A security review of 1,300 AppStore applications

Jan Seredynski
Mobile Security Engineer @ Guardsquare

Prices for hacking an iPhone

$100,000 - local privilege escalation
(e.g. installing a malicious app from AppStore)

$200,000 - Safari sandbox escape and remote code execution
(e.g. opening an infected website)

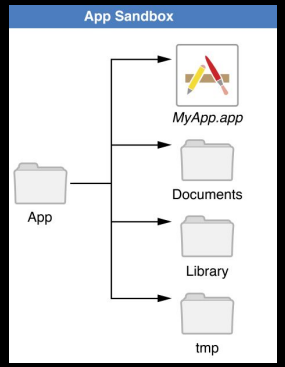
$200,000 - malicious media file
(e.g. opening a file to infect the phone)

$500,000 - via a popular app
(e.g. infecting the device through
Email, Whatsapp, Telegram or Signal)

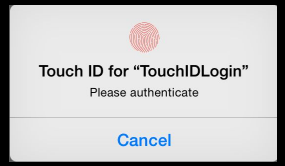
Based on a bounty program of zerodium.com

What happens after the phone gets infected

Malicious code



preferences
databases
media
tmp files
cached cookies
cached responses



keychain

Runtime Application Self Protection

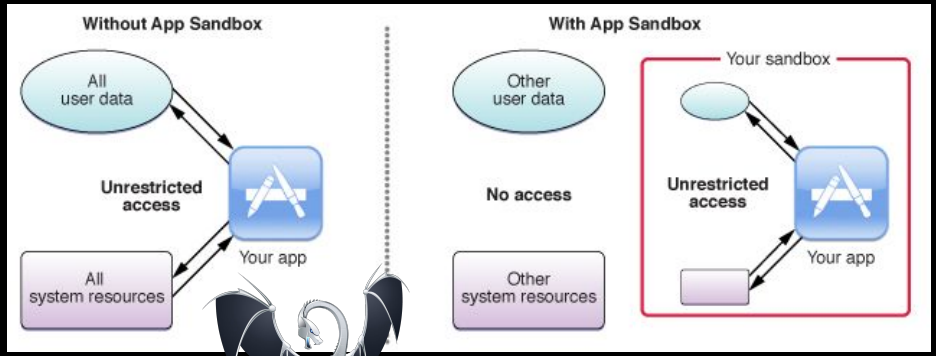
File artifacts

Sandbox

Filesystem permissions

Debug

Instrumentation



/bin/bash
MobileSubstrate.dylib
lldb


```
MNT_RDONLY = 0
MNT_NOSUID = 0
```

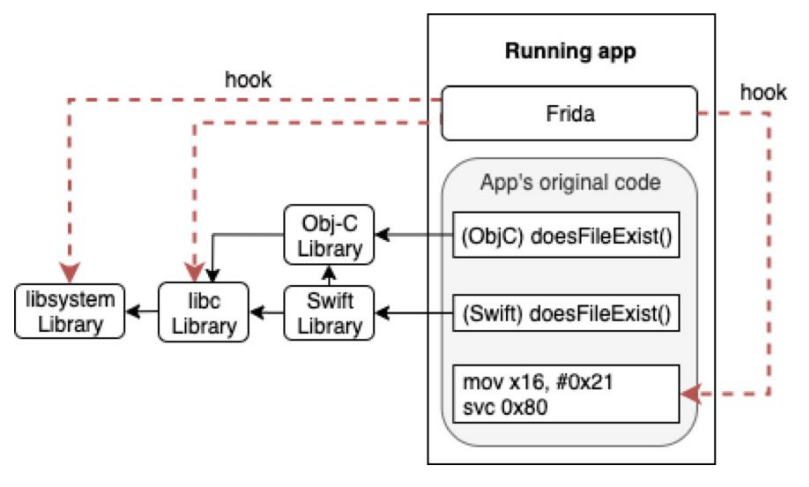
```
_dyld_image_count()
_dyld_get_image_header()
```

Question:

How many apps use Runtime Application Self Protection?

Search for RASP sentinels

Dynamic analysis: FRIDA



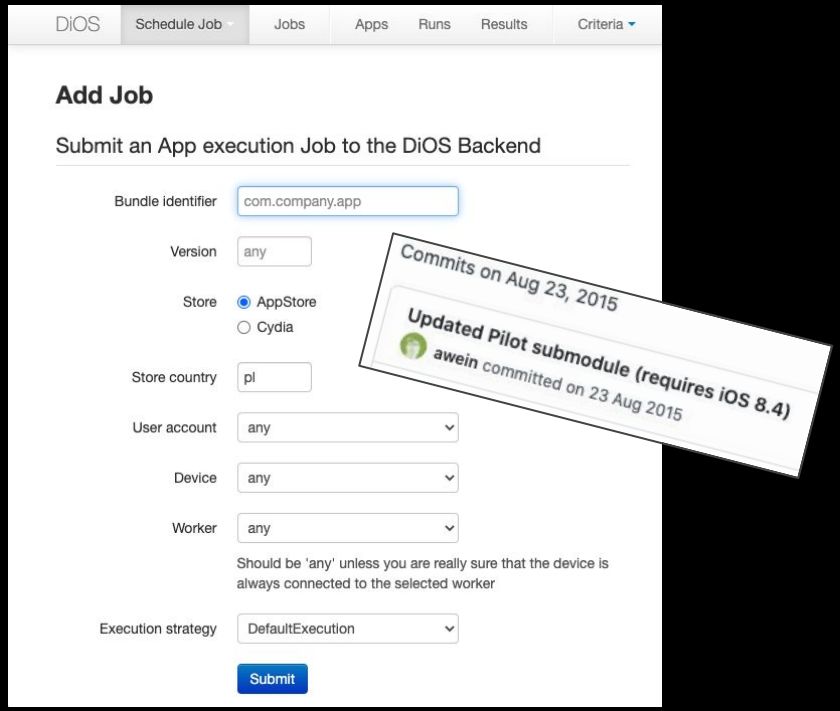
Static analysis:

- strings “/bin/bash”
- imports (fork, ptrace, lstat, …)
- system calls instructions
- known frameworks(e.g. TrustKit)

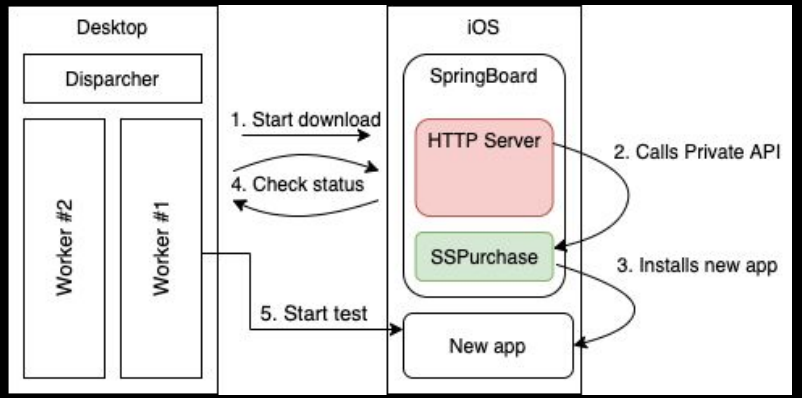
Automate app download and installation from AppStore

Feel free to add your ideas to Q&A section

DiOS = Scheduler + AppStore crawler

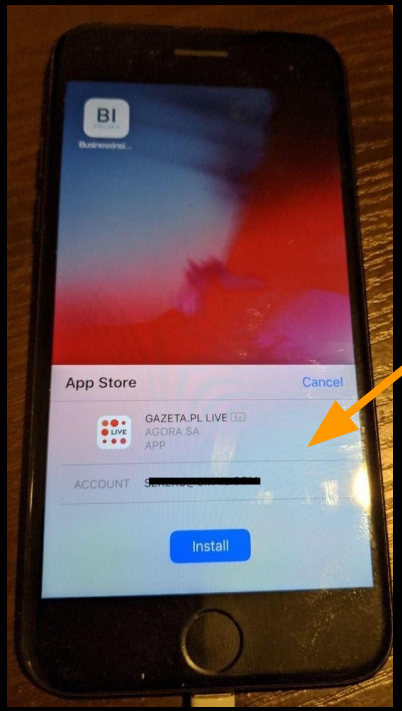


DiOS Dispatcher



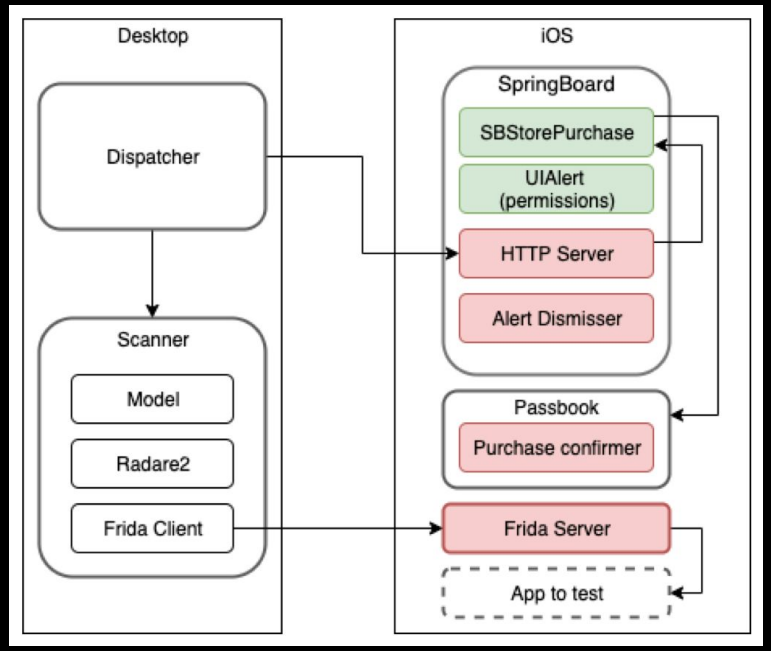
DiOS design

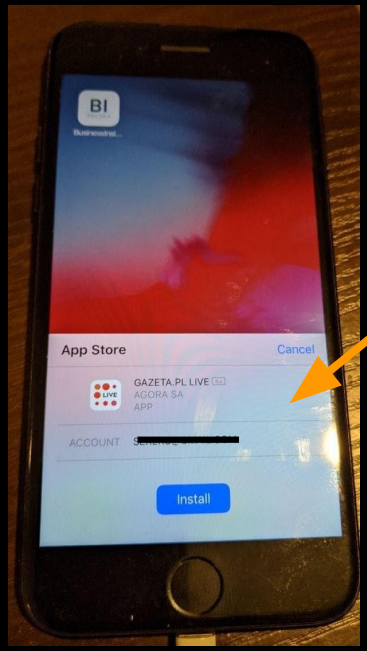
New extra step in iOS 11



What is it screen?

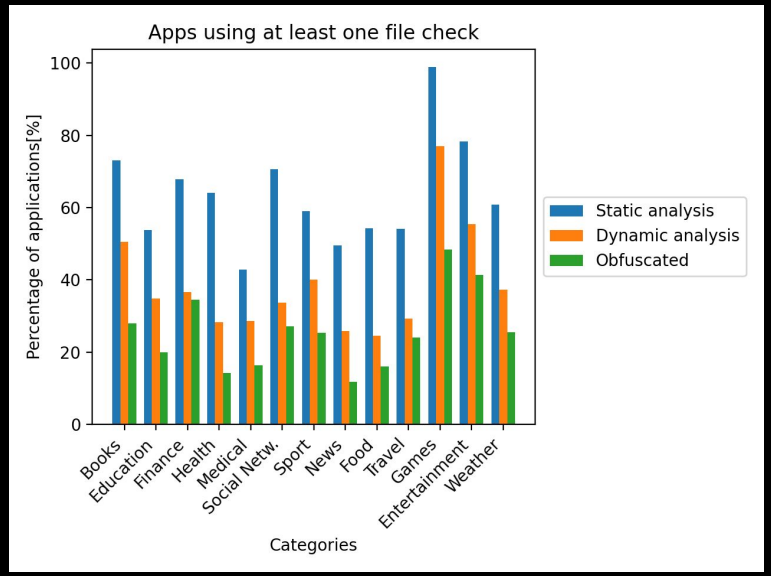
The final design





Passbook app

Results - File artifacts

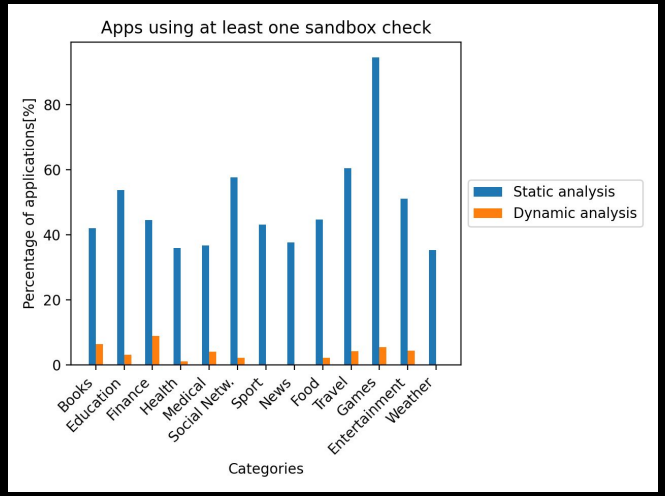


Apps checks for 8 files on average

Mostly checked files (out of first 1000 apps):
/Applications/Cydia.app 499 times
/bin/bash 415
/usr/sbin/sshd 251

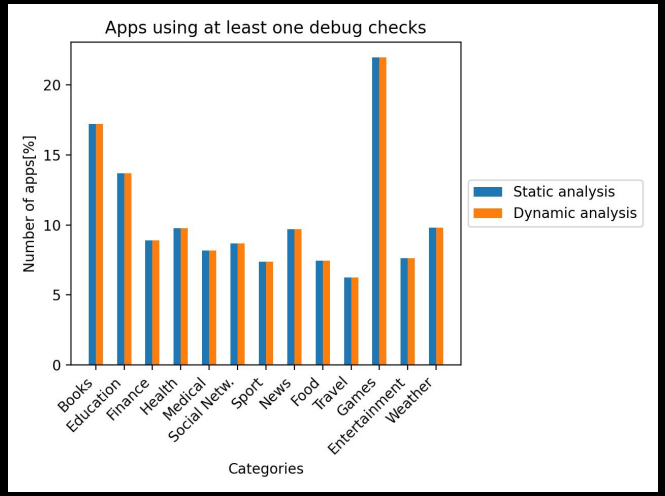
1,300 apps = 2min * 1300 = ~2days

Sandbox



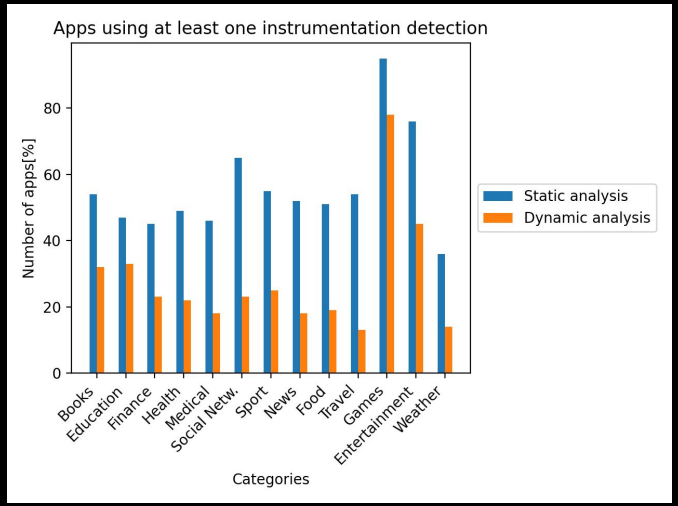
fork, kill, popen

Debug



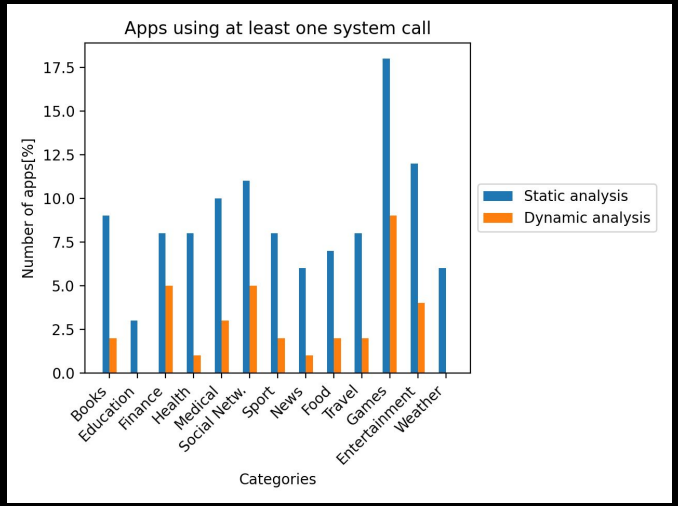
ptrace, sysctl, getppid

Instrumentation



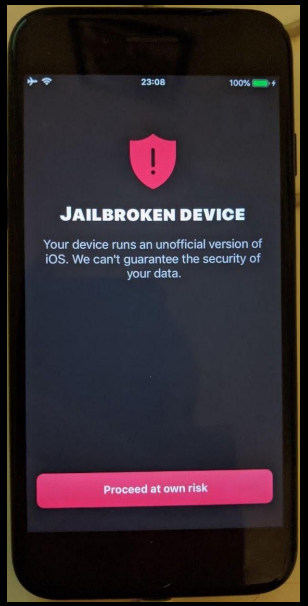
_dyld_get_image_name,
_dyld_get_image_header,
dladdr

System calls



sysctl, ptrace, write, unlink
access, bind, symlink,
socket, setsockopt

Summary



Bunq

- about 60% of apps has at least 1 kind of RASP protection
- don’t expect the whole AppStore to be like that
- do vendors protect us or themselves?
  (finance vs games)

- Many apps run RASP protection after login
  -> Is it really a good idea?

Thank you

Questions?