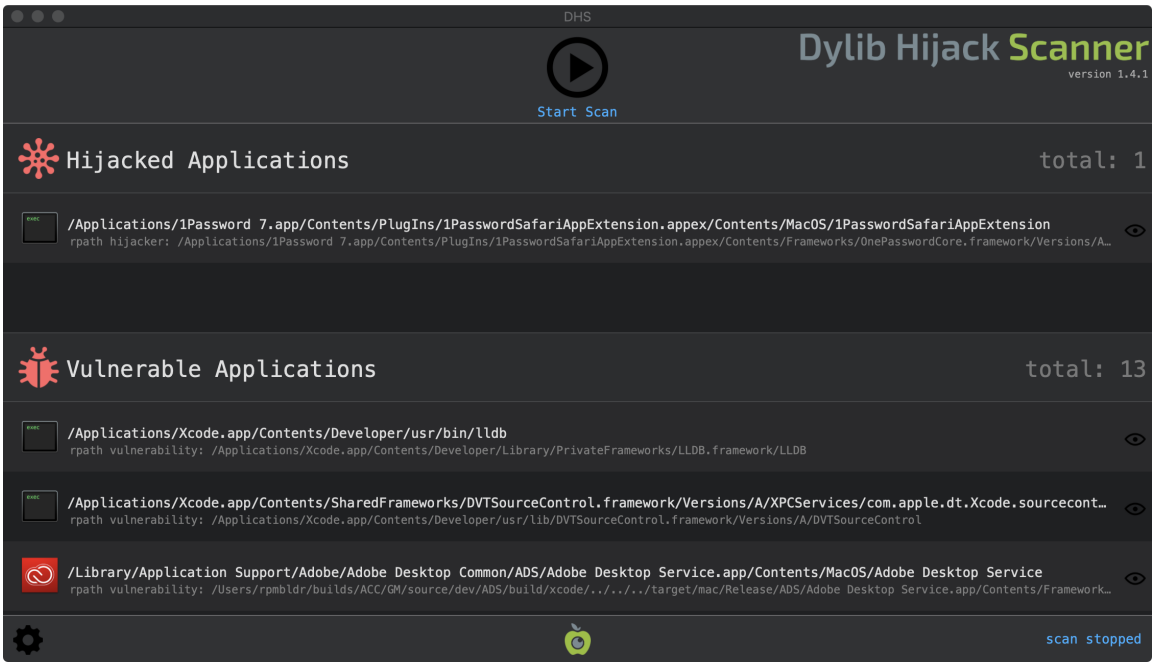
The details behind this macOS attack were presented at CanSecW, in a presentation titled, **'DLL Hijacking' on OS X? #@%& Yeah!**

Supported OS: macOS 11+

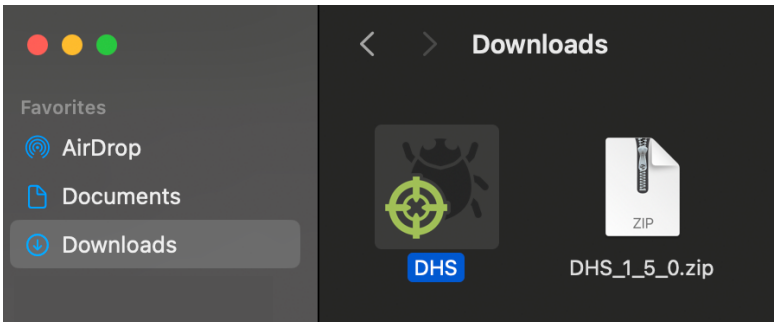
Current version: 1.5.1 (**change log**)

Zip's SHA-1: 4B76EFAE3A7E00B1034399B699861B86FFC84927

Source Code: **Dylib Hijack Scanner**

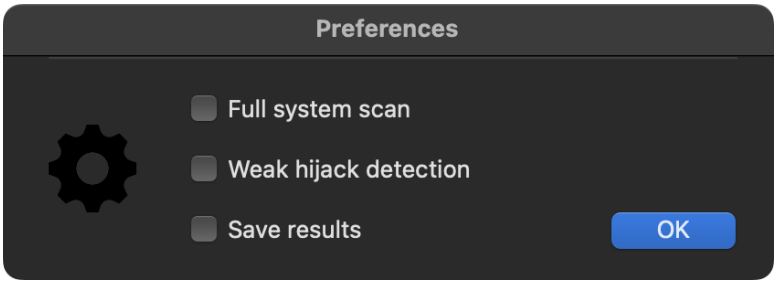


To use DHS, first **download** the zip archive containing the application. Depending on your browser, you may need to manually unzip the application by double-clicking on the zipped archive:



To run the application and begin a scan, simply double click on 'DHS.app' and press the 'Start Scan' button. DHS will then scan and detect any applications that have been hijacked, or are vulnerable to hijacking. It is likely that several vulnerable applications will be detected. This is quite common and don't mean your computer is hacked. However, if there are any applications listed under 'Hijacked Applications' this could be an issue. It may be a false positive, or an actual hijacking (see the FAQs below for details). If you need help identifying sorting this out, feel free to **email** me.

Clicking the 'gear' icon on the bottom left of the window, will bring up DHS's preferences. These check boxes can be selected to control the execution of DHS. For example, selecting 'full scan' will cause DHS to perform a scan of the entire file-system. Selecting 'weak hijacker detction' will cause DHS to look for hijackers that abuse weak imports. Finally, selecting 'save results' will cause DHS to log all findings (as JSON) to a file in the application's directory named 'dhsFindings.txt'.



DHS is designed to favor reporting false positives over supressing false negatives. While this will uncover a wider range of malicious hijackers, it may also result in legitimate dylibs being flagged. If something is flagged on your computer, is recommended you first consult the **list** of known false positives.

FAQs

Q: DHS found some vulnerable applications, should I be worried?

automatically started by the OS, to gain persistence (by simply planting a malicious dynamic library). It is important to understand that in order to abuse a vulnerable application, an attacker would have to already have compromised your computer. At this point, all bets are off anyways.

Q: Are there patches available for the vulnerable applications?
A: Due to the fact dylib hijacks abuse legitimate functionality of the core OS, there are not any per-application patches available. In the future, Apple may introduce OS-level security features, such as requiring all libraries to be signed, which may mitigate this attack.

Q: DHS found an hijacked application, now what?
A: First off, don't freak out - especially if the type of hijack is weak. Without getting into the (boring) technical details, there may be legitimate scenarios that cannot be differentiated from a malicious hijack. To err on the side of caution, DHS is tuned to report false positives instead of false negatives. If a potential hijack is detected, there are several options that may determine if the hijacker dlyib is malicious. First, check if the flagged dynamic library (whose path is reported in the light gray sub-text of the row) is on the **list** of known false positives. If not, perhaps submit the dylib to **VirusTotal**, which will scan the file with a myriad of anti-virus engines. If you are still concerned, perhaps google the hash of the file, run strings on it, or **email** me and attach the flagged file :)