
State of iOS Hacking in 2024: An Overview
Lars Fröder
Cellebrite Labs

About Me

- Security Researcher from Germany, Earth
- Started iOS development journey in 2017, research in 2022
- Employed at Cellebrite Labs

- Developed various iOS jailbreak system extensions (“tweaks”)
- Developer of TrollStore and Dopamine Jailbreak


opa334dev

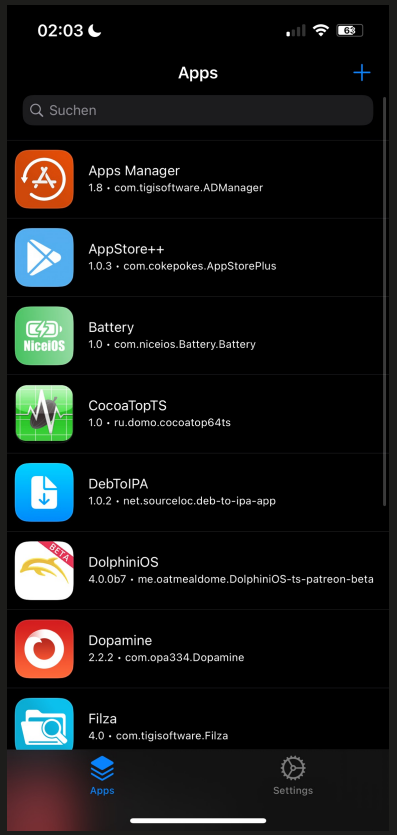

opa334@infosec.exchange

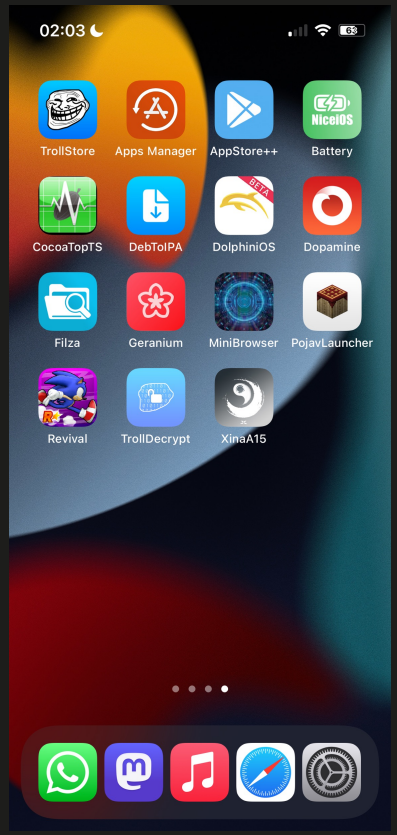
Agenda

TrollStore

Dopamine

TrollStore

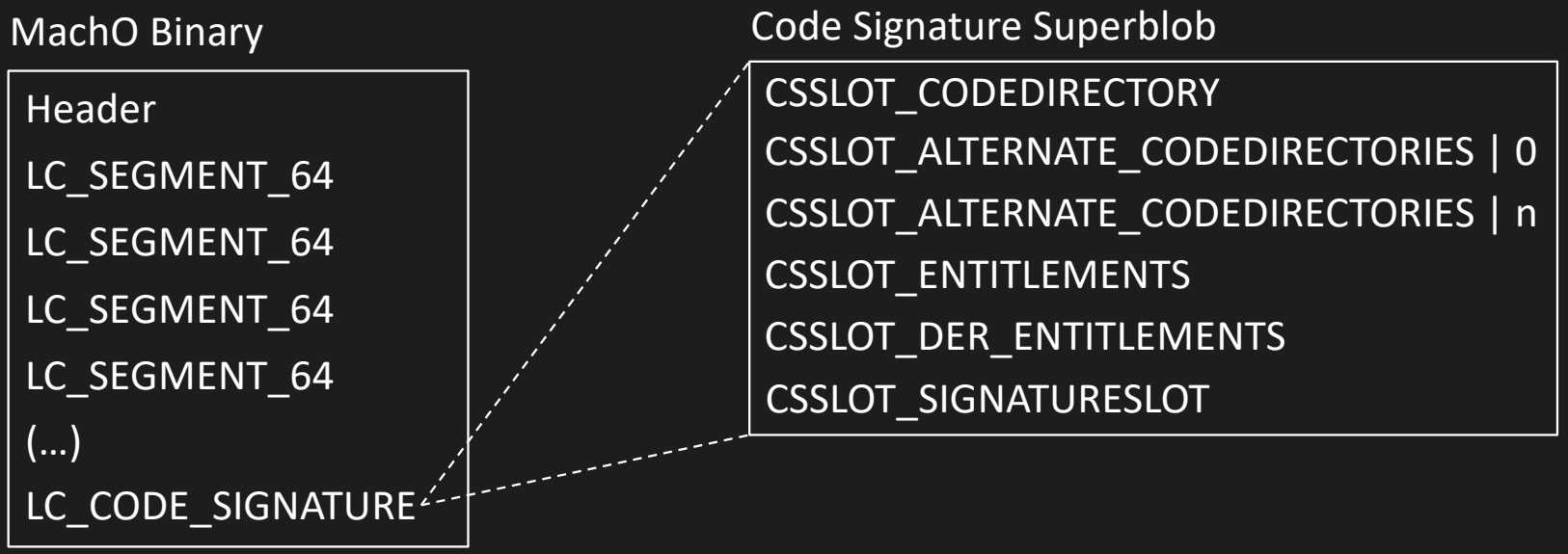

02:03
Apps
Suchen
Apps Manager
1.8 • com.tigisoftware.ADManager
AppStore++
1.0.3 • com.cokepokes.AppStorePlus
Battery
1.0 • com.niceios.Battery.Battery
CocoaTopTS
1.0 • ru.domo.cocoatop64ts
DebToIPA
1.0.2 • net.sourceloc.deb-to-ipa-app
DolphiniOS
4.0.0b7 • me.oatmealdome.DolphiniOS-ts-patreon-beta
Dopamine
2.2.2 • com.opa334.Dopamine
Filza
4.0 • com.tigisoftware.Filza
Apps
Settings


02:03
TrollStore
Apps Manager
AppStore++
Battery
CocoaTopTS
DebToIPA
DolphiniOS
Dopamine
Filza
Geranium
MiniBrowser
PojavLauncher
Revival
TrollDecrypt
XinaA15

Code Signature Enforcement

- Every executables requires a valid code signature to run
  - System executables: “Ad hoc” signed, “code directory hash” in trust cache
  - AppStore executables: Signed by Apple on submission using “Apple iPhone OS Application Signing” certificate
  - Xcode App executables: Signed by Developer certificate issued by Apple, extremely limited
- Checked by the Kernel on execution
  - During posix_spawn or execve syscall

Code Signatures



Code Directories

Code Signature Superblob

CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ALTERNATE_CODEDIRECTORIES | n
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT

- Contain hashes of all executable pages within the binary
- Additionally contain hashes of other relevant data (e.g. CSSLOT_ENTITLEMENTS)
- One Code Directory has one hash type, (e.g. SHA1, SHA256, …)
- One binary can have multiple code directories with different hash types

Entitlements

Code Signature Superblob

CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ALTERNATE_CODEDIRECTORIES | n
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT

- Describe the permissions of the binary
- Kernel drivers it can access
- File paths it can read/write to/from
- Whether it the binary is sandboxed
- Whether the binary may be debugged by other processes
- Etc…

Signature Slot

Code Signature Superblob

CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ALTERNATE_CODEDIRECTORIES | n
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT

- Contains cryptographically signed hash of code directories
- Signed with Apple or Developer cert
- Adhoc signed binaries do not have a signature, those are verified via the trust cache
- Can have multiple signers

CVE-2023-41991

- Part of Intellexa “Predator” Spyware
- LPE in exploit chain
- Used against oppositional politician in Egypt
- Discovered in the wild by Google TAG
- Reconstructed via patchdiffing by @alfiecg_dev
- Fixed in iOS 16.7, 17.0.1 and macOS 13.6

CVE-2023-41991

- Within the CoreTrust Kernel Extension, which is responsible for checking the code signature of App Store apps
- Called by AMFI (Apple Mobile File Integrity) Kernel Extension
- One of the most complex bugs I have seen
- Multiple quirks combined allow a fakesigned binary to run
  - CoreTrust only checks whether the last signer of a signature is valid (or rather, uses the same error variable for every signer, meaning it will just be overwritten by the last check)
  - CoreTrust returns the CodeDirectory hash of the first signer back to AMFI
  - CoreTrust only passes the first signer to the function that checks whether the binary is App Store signed

CVE-2023-41991: Code Directory

Code Signature Superblob

CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT

- Code Directory stolen from a validly signed App Store app
- Type: SHA1
- None of contained hashes match our binaries executable pages, nor our entitlements or anything else

CVE-2023-41991: Alternate Code Directory

Code Signature Superblob

```
CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT
```

- Actual code directory that's valid for our binary
- Type: SHA256 (Kernel prefers SHA256 over SHA1)
- Nothing special about it, really

CVE-2023-41991: Signature Slot

Code Signature Superblob

CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT

- Signer 1 (TrollStore certificate)
  - Our certificate, signed data controlled by us
  - Valid hash for main code directory (SHA1)
  - Valid hash for alternate code directory (SHA256)
- Signer 2 (Apple certificate)
  - Stolen from the same App Store app binary as the main code directory
  - Valid hash for main code directory (SHA1)
  - Invalid hash for alternate code directory (SHA256)

CVE-2023-41991: Entitlements

Code Signature Superblob

CSSLOT_CODEDIRECTORY
CSSLOT_ALTERNATE_CODEDIRECTORIES | 0
CSSLOT_ENTITLEMENTS
CSSLOT_DER_ENTITLEMENTS
CSSLOT_SIGNATURESLOT

- Fully attacker controlled since their hashes are in the alternate code directory (SHA256) that we also fully control
- Gives you arbitrary permissions to do anything you want*
- *Except anything involving overtaking system processes, since these are isolated from the rest of the system and the system thinks we are an App Store app

Intellexa Office when they found this bug (probably)

Us flexing the POC on Twitter (what's X???)

opa334
@opa334dev

Quick! I want to run a binary on my device to print some nice artwork but I just get "zsh: killed" 😕

Anyone knows how to fix this???

Post übersetzen

12:00 vorm. · 26. Nov. 2023 · **62.725** Mal angezeigt

10 8 164 7

Us flexing the POC on Twitter (what's X???)

Us flexing the POC on Twitter (what's X???)

Big Shoutout to @alfiecg_dev!!!

(He can’t be here since he’s a minor)

TrollStore

- App-Installer that itself is signed with CoreTrust bug
- Gets root via persona-mgmt entitlement
- Accepts unsigned IPA files (apps) to be opened within it
- Applies CoreTrust bug on all executables in the app bundle
- Places app on the filesystem
- Adds it to the icon cache
- App appears on home screen and is usable like any other app

TrollStore vs. Jailbreak

- Persistent
- Only explicitly signed binaries can execute
- Not able to spawn launch daemons
- No system wide tweak injection

- Non-persistent (unless chained with bug that archives persistence on boot)
- All unsigned binaries can execute
- Able to spawn launch daemons
- System wide tweak injection

Agenda

TrollStore

Dopamine

Dopamine

- Full jailbreak utilizing Kernel exploit and PPL bypass
  - Kernel exploit: kfd landa (CVE-2023-41974)
  - PPL bypass: Operation Triangulation (CVE-2023-38606)
- Modify system in a way that all unsigned binaries can be executed
- Enable system wide tweak injection (system extensions)
- Cannot modify Kernel code / constant data, since it is protected by KTRR
- Can modify all mutable data

Dopamine: Codesign Bypass

- Instead of hooking Kernel code, hook Userspace code
- Userspace code is only PPL protected (wx_allowed bit in process structure)
- Dynamically loaded trust caches (Xcode functionality) are only PPL protected

- Idea: Hook “posix_spawn” system wide to automatically add a binaries code directory hash to trust cache before the system tries to execute it

Dopamine: Launchd Exploit Server

- launchd: Pid 1, the systemd of Apple operating systems
- From jailbreak app, get a task port to launchd and use it to create a new thread that calls dlopen on our (trust cached) library
- Library retrieves primitives from exploit app, then exposes jailbreak API to the rest of the system
  - IPC call to add a binaries code directory hash to trust cache
  - IPC call to disable runtime codesigning in a process

posix_spawn hook

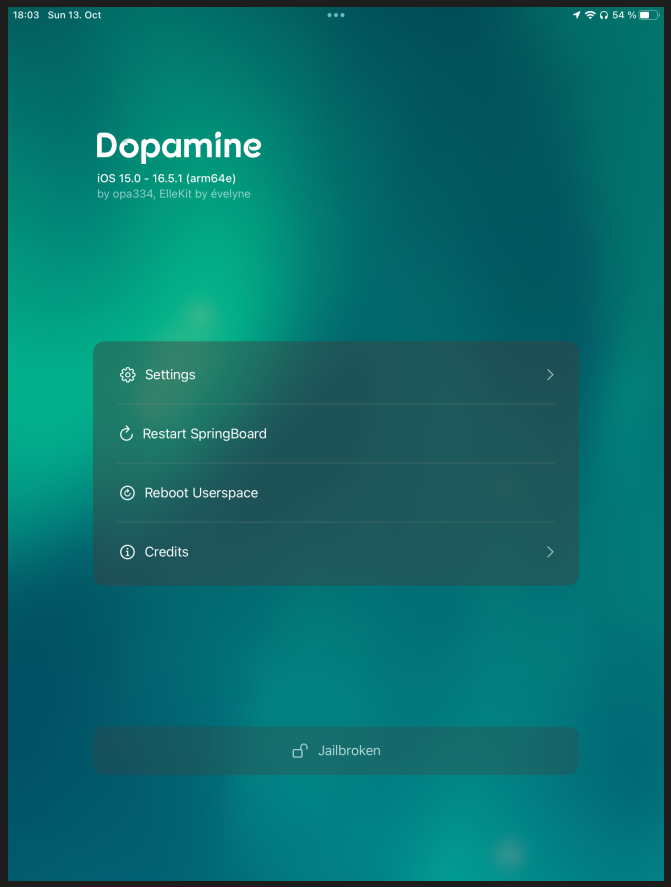
```
int
posix_spawn(pid_t *restrict pid, const char *restrict path,
    const posix_spawn_file_actions_t *file_actions,
    const posix_spawnattr_t *restrict attrp, char *const argv[restrict],
    char *const envp[restrict]);
```

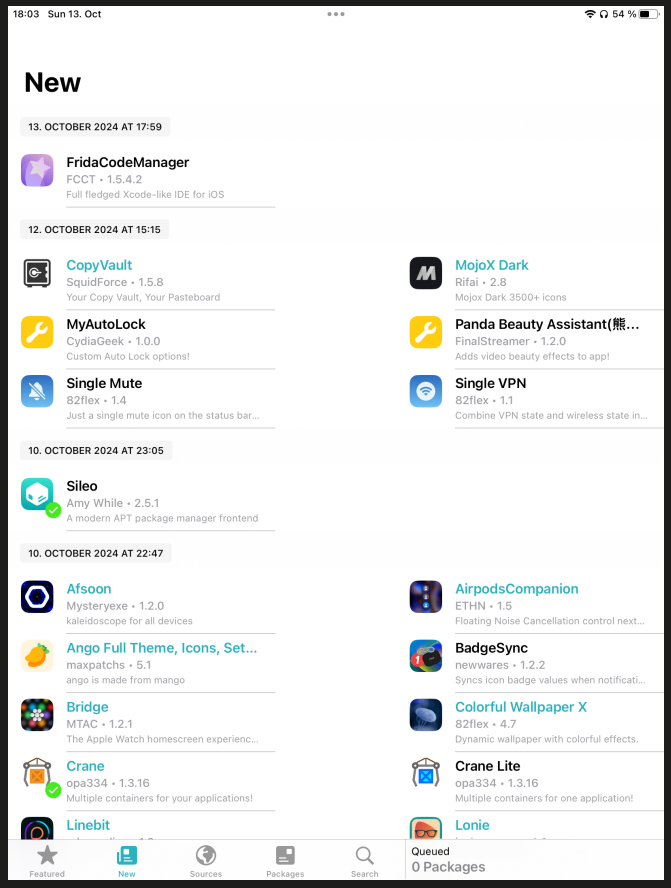
- Use jailbreak server in launchd to add the binary to trust cache
- Add DYLD_INSERT_LIBRARIES to reinject hook dylib into child

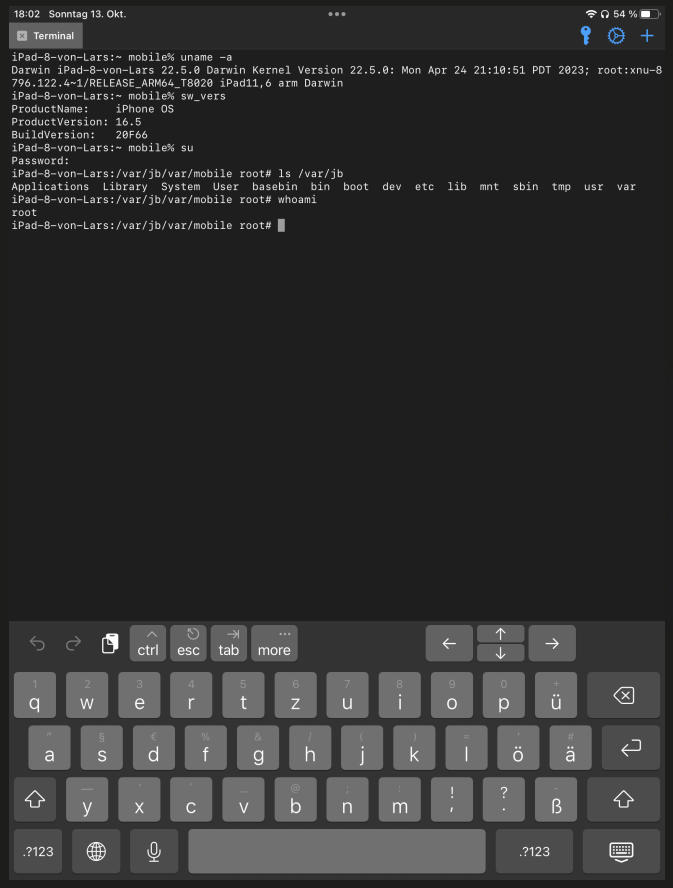
Dopamine: Summary

- launchdhook.dylib
  - Provides exploit/jailbreak server IPC calls
  - Loads third party launch daemons
  - Kickstarts posix_spawn hook to bypass codesigning via adding the binary to trust cache and injects systemhook.dylib into any child process
  - Injected into launchd during jailbreak
- systemhook.dylib
  - On injection, disables runtime codesigning via IPC to launchd / launchdhook
  - Hooks posix_spawn to bypass codesigning by sending binary path to launchd / launchdhook and to reinject systemhook.dylib into any child process
  - Enables tweak injection by additionally dlopen’ing tweak injection framework

Dopamine


18:03 Sun 13. Oct
54 %
Dopamine
iOS 15.0 - 16.5.1 (arm64e)
by opa334, ElleKit by évelyne
Settings
Restart SpringBoard
Reboot Userspace
Credits
Jailbroken


18:03 Sun 13. Oct
54 %
New
13. OCTOBER 2024 AT 17:59
FridaCodeManager
FCCT • 1.5.4.2
Full fledged Xcode-like IDE for iOS
12. OCTOBER 2024 AT 15:15
CopyVault
SquidForce • 1.5.8
Your Copy Vault, Your Pasteboard
MojoX Dark
Rifai • 2.8
Mojox Dark 3500+ icons
MyAutoLock
CydiaGeek • 1.0.0
Custom Auto Lock options!
Panda Beauty Assistant(熊...
FinalStreamer • 1.2.0
Adds video beauty effects to app!
Single Mute
82flex • 1.4
Just a single mute icon on the status bar...
Single VPN
82flex • 1.1
Combine VPN state and wireless state in...
10. OCTOBER 2024 AT 23:05
Sileo
Amy While • 2.5.1
A modern APT package manager frontend
10. OCTOBER 2024 AT 22:47
Afsoon
Mysteryexe • 1.2.0
kaleidoscope for all devices
AirpodsCompanion
ETHN • 1.5
Floating Noise Cancellation control next...
Ango Full Theme, Icons, Set...
maxpatchs • 5.1
ango is made from mango
BadgeSync
newwares • 1.2.2
Syncs icon badge values when notificati...
Bridge
MTAC • 1.2.1
The Apple Watch homescreen experienc...
Colorful Wallpaper X
82flex • 4.7
Dynamic wallpaper with colorful effects.
Crane
opa334 • 1.3.16
Multiple containers for your applications!
Crane Lite
opa334 • 1.3.16
Multiple containers for one application!
Linebit
Lonie
Featured
New
Sources
Packages
Search
Queued
0 Packages


18:02 Sonntag 13. Okt.
54 %
Terminal
iPad-8-von-Lars:~ mobile% uname -a
Darwin iPad-8-von-Lars 22.5.0 Darwin Kernel Version 22.5.0: Mon Apr 24 21:10:51 PDT 2023; root:xnu-8796.122.4~1/RELEASE_ARM64_T8020 iPad11,6 arm Darwin
iPad-8-von-Lars:~ mobile% sw_vers
ProductName: iPhone OS
ProductVersion: 16.5
BuildVersion: 20F66
iPad-8-von-Lars:~ mobile% su
Password:
iPad-8-von-Lars:/var/jb/var/mobile root# ls /var/jb
Applications Library System User basebin bin boot dev etc lib mnt sbin tmp usr var
iPad-8-von-Lars:/var/jb/var/mobile root# whoami
root
iPad-8-von-Lars:/var/jb/var/mobile root#
ctrl
esc
tab
more


Let’s Talk?
Lars Fröder
Cellebrite Labs