How to Bypass Root & Jailbreak Detection

HASRAN ADDAHRONI

Why We want to Root and JailBreak the devices?

- Freedom of your own devices

Rooting in Androids

- Super SU

Rooting in Androids

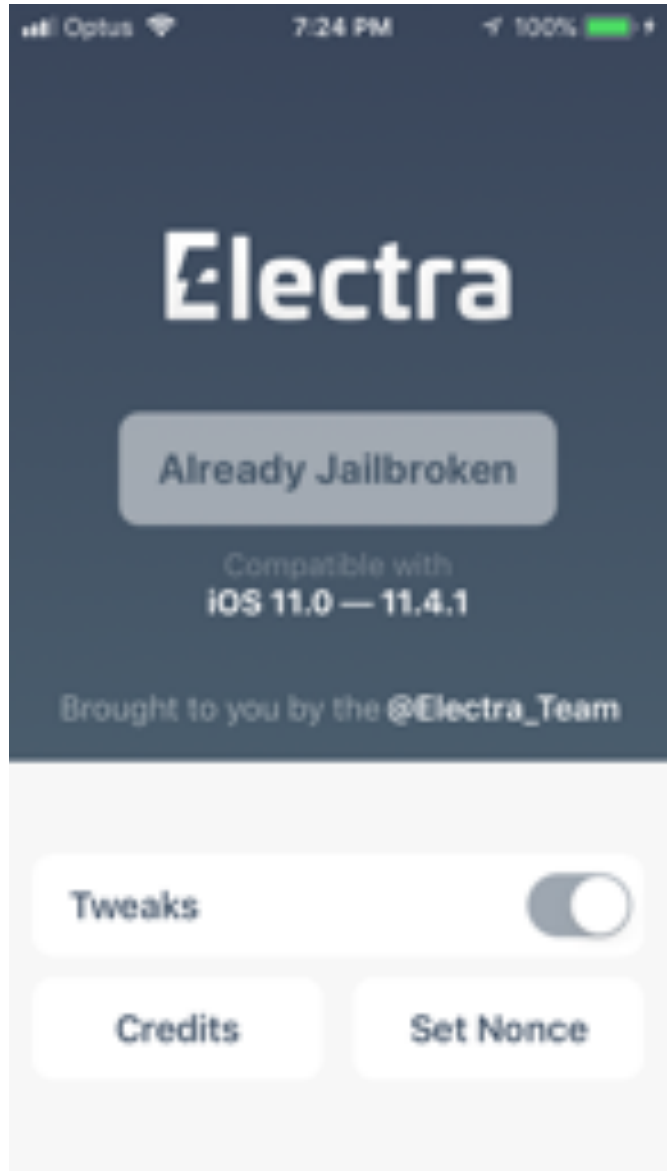
- Magisk

JailBreaking the iOS

- Yalu
  - Supports: iOS 10.x
  - https://yalu.qwertyoruiop.com

JailBreaking the iOS

- Electra
  - Supports: iOS 11.0 – 11.4.1
  - https://coolstar.org/electra/


Optus
7:24 PM
100%
Electra
Already Jailbroken
Compatible with
iOS 11.0 — 11.4.1
Brought to you by the @Electra_Team
Tweaks
Credits
Set Nonce

JailBreaking the iOS

- Uncover
  - Support: iOS 11.x – 12.2
  - https://github.com/pwn20wndstuff/Undecimus


9:41
unc0ver jailbreak for iOS 11.0-11.4b3
by @pwn20wnd & @sbingner
UI by @Dennisbednarz & Samg_is_a_Ninja
Jailbreak
Jailbreak
Settings

Rooted Detection Mechanism

- File system-based detection
  - Searching for apps: SuperSU, rootcloak, sslunpining.
- Directory Permissions
  - Checking for /data, /system, /proc writeability.
- Commands checking
  - Checking for su and busybox.

JailBroke Detection Mechanism

- Filesystem-based Detection
  - New Files Created, Directory permissions, Size of /etc/fstab file, Existence of symbolic links, Writing files
- OpenSSH Service Detection
- Cydia Scheme Detection
- Reference: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/jailbreak-detection-methods/

Bypass Rooted Detection Mechanism

- Patched the smali & rooted detection algorithm

Bypass Rooted Detection Mechanism

- RootCloak
  - Xposed Modules

Bypass Rooted Detection Mechanism

- Magisk hide

Bypass JailBroke Detection

- tsprotector

Bypass JailBroke Detection

- Liberty Lite

Demo

Q&A