Jekyll on iOS: When Benign Apps Become Evil

Apple adopts the mandatory app review and code signing mechanisms to ensure that only approved apps can run on iOS devices. In this paper, we present a novel attack method that fundamentally defeats both mechanisms. Our method allows attackers to reliably hide malicious behavior that would otherwise get their app rejected by the Apple review process. Once the app passes the review and is installed on an end user's device, it can be instructed to carry out the intended attacks.

The key idea is to make the apps remotely exploitable and subsequently introduce malicious control flows by rearranging signed code. Since the new control flows do not exist during the app review process, such apps, namely Jekyll apps, can stay undetected when reviewed and easily obtain Apple's approval.

We implemented a proof-of-concept Jekyll app and successfully published it in App Store. We remotely launched the attacks on a controlled group of devices that installed the app. The result shows that, despite running inside the iOS sandbox, Jekyll app can successfully perform many malicious tasks, such as stealthily posting tweets, taking photos, stealing device identity information, sending email and SMS, attacking other apps, and even exploiting kernel vulnerabilities.

Note: Updated version contains the corrected acknowledgements

Open Access Media

BibTeX

@inproceedings {180384,
author = {Tielei Wang and Kangjie Lu and Long Lu and Simon Chung and Wenke Lee},
title = {Jekyll on {iOS}: When Benign Apps Become Evil},
booktitle = {22nd USENIX Security Symposium (USENIX Security 13)},
year = {2013},
isbn = {978-1-931971-03-4},
address = {Washington, D.C.},
pages = {559--572},
url = {https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang_tielei},
publisher = {USENIX Association},
month = aug
}

Presentation Video

Presentation Audio
