iOS Hacking

Aprendendo a Explorar Maçãs

Rodrigo Laneth

Maio de 2020

Visão Geral

- checkm8
- JTAG/SWD
- DCSD
- CPFM
- Corellium
- Brasil

Como debugar o iOS?

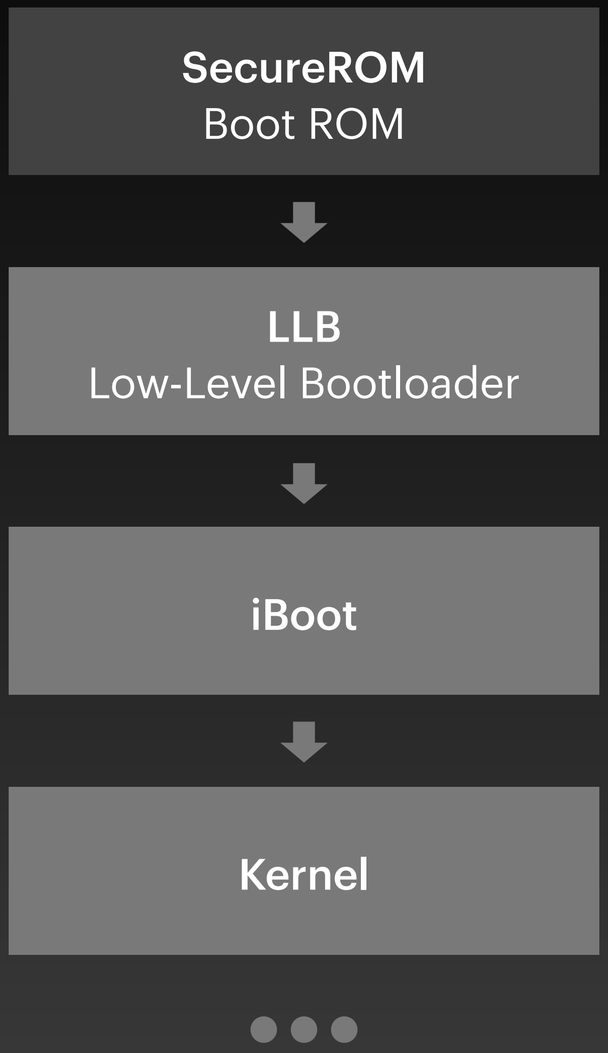
Photo by Youssef Sarhan on Unsplash

Kaguya-sama: Love is War (Season 1, Episode 11)

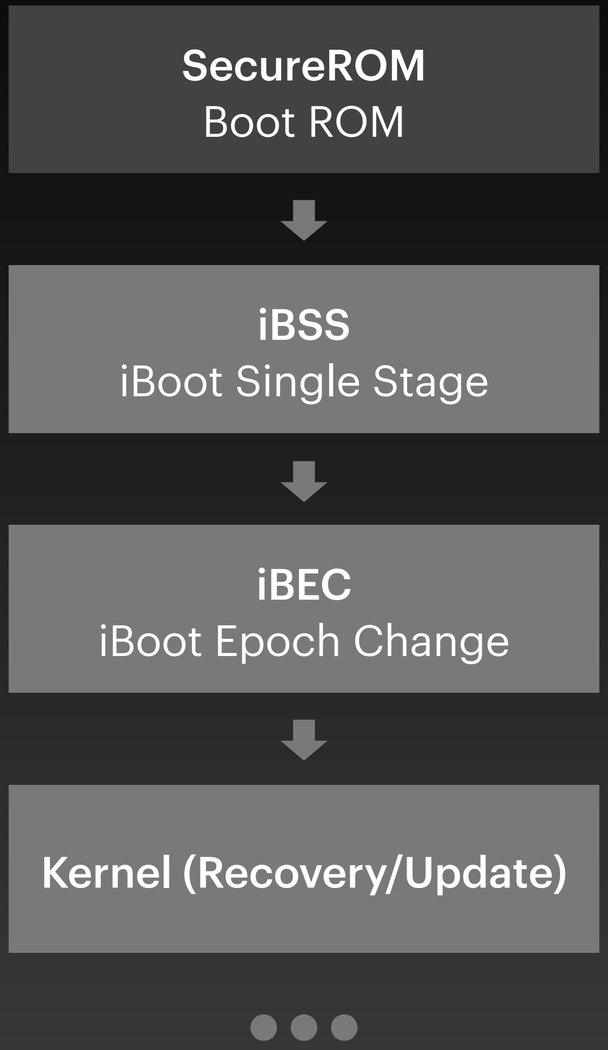
checkm8

https://twitter.com/axi0mX/status/1175422016701685 76

Boot do iOS



DFU


SecureROM
Boot ROM
iBSS
iBoot Single Stage
iBEC
iBoot Epoch Change
Kernel (Recovery/Update)

“Newer devices (and thus, SecureROM versions) still have four separate images, but inspecting them (past decryption) reveal they are all identical. In other words, one single iBoot image now handles all phases.”

*OS Internals Volume II, by Jonathan Levin

http://newosxbook.com/bonus/iBoot.pdf

checkm8

- permanent unpatchable bootrom exploit for hundreds of millions of iOS devices
- meant for researchers, this is not a jailbreak with Cydia yet
- allows dumping SecureROM, decrypting keybags for iOS firmware, and demoting device for JTAG
- current SoC support: s5l8947x, s5l8950x, s5l8955x, s5l8960x, t8002, t8004, t8010, t8011, t8015
- future SoC support: s5l8940x, s5l8942x, s5l8945x, s5l8747x, t7000, t7001, s7002, s8000, s8001, s8003, t8012
- full jailbreak with Cydia on latest iOS version is possible, but requires additional work

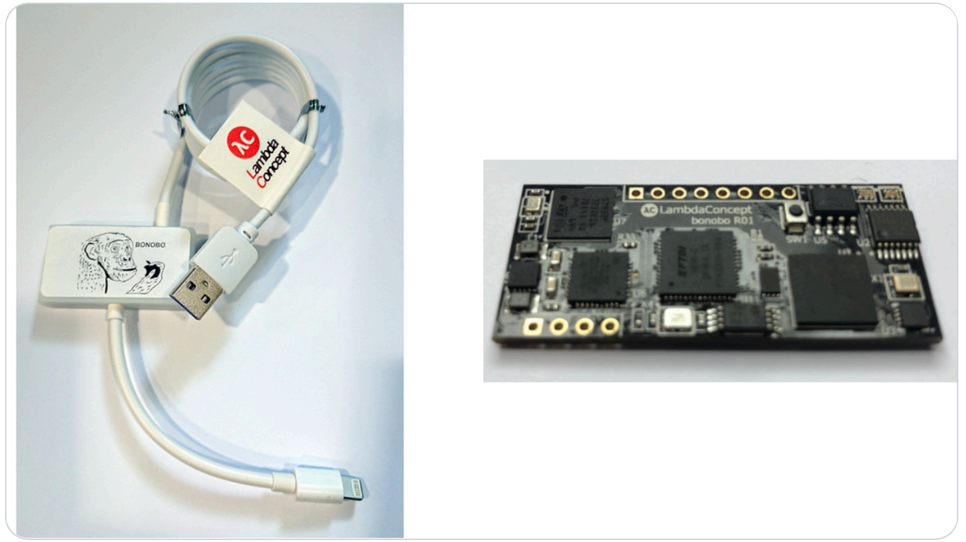
https://github.com/axi0mX/ipwndfu

JTAG/SWD

LambdaConcept
@LambdaConcept

And now you can debug your demoted iPhone over JTAG/SWD with the Bonobo Cable and OpenOCD ! !
shop.lambdaconcept.com/home/37-bonobo...

Traduzir Tweet



12:46 PM · 27 de set de 2019 · Twitter Web App

https://twitter.com/LambdaConcept/status/1177610444804153344

BONOBO JTAG/SWD DEBUG CABLE

Back in stock ! 🙂

IPHONE DEBUGGING REQUIRES PROPER TOOLS.

The Bonobo cable connects to your target through Lightning and allows CPU debugging through JTAG/SWD using OpenOCD + AArch64 GDB. Among others, you can: access all CPUs and registers, single step, put hardware breakpoints, dump memory, etc... Perfect for security research.

The target serial console can be accessed on the control PC through Minicom (iBoot prompt), as well as Lightning USB (For DFU, USB exploitation, demote, etc.)

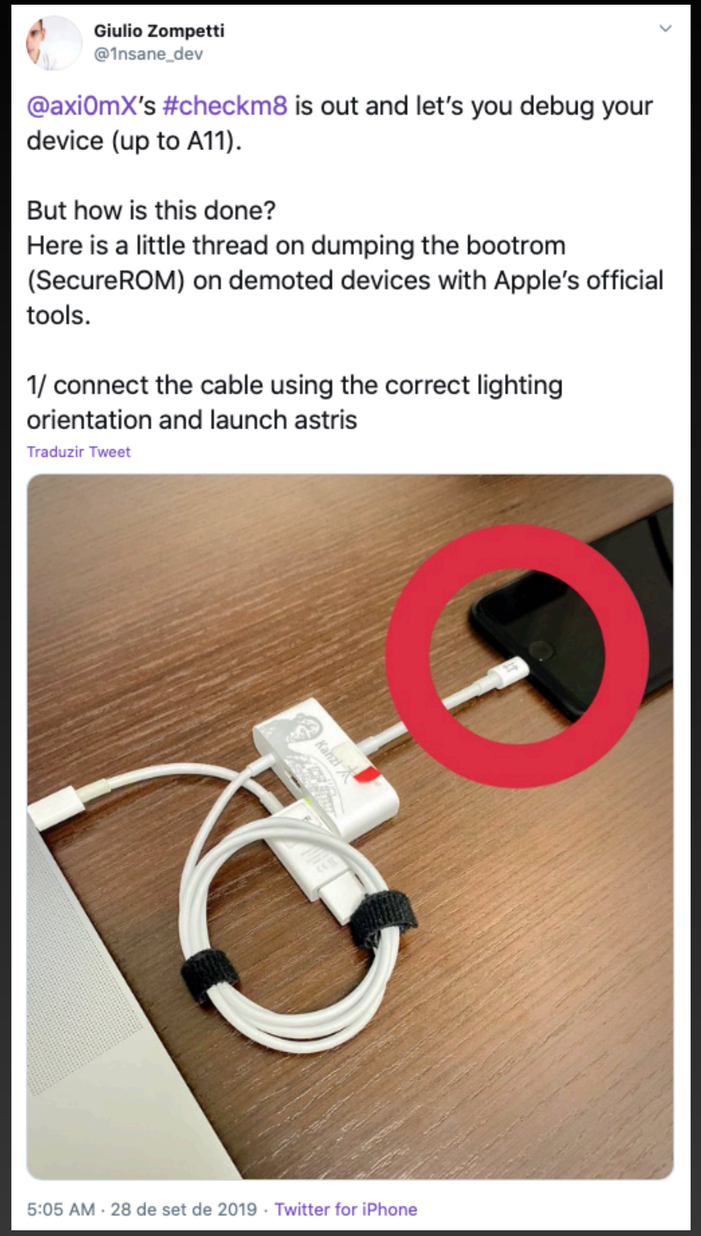
Need **more informations**.

Purchase now ›

http://bonoboswd.com

https://twitter.com/nyan_satan/status/1090989650280398849

GorillaSWD (via @laobaiTD)
https://twitter.com/laobaiTD/status/1026546353319493632



https://twitter.com/1nsane_dev/status/1177856941139337216

Kanzi Cable

The **Kanzi Cable** is a JTAG/SWD Cable capable of debugging CPFM 00 or 01 devices (EVT and DVT devices) which have the Lighting port, using software called Astris. It can be connected to another SWD debugger, using the SWD port, and it can also do UART/Serial. They can be purchased from obscure markets. There are two known types of the Kanzi cable. The normal version and a prototype version with PROTO etched to it.

A Normal Kanzi Cable

Uses

Dumping the SecureROM

One use of the cable is dumping the SecureROM from devices. This can be done using commands such as this one.

This hardware article is a "stub", an incomplete page. Please add more content to this article and remove this tag.

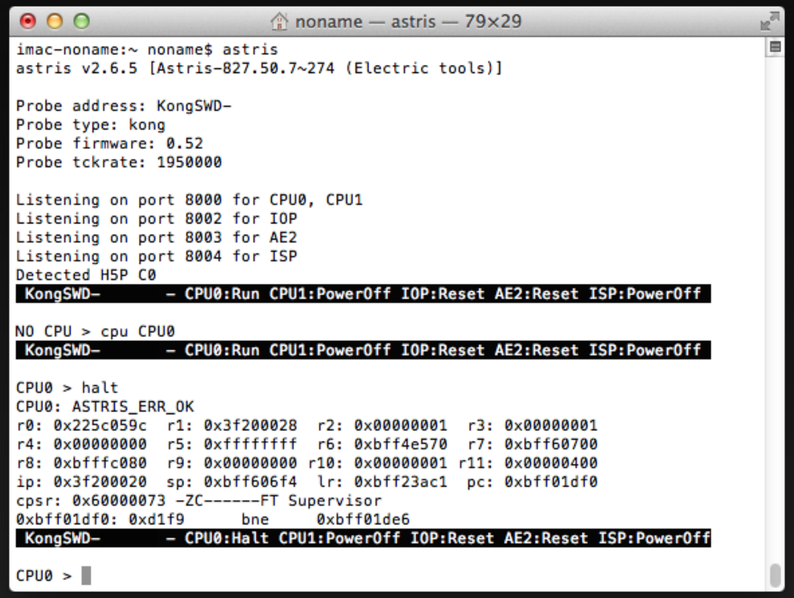
Categories: Article stubs | Cables

Main page
Community portal
Current events
Recent changes
Random page
Help

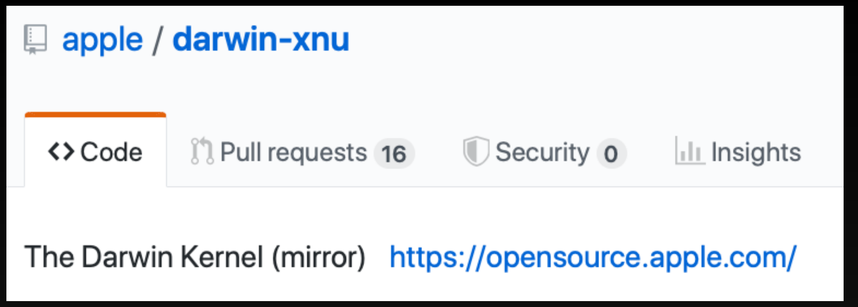
Miscellaneous
Ground rules
Timeline

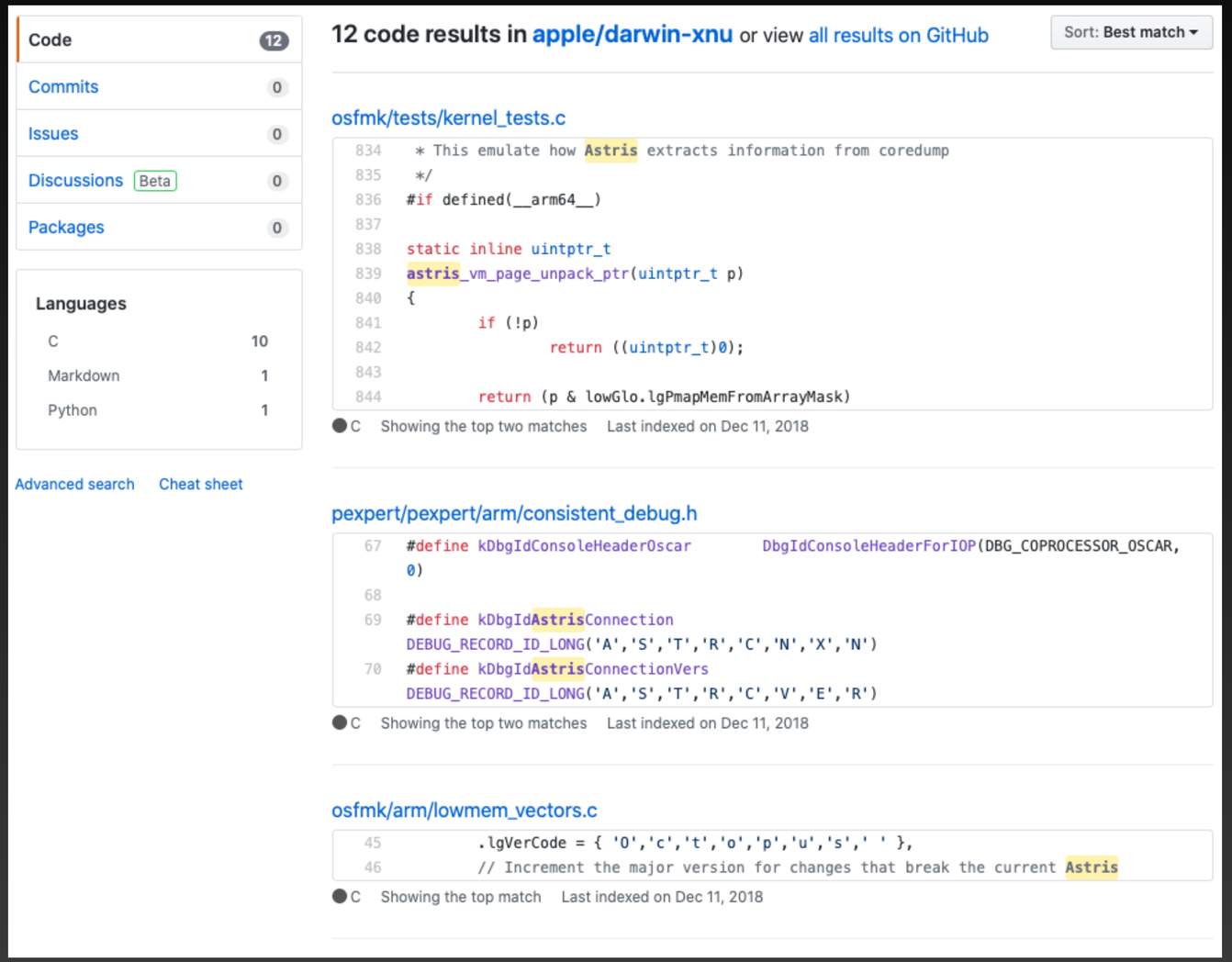
Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

https://www.theiphonewiki.com/wiki/Kanzi_Cable



https://twitter.com/nyan_satan/status/1090989661768613889

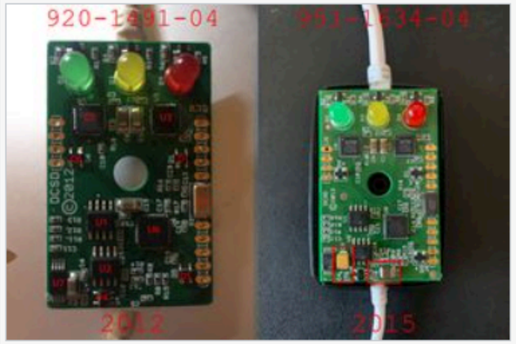

apple / darwin-xnu
Code
Pull requests 16
Security 0
Insights
The Darwin Kernel (mirror) https://opensource.apple.com/


Code 12
Commits 0
Issues 0
Discussions Beta 0
Packages 0
Languages
C 10
Markdown 1
Python 1
Advanced search
Cheat sheet
12 code results in apple/darwin-xnu or view all results on GitHub
Sort: Best match
osfmk/tests/kernel_tests.c
834 * This emulate how Astris extracts information from coredump
835 */
836 #if defined(__arm64__)
837
838 static inline uintptr_t
839 astris_vm_page_unpack_ptr(uintptr_t p)
840 {
841 if (!p)
842 return ((uintptr_t)0);
843
844 return (p & lowGlo.lgPmapMemFromArrayMask)
C Showing the top two matches Last indexed on Dec 11, 2018
pexpert/pexpert/arm/consistent_debug.h
67 #define kDbgIdConsoleHeaderOscar DbgIdConsoleHeaderForIOP(DBG_COPROCESSOR_OSCAR, 0)
68
69 #define kDbgIdAstrisConnection DEBUG_RECORD_ID_LONG('A','S','T','R','C','N','X','N')
70 #define kDbgIdAstrisConnectionVers DEBUG_RECORD_ID_LONG('A','S','T','R','C','V','E','R')
C Showing the top two matches Last indexed on Dec 11, 2018
osfmk/arm/lowmem_vectors.c
45 .lgVerCode = { 'O','c','t','o','p','u','s',' ' },
46 // Increment the major version for changes that break the current Astris
C Showing the top match Last indexed on Dec 11, 2018

DCSD

DCSD Cable

The **DCSD Alex cable** is used in factories to communicate over serial to run tests and write to the SysCfg (for serial definitions, etc) during production. These cables are produced by ShenZhen Alex Connector Co., Ltd. in China. They can be purchased from obscure markets. There are two known types of DCSD cable. An older one, with lights and only one USB female USB connector, and a newer model, which lacks lights, and has two female USB connectors.



Annotated photo of the original Alex DCSD PCB

Contents [hide]

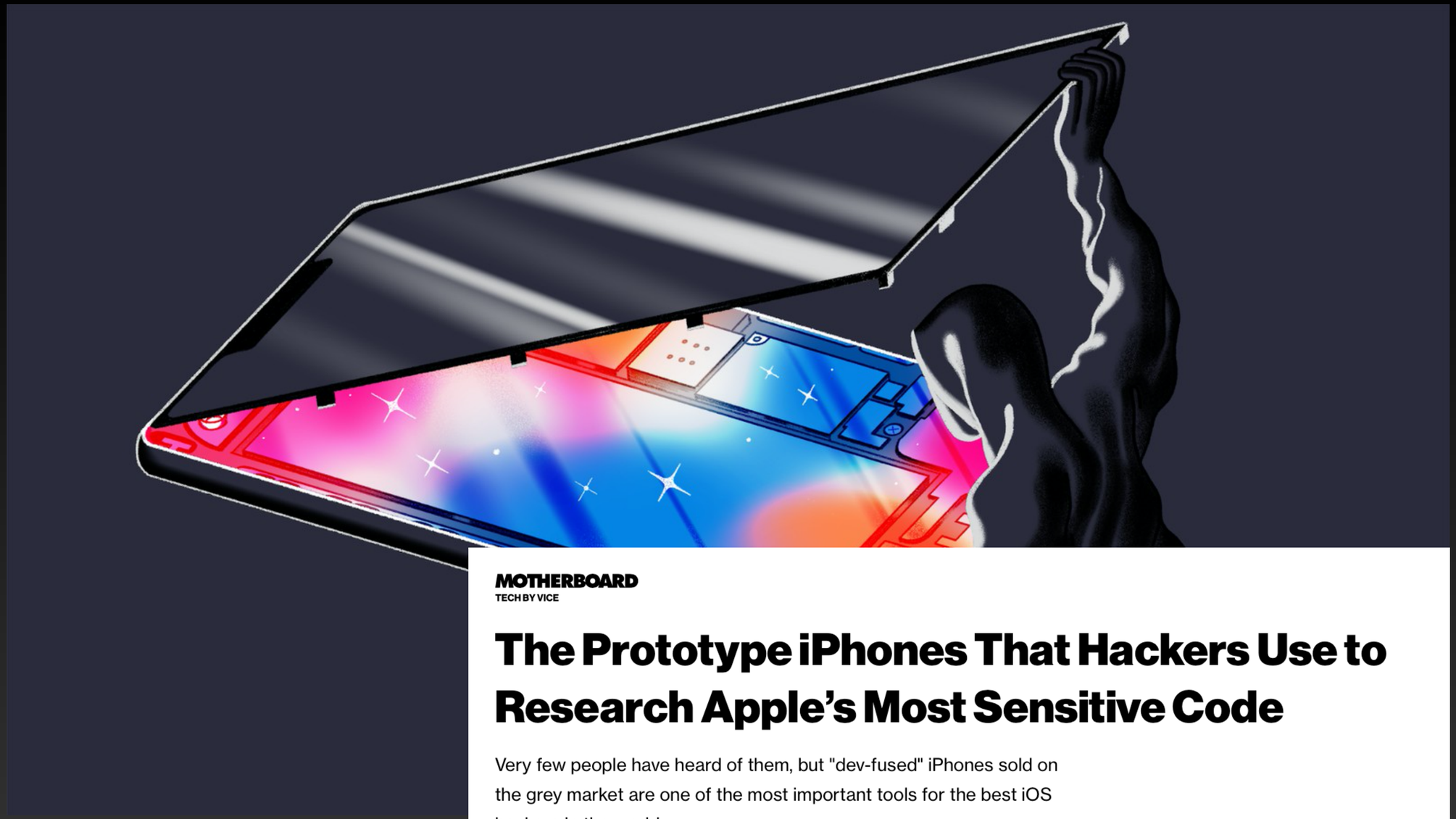
https://www.theiphonewiki.com/wiki/DCSD_Cable

https://twitter.com/j4nf4b3l/status/1263784178799259648

CPFM

Chip Fuse Mode

Insecure/Secure	Development/ Production	CPFM
0	0	0
1	0	1
1	1	3



MOTHERBOARD
TECH BY VICE

The Prototype iPhones That Hackers Use to Research Apple's Most Sensitive Code

Very few people have heard of them, but "dev-fused" iPhones sold on the grey market are one of the most important tools for the best iOS hackers in the world.

By Lorenzo Franceschi-Bicchierai

Mar 6 2019, 3:23pm Share Tweet Snap

https://www.vice.com/en_us/article/gyakgw/the-prototype-dev-fused-iphones-that-hackers-use-to-research-apple-zero-days

Behind the Scenes with iOS Security

Black Hat 2016

Ivan Krstić
Head of Security Engineering and Architecture, Apple

SoC Security Mode

Demotion

Production devices can be "demoted" to enable some debugging features like JTAG and loading development software on the AP (but not the SEP)

Requires full OS erase and device explicitly authorized by the personalization server

Forces a different UID on the SEP, no access to existing user data after demotion

SoC mode	AP status	SEP status	SEP UID
Development fused	Development	Development	Development
Production fused	Production	Production	Production
AP demoted	Development	Production	Development

https://www.blackhat.com/docs/us-16/materials/us-16-Krstic.pdf

https://twitter.com/hackerfantastic

“Most of the time, to hack targets using apple it's a simple case of how much money do you have. It can run into $100k for a good vuln dev environment. People have gone broke just trying (hi). Community collaboration kept jailbreaking alive as a hobbyist community open since IOS11”

Hacker Fantastic, 18 de agosto de 2019

https://twitter.com/hackerfantastic/status/1163197724050821120

Apple Developer Program US$ 99/ano

Hardware Apple entre US$ 2.000 e US$ 10.000

Equipamentos eletrônicos US$ 10.000

Cabos e material para cabos US$ 5.000

iPhone de desenvolvimento/protótipo US$??

https://twitter.com/hackerfantastic/status/1163657799793987584

Corellium

POR LUIZ GUSTAVO RIBEIRO

Apple processa empresa por replicar ilegalmente o iOS

Plataforma oferece suporte ao iOS, mas sem os devidos direitos autorais

16/08/2019 • 12:27 18

No processo, aberto ontem (15/8) no Tribunal do Sul da Flórida, a Apple acusa a Corellium de violar seus direitos autorais por ter replicado ilegalmente o seu sistema operacional móveis e alguns apps da Maçã que rodam no iPhone e no iPad.

Vale notar que "copiar" o sistema móvel da Maçã é justamente o objetivo da Corellium, uma vez que tais plataformas de virtualização pretendem oferecer o visual e os recursos de determinado sistema, em outro. No entanto, o problema aqui é que a desenvolvedora fez isso sem a devida autorização da Apple.

> A Corellium simplesmente copiou tudo: o código, a interface gráfica do usuário, os ícones — tudo isso, com detalhes precisos.

Durante a conferência de segurança Black Hat, que aconteceu em Las Vegas na última semana, a Corellium enfatizou que o seu "produto Apple" é uma cópia exata do iOS, capaz até mesmo de contribuir para que pesquisadores e hackers encontram e testes vulnerabilidades como se fosse o sistema original da Maçã.

https://macmagazine.uol.com.br/post/2019/08/16/apple-processa-empresa-por-replicar-ilegalmente-o-ios/

Apple and DOJ fight over photos that have ‘national security concerns’

Ben Lovejoy - May. 5th 2020 5:03 am PT @benlovejoy

Apple’s lawsuit against virtualization company Corellium has taken a surprising turn, as the Department of Justice claims that photos Apple wants to introduce into evidence may have ‘national security concerns.’

The DOJ wants Apple to hand over the photos before introducing them into evidence so that it can examine them before deciding whether the government has an interest in the case …

https://9to5mac.com/2020/05/05/national-security-concerns/

Corellium

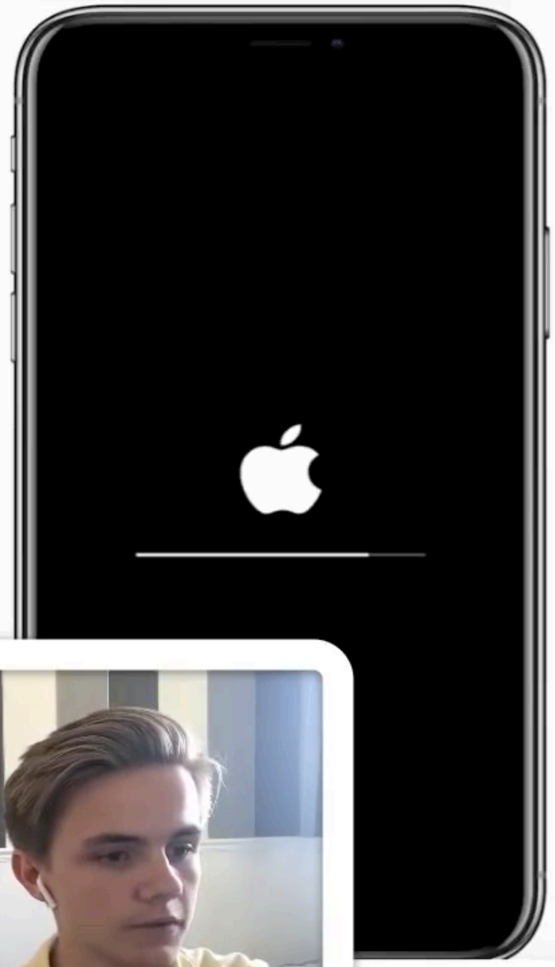
CORELLIUM

Find Device

DEVICES HELP Billy Ellis

B iPhone X (iPhone X | 12.0)

Snapshot Pause Restart



CONSOLE CYCRIPT

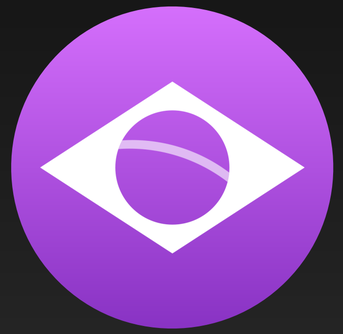
```
remove_purgatory_entry:6105: error 2 removing purgatory entry 3/0x11df1-dead for ino 73201
cleanup_purgatory_dir:15498: *** Cleaning purgatory removed 1 entries but found 1 BAD entries
ERROR: sendCommandToSEP: AssertMacros: err == 0  (value = 0x8),  file: /BuildRoot/Library/Caches/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDriver/ApplePearlSEPDriver.cpp, line: 10026

ERROR: sepTransactWorker: AssertMacros: err == 0  (value = 0x8),  file: /BuildRoot/Library/Caches/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDriver/ApplePearlSEPDriver.cpp, line: 10211

ERROR: sepTransact: AssertMacros: err == 0  (value = 0x8),  file: /BuildRoot/Library/Caches/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDriver/ApplePearlSEPDriver.cpp, line: 10315

ERROR: sepTransactToIOMD: AssertMacros: err == 0  (value = 0x8),  file: /BuildRoot/Library/Caches/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDriver/ApplePearlSEPDriver.cpp, line: 10356

ERROR: performCommandGated: AssertMacros: err == 0  (value = 0x8),  file: /BuildRoot/Library/Caches/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDriver/ApplePearlSEPDriver.cpp, line: 971

ERROR: ApplePearlUserClient::extPerform: AssertMacros: err == 0  (value = 0x8),  file: /BuildRoot/Library/Caches/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDriver/ApplePearlUserClient.cpp, line: 219
```


SSH ssh -p22 root@10.11.1.1

iPhone Virtualisation Demo/Preview Using Corellium | Platform Demo from Chris Wade
by Billy Ellis https://www.youtube.com/watch?v=6rmTfmdUIVY

Há espaço para pesquisa em Apple no Brasil?

Photo by sergio souza on Unsplash



Apple Hacking 🇧🇷

https://t.me/applehackingbr

Agradecimentos

- **Davidson Francis (@Theldus)**
  https://github.com/theldus
- **Gustavo Oliveira (@Highustavo)**
  https://twitter.com/Highustavo
- **@Lilith**
  https://t.me/Srt_Lilith
- **Renato Hormazabal (@hex0x42424242)**
  https://twitter.com/hex0x42424242

Obrigado!

Site rlaneth.com
Telegram @rlaneth