EntySec

iOS Malware

Overview of Apple iOS malware

Ivan Nikolskiy

Content

■ **What is iOS?**
Basic overview of the Apple iOS

■ **iOS security layers**
Security in iOS

■ **Jailbreak**
What is jailbreak?

■ **Attack chain**
Explain how malware access iOS

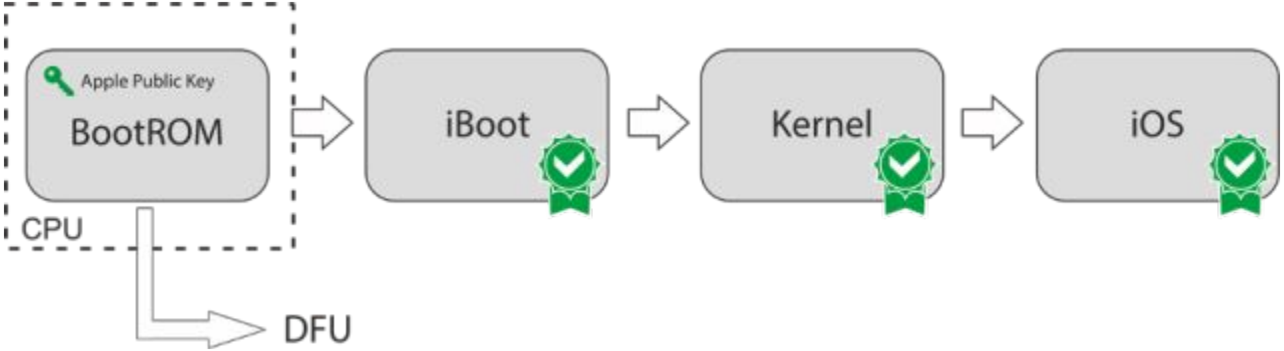
■ **Cydia malicious tweaks**
How malware uses Cydia

What is iOS?

- Security & Reliability
- User-friendly interface
- Closed source code
- Additional security measures in AppStore

What is iOS? (versions)

iOS security layers



Sandbox

Each app is ran inside a sandbox and can’t access system files

Signature check

The iBoot checks signature of a kernel image

AMFI

Checks app signature to prevent execution of unsigned code

Secure Enclave (SEP)

Responsible for data protection, Touch ID and Face ID

LLB

Checks the signature of iBoot before jumping to it

R/O rootfs

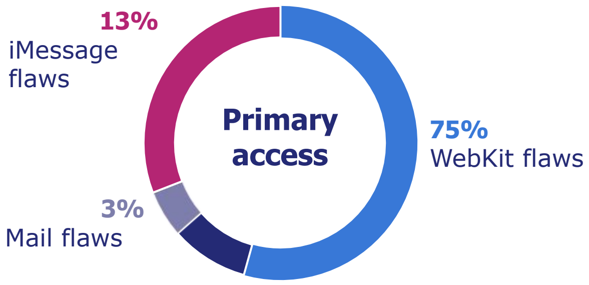
The rootfs (aka /) is mounted as read-only by default

Jailbreak

- Remount file systems as R/W (if /etc/fstab is present)
- Disable sandbox
- Disable code signature checks
- Patch ramdisk (if possible)

< 5.1.1	5.1.1 - 10.3.4	10.3.4 - 15.4.1	>= 17
Redsn0w, Absinthe	H3lix, Pangu, Blizzard, Phoen1x	Electra, Unc0ver, Checkra1n, Dopamine, Palera1n	No jailbreak available

Attack chain



Attack chain

Primary access to the system

Can be achieved via the WebKit flaws or other flaws

Do jailbreak (aka security bypass)

Disable security checks (!)

Execute implant & connect to C2

(i) Migrate it to the process

Cydia malicious tweaks

What is Cydia?

- Package manager for jailbroken iPhones (AppStore)
- All popular jailbreaks install Cydia
- Anybody can upload their tweaks and apps to Cydia

Cydia malicious tweaks (e.g.)

What malicious tweaks can do?

- Track user activity and exfiltrate user data
- Manage phone remotely, deleting files, make calls, etc.
- Wipe all data and make phone completely unusable
- Flood phone browser with ads (AdWare)

EntySec

The End

Thanks for Your Attention

- *EntySec's website*
  entysec.com
- *My website*
  founder.entysec.com
- *This presentation can be found at*
  entysec.com/agenda/ios_malware.pdf