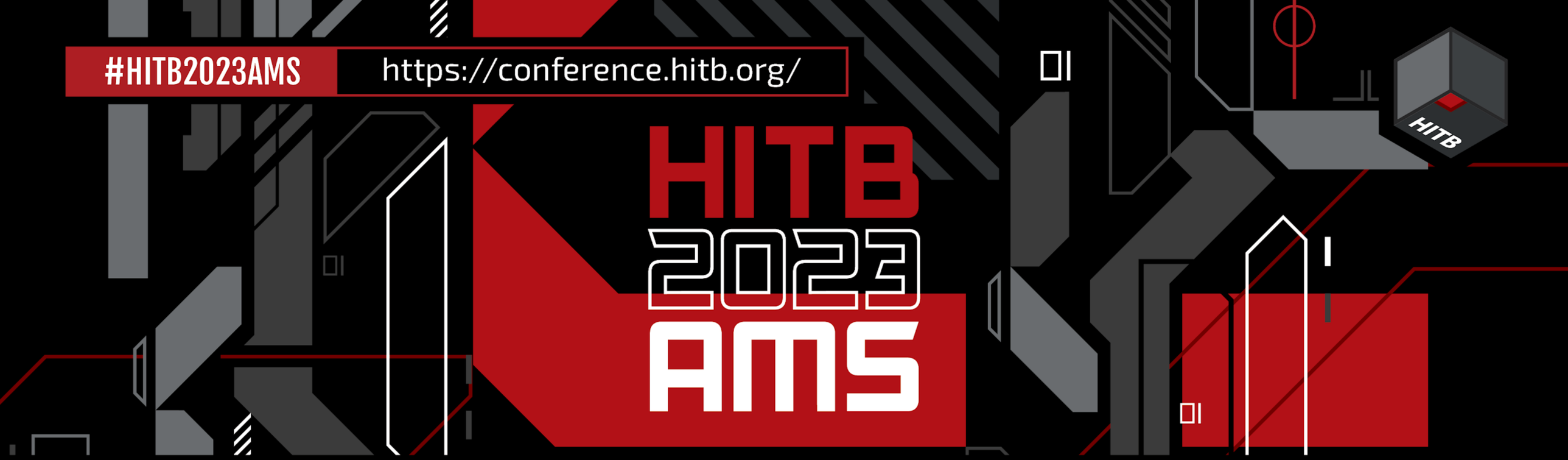


Poisoned Apples: Current State of iOS Malware detection

Matthias Frielingsdorf | Trail of Bits (iVerify)

Who am I

Matthias Frielingsdorf

Former: Mobile Security Team @ Deutsche Bahn

Now: iOS Security Researcher at Trail of Bits (iVerify)

Twitter: @helthydriver

iOS Exploits?

Started with iOS 14.4

Older versions often patched

More Information is not available

3rd party reports are sometimes available

iOS 16.4.1 and iPadOS 16.4.1

Released April 7, 2023

IOSurfaceAccelerator

Available for: iPhone 8 and later, iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.

Description: An out-of-bounds write issue was addressed with improved input validation.

CVE-2023-28206: Clément Lecigne of Google's Threat Analysis Group and Donncha Ó Cearbhaill of Amnesty International's Security Lab

WebKit

Available for: iPhone 8 and later, iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: A use after free issue was addressed with improved memory management.

WebKit Bugzilla: 254797
CVE-2023-28205: Clément Lecigne of Google's Threat Analysis Group and Donncha Ó Cearbhaill of Amnesty International's Security Lab

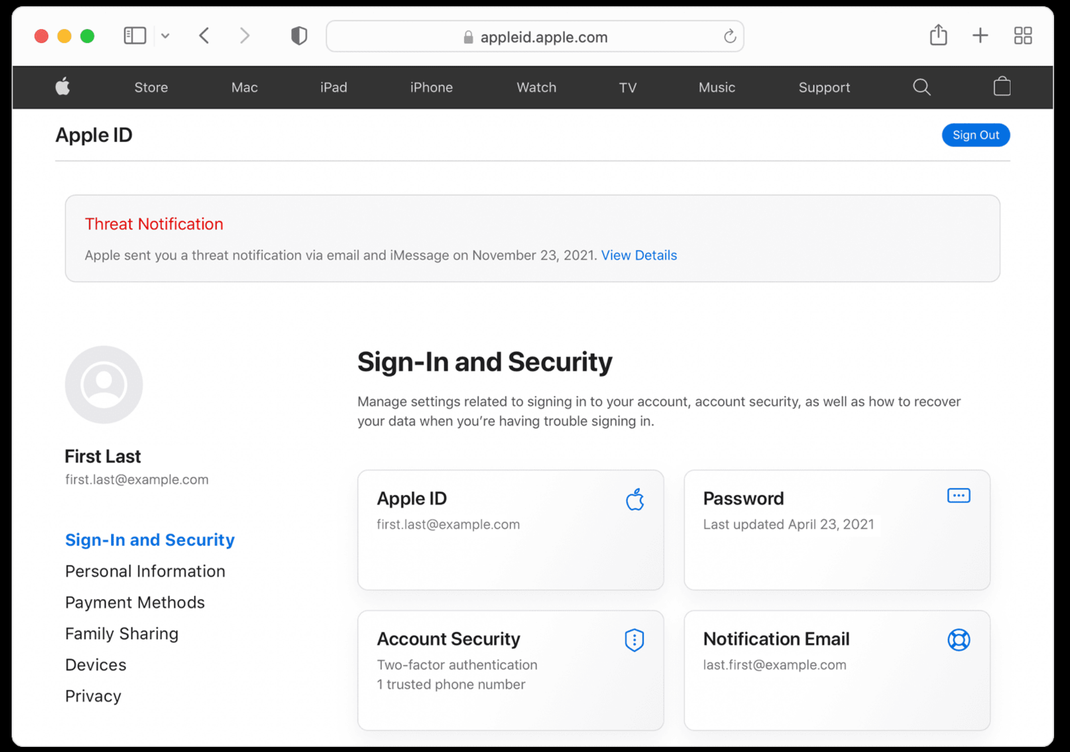
https://support.apple.com/en-us/HT213720

iOS Threat Notifications 2021

iMessage + Email to associated AppleID

Visible on https://appleid.apple.com

Help available at: https://securityplanner.consumerreports.org/tool/emergency-resources



https://support.apple.com/en-us/HT212960

iOS CVEs - „actively exploited“

CVE-2016-4657	CVE-2016-4655	CVE-2016-4656	CVE-2018-4442	
CVE-2017-13861	CVE-2017-2505	CVE-2018-4438	CVE-2017-7064	
CVE-2019-6217	CVE-2018-4122	CVE-2019-7287	CVE-2019-7286	
CVE-2020-27932	CVE-2019-6225	CVE-2020-27930	CVE-2020-27950	
CVE-2021-31010	CVE-2021-30983	CVE-2021-30663	CVE-2021-30883	
CVE-2021-30858	CVE-2021-30860	CVE-2021-30661	CVE-2021-1870	CVE-2022-42827
CVE-2021-30807	CVE-2021-30665	CVE-2021-1879	CVE-2021-1782	CVE-2022-42856
CVE-2021-30666	CVE-2021-1871	CVE-2021-30761	CVE-2021-30762	CVE-2023-23529
CVE-2022-22674	CVE-2021-30869	CVE-2022-32917	CVE-2022-32893	CVE-2023-28205
CVE-2022-22675	CVE-2022-22587	CVE-2022-32894	CVE-2022-22620	CVE-2023-28206

Today

1. Study of Recent Examples of 0/1 - Click Malware
2. Detection Capabilities - App
3. Detection Capabilities - Companion / MDM
4. Detection Capabilities - Forensic
5. Synthesis
6. Improving & Further Research

1. Study of recent examples of Malware

2016 Pegasus v1

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 iOS 14 iOS 15 iOS 16

Infection Vector

WebKit

Targets

Humans Rights Activists
Journalists

Detection & Technical Analysis

CitizenLab and Lookout

CVEs

CVE - 2016 - 4657 WebKit
CVE - 2016 - 4655 Infoleak
CVE - 2016 - 4656 Kernel

Detection

Access to one Infection URL

IOCs

URLs
Files
Processes

Attribution

NSO

https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

2019 - A campaign against Uygures

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 iOS 14 iOS 15 iOS 16

Infection Vector

WebKit

Targets

Uygures in Nepal

Detection & Technical Analysis

Google TAG & Google Project 0

CVEs

CVE - 2017 - 2505	WebKit
CVE - 2017 - 7064	WebKit
CVE - 2018 - 4122	WebKit
CVE - 2018 - Unk.	WebKit
CVE - 2018 - 4438	WebKit
CVE - 2018 - 4442	WebKit
CVE - 2019 - 6217	WebKit
CVE - 2019 - 7287	Kernel
CVE - 2019 - 7286	Sand. Esc.
CVE - 2017 - 13861	Kernel
CVE - 2019 - 6225	Kernel

Detection

Detection of Infiltration Network
Implant + Exploit Download

IOCs

File
URLs
Process

Attribution

Unknown
(Maybe China)

https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html
https://googleprojectzero.blogspot.com/2019/08/jsc-exploits.html
https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

2021 Pegasus v2

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 iOS 14 iOS 15 iOS 16

Infection Vector

iMessage

Targets

Humans Rights Activists
Journalists,Politicians

Detection & Technical Analysis

CitizenLab, Amnesty International & Google Project 0

CVEs

CVE - 2021 - 30860	iMessage
iOS 10	iMessage
iOS 11	VoWiFi
iOS 12	iMessage
iOS 13	PhotoStream
iOS 13	IMTransco.

Detection

Forensic Analysis of infected iPhones
Infiltration / CnC Infrastructure

IOCs

Files
URLs
Processes
Email Adresses
iCloud Adresses

Attribution

NSO

https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/
https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

2021 - Predator

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 iOS 14 iOS 15 iOS 16

Infection Vector

WebKit

Targets

Meta Manager, Politician, Journalist

Detection & Technical Analysis

CitizenLab

CVEs

iOS 13	Unknown
iOS 14	Unknown

Detection

Forensic Analysis

IOCs

Files
Processes
URLs
Shortcut

Attribution

Cytrox

https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html

2022 - Hermit

iOS 9 — iOS 10 — iOS 11 — iOS 12 — iOS 13 — iOS 14 — iOS 15 — iOS 16

Infection Vector

Sideloaded App

Targets

Kazakhstan, Italy

Detection & Technical Analysis

Google Project 0, Google Tag, Lookout (Android)

CVEs

CVE - 2018 - 4344	Lightspeed
CVE - 2019 - 8605	SockPort2
CVE - 2020 - 3837	TimeWaste
CVE - 2020 - 9907	AveCesare
CVE - 2021 - 30883	Clicked2
CVE - 2021 - 30983	Clicked3

Detection

Access to the App and infection URL

IOCs

App
URLs
Provisioning Profile

Attribution

RCS Labs

https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/
https://googleprojectzero.blogspot.com/2022/06/curious-case-carrier-app.html
https://www.sans.org/webcasts/a-hermit-out-of-its-shell-the-surveillanceware-industry-current-threats/
https://www.lookout.com/blog/hermit-spyware-discovery

12

2023 - Reign

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 **iOS 14** iOS 15 iOS 16

Infection Vector

Calendar Events

Targets

Civil Society

Detection & Technical Analysis

CitizenLab & Microsoft Threat Intelligence

CVEs

iOS 14

ENDOFDAYS

Detection

Access to Loader & Forensic

IOCs

Files
Processes
URLs

Attribution

QuaDream

https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/
https://security-blog-prod-wp01.azurewebsites.net/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/

13

2023 - Jamf Threat Labs Report

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 iOS 14 iOS 15 iOS 16

Infection Vector

Unknown

Targets

Journalists

Detection & Technical Analysis

Jamf Threat Labs

CVEs

iOS 14 Unknown
iOS 15 Unknown

Detection

Forensic Analysis

IOCs

Files
Processes

Attribution

NSO, Unknown

https://www.jamf.com/blog/threat-advisory-mobile-spyware-continues-to-evolve/

14

2023 - Pegasus v3

iOS 9 iOS 10 iOS 11 iOS 12 iOS 13 iOS 14 iOS 15 iOS 16

Infection Vector

Homekit, iMessage, FindMy

Targets

Mexico Civil Society

Detection & Technical Analysis

CitizenLab

CVEs

iOS 15	FINDMYPWN
iOS 15	LATENTIMAGE
iOS 16	PWNYOURHOME

Detection

Forensic Analysis

IOCs

Files
Processes
Crashlog

Attribution

NSO

https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

iOS CVEs - map „exploited“ to reports

CVE-2016-4657	CVE-2016-4655	CVE-2016-4656	CVE-2018-4442	
CVE-2017-13861	CVE-2017-2505	CVE-2018-4438	CVE-2017-7064	
CVE-2019-6217	CVE-2018-4122	CVE-2019-7287	CVE-2019-7286	
CVE-2020-27932	CVE-2019-6225	CVE-2020-27930	CVE-2020-27950	
CVE-2021-31010	CVE-2021-30983	CVE-2021-30663	CVE-2021-30883	
CVE-2021-30858	CVE-2021-30860	CVE-2021-30661	CVE-2021-1870	CVE-2022-42827
CVE-2021-30807	CVE-2021-30665	CVE-2021-1879	CVE-2021-1782	CVE-2022-42856
CVE-2021-30666	CVE-2021-1871	CVE-2021-30761	CVE-2021-30762	CVE-2023-23529
CVE-2022-22674	CVE-2021-30869	CVE-2022-32917	CVE-2022-32893	CVE-2023-28205
CVE-2022-22675	CVE-2022-22587	CVE-2022-32894	CVE-2022-22620	CVE-2023-28206

Report available

CVE in Report unknown

Target Data

Sample	App List	Crash Logs	Files	Network	Processes
2019		✓	✓	✓	✓
Hermit	✓	✓	✓	✓	✓
Jamf Report			✓		✓
Reign		✓	✓	✓	✓
Pegasus		✓	✓	✓	✓
Predator		✓	✓	✓	✓

Target Malware Categories

Malicious

App*

MDM

Companion

Forensic

Apps

Profiles

Known Implants

Unknown Implants

* Under the assumption of a sandboxed app

2. Detection Capabilities - App

Jailbreaks

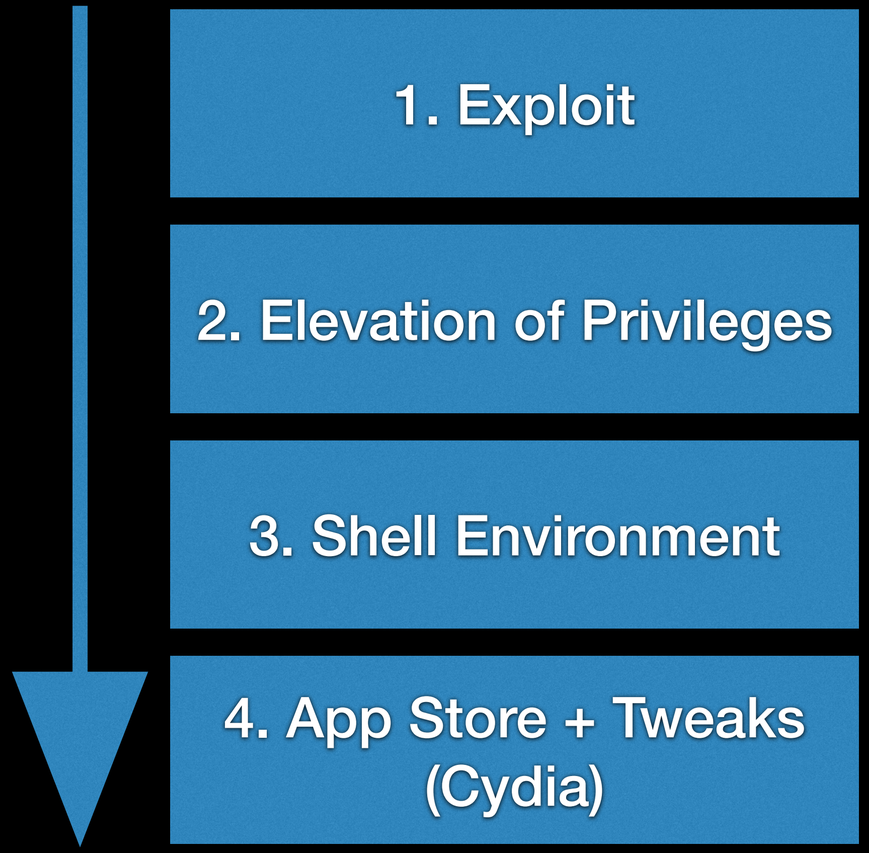
App Jailbreaks

- Need an Application to start the jailbreak
- Semi (Untethered)
- unc0ver, Fugu15, Cheyote (not released)

Boot Jailbreaks

- Jailbreak during device boot
- Tethered
- Checkra1n, Palera1n

The process of jailbreaking



Malware vs Jailbreaks

Malware

Jailbreaks

Attacker oriented	User - oriented
0-Days	Known Exploits
Stealth	Open
Extract Data + Control	Liberate Device + Apps
(Un)detectable	Detectable
Only few known examples	Many known examples
Targeted	Mass Market

Jailbreak Detection in 2023

Detection Mechanisms

Files / Folders on disk

Changes on the device (remounted root partition)

Process / SharedCache Injection

Disabled Security Mechanisms

Protocol Handlers

Reporting …

- „Jailbreak“ detected
- One event triggers detection

Malware detection with Apps

We can use everything that Apple allows us to do ;)

- Check for for the existence of a file
-> We cant read it (so we don’t know if its really an issue)
-> „com.apple.CrashReporter.plist“ a bad example (also in Beta)

- Install a VPN Profile / Proxy to inspect network traffic
-> We cant decrypt traffic
-> If the infrastructure is known we can use it to detect infections

- Similar to jailbreaks we can detect the absence of security mechanisms or manipulation of the app

2. Detection Capabilities - App - Data

Method	App List	Crash Logs	Files	Network	Processes
App*			✓**	✓	

* Under the assumption of a sandboxed app ** Only for known file path

2. Detection Capabilities - App - Malware

Malicious	App*	MDM	Companion	Forensic
Apps				
Profiles				
Known Implants	✓**			
Unknown Implants				

* Under the assumption of a sandboxed app ** Only for known file path

3. Detection Capabilities - Companion / MDM

Mobile Device Management - MDM

Allows companies to control certain behavior of iOS devices

Features depend on:

- Apples MDM Protokoll

https://developer.apple.com/documentation/devicemanagement
https://github.com/apple/device-management

- Supervised vs. Non-Supervised Devices

https://support.apple.com/en-gb/guide/deployment/dep0f7dd3d8/web

Mobile Device Management - MDM

Detection:

- DeviceInformation (iOS Version…)
- ConfigurationProfileList
- CertificateList
- ProvisioningProfileList
- InstalledApplicationList

Mobile Device Management - MDM

Prevention:

- Trust new proprietary in-house apps developers
- Users accept untrusted TLS certificates
- Allow a configuration profile to be installed (Supervised Only)

Companion App - lockdownd

Uses Apple's Lockdown Daemon (lockdownd) on a desktop

- Used by Xcode, Apple Configurator, iTunes, …

- Starts services that are accessible via USB connections

Can be accessed via commercial tools like iMazing or FOSS like libimobiledevice

- https://libimobiledevice.org

-> Currently developed by @nikias

-> Available for Linux, Mac & Windows

libimobiledevice - Supported (iOS 13.5)

Lockdown Service	Status	iOS Version	Comment
com.apple.afc	Done	13.5.1	Fully implemented except a few details.
com.apple.companion_proxy	Partly	11	
com.apple.iosdiagnostics.relay	Done	11	Fully implemented except a few details.
com.apple.mobile.diagnostics_relay	Done	11	Fully implemented.
com.apple.mobile.heartbeat	Done	11	Fully implemented.
com.apple.mobile.house_arrest	Done	11	Fully implemented.
com.apple.mobile.insecure_notification_proxy	Done	11	Fully implemented.
com.apple.mobile.installation_proxy	Done	11	Fully implemented.
com.apple.mobile.mobile_image_mounter	Done	11	Fully implemented.
com.apple.mobile.notification_proxy	Done	11	Fully implemented.

libimobiledevice - Supported (iOS 13.5)

Lockdown Service	Status	iOS Version	Comment
com.apple.mobileactivationd	Done	11	Fully implemented.
com.apple.mobilebackup	Done	11	Fully implemented.
com.apple.mobilebackup2	Done	11	Fully implemented.
com.apple.mobilesync	Partly	11	Partly implemented.
com.apple.preboardservice	Partly	11	Partly implemented.
com.apple.preboardservice_v2	Partly	11	Partly implemented.
com.apple.springboardservices	Partly	11	Partly implemented.
com.apple.syslog_relay	Done	11	Fully implemented.
com.apple.webinspector	Done	11	Fully implemented.

libimobildevice - unsupported (iOS 13.5)

Lockdown Service	Status	iOS Version	Description
com.apple.atc	None	11	
com.apple.atc2	None	11	
com.apple.bluetooth.BTPacketLogger	None	11	
com.apple.crashreportcopymobile	Done	11	*Is implemented - but unsure if fully supported
com.apple.crashreportmover	Done	11	*Is implemented - but unsure if fully supported
com.apple.idamd	None	11	
com.apple.misagent	None	11	
com.apple.mobile.assertion_agent	None	11	
com.apple.mobile.file_relay	None	11	
com.apple.mobile.MCInstall	None	11	
com.apple.os_trace_relay	None	11	
com.apple.pcapd	None	11	
com.apple.PurpleReverseProxy.Conn	None	11	
com.apple.PurpleReverseProxy.Ctrl	None	11	
com.apple.streaming_zip_conduit	None	11	

libimobildevice - Tools

Utility	Description	Detection Features
idevice_id	List attached devices or print device name of given device	
idevicebackup2	Create or restore backup for devices (idevicebackup for iOS < 4)	
idevicecrashreport	Retrieve crash reports from a device	Retrieve Crashlogs & Sysdiagnose Information
idevicedate	Display the current date or set it on a device	
idevicedebug	Interact with the debugserver service of a device	
idevicedebugserverproxy	Proxy a debugserver connection from a device for remote debugging	
idevicediagnostics	Interact with the diagnostics interface of a device	
ideviceenterrecovery	Make a device enter recovery mode	
ideviceimagemounter	Mount disk images on the device	
ideviceinfo	Show information about a connected device	
*ideviceinstaller	*Manage Apps on the device	*List Apps
idevicename	Display or set the device name	
idevicenotificationproxy	Post or observe notifications on a device	
idevicepair	Manage host pairings with devices and usbmuxd	
ideviceprovision	Manage provisioning profiles on a device	Retrieve Provisioning Profiles -> 3rd Party Apps
idevicescreenshot	Gets a screenshot from the connected device	
idevicesetlocation	Simulate location on device	
idevicesyslog	Relay syslog of a connected device	Live Syslog Information

3. Detection Capabilities - Companion / MDM - Data

Method	App List	Crash Logs	Files	Network	Processes
App*			✓**	✓	
MDM	✓				
Companion	✓	✓		✓	
Backup					
Sysdiagnose					

* Under the assumption of a sandboxed app ** Only for known file path

3. Detection Capabilities - Companion / MDM - Malware

Malicious	App*	MDM	Companion	Forensic
Apps		✓	✓	
Profiles		✓	✓	
Known Implants	✓**			
Unknown Implants				

* Under the assumption of a sandboxed app ** Only for known file path

4. Detection Capabilities - Forensics

4. Detection Capabilities - Forensics

File System:

- iTunes Backup (via lockdownd)
- Full FileSystem extraction (Jailbreak required)

Diagnostic Information:

- CrashLogs (via lockdownd)
- Sysdiagnose (via lockdownd)

Forensic Data - iTunes Backup

Can be created on multiple ways

- Commercial Forensic Tool (Cellebrite, Elcomsoft, Magnet…)
- iMazing (there is a free version available)
- iTunes / Finder
- libimobildedevice

Encrypted & Unencrypted Backups
- Encrypted Backups contain a lot more sensitive information

Forensic Data - Analyzing Backups

Commercial Tools (Cellebrite, Magnet, …)
- Will help to decode data and display contents
- Not focused on malware detection

Multiple opensource tools available like:
- https://github.com/avibrazil/iOSbackup (Python)
- Allow easy access to data. Parsing iOS files (plist, sqlite databases, NSKeyedArchiver… might be cumbersome

Trainings available to navigate iOS Backups / FS data
e.g. SANS FOR 518 (Created by Sarah Edwards)

Forensic Data - Analyzing Backups - MVT

Developed by Amnesty International Tech Lab

Created to make iOS forensic artifact analysis a lot easier
Focus on Spyware Analysis
- https://mvt.re/

- https://github.com/mvt-project/mvt

Works on iTunes Backups & FileSystem dumps, supports STIX2 for IOCs

* Amnesty Investigations IOCs - https://github.com/AmnestyTech/investigations

Forensic Data - Analyzing Backups - MVT

On backup analysis records are extracted

- Some sample records* are:

Record	Specific Files	Detection Features
applications.json	Info.plist, iTunesMetadata.plist	List of Apps, Non AppStore Apps
configuration_profiles.json	Configuration Profiles	Configuration Profiles
shortcuts.json	/private/var/mobile/Library/Shortcuts/Shortcuts.sqlite	Might be used for persistence
interaction_c.json	/private/var/mobile/Library/CoreDuet/People/interactionC.db	Interaction with installed Apps
manifest.json	Manifest.db	Some FilePaths
os_analytics_ad_daily.json	/private/var/mobile/Library/Preferences/com.apple.osanalytics.addaily.plist	Data Usage by Processes
datausage.json	/private/var/wireless/Library/Databases/DataUsage.sqlite	Network Data Usage by Processes, Bundle Identifier
profile_events.json	Configuration Profiles	Changes on Configuration Profiles
shutdown_log.json		
tcc.json	/private/var/mobile/Library/TCC/TCC.db,	Access to Microphone, Camera, Location

- Additionally records for Domains/URLs & FileSystem dumps

* https://docs.mvt.re/en/latest/ios/records/

Forensic Data - Crashes & Sysdiagnose

iOS keeps logs app and kernel crashes; can be seen in the settings app:

- *Settings -> Data Privacy & Security*
-> Analysis & Improvements -> Analysis Data

Sysdiagnose has to be triggered manually & will be available in the same place
-> iPhone X key combination: Volume Up + Down + Power for 0.7 Seconds)

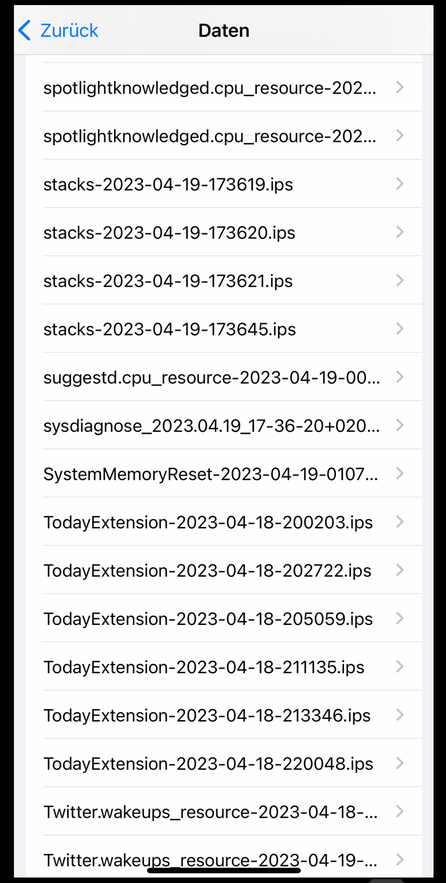
https://developer.apple.com/bug-reporting/profiles-and-logs/?name=sysdiagnose

Forensic Data - Crashes & Sysdiagnose

1) Key combination 2) Wait ~ 5 min 3) Check folder

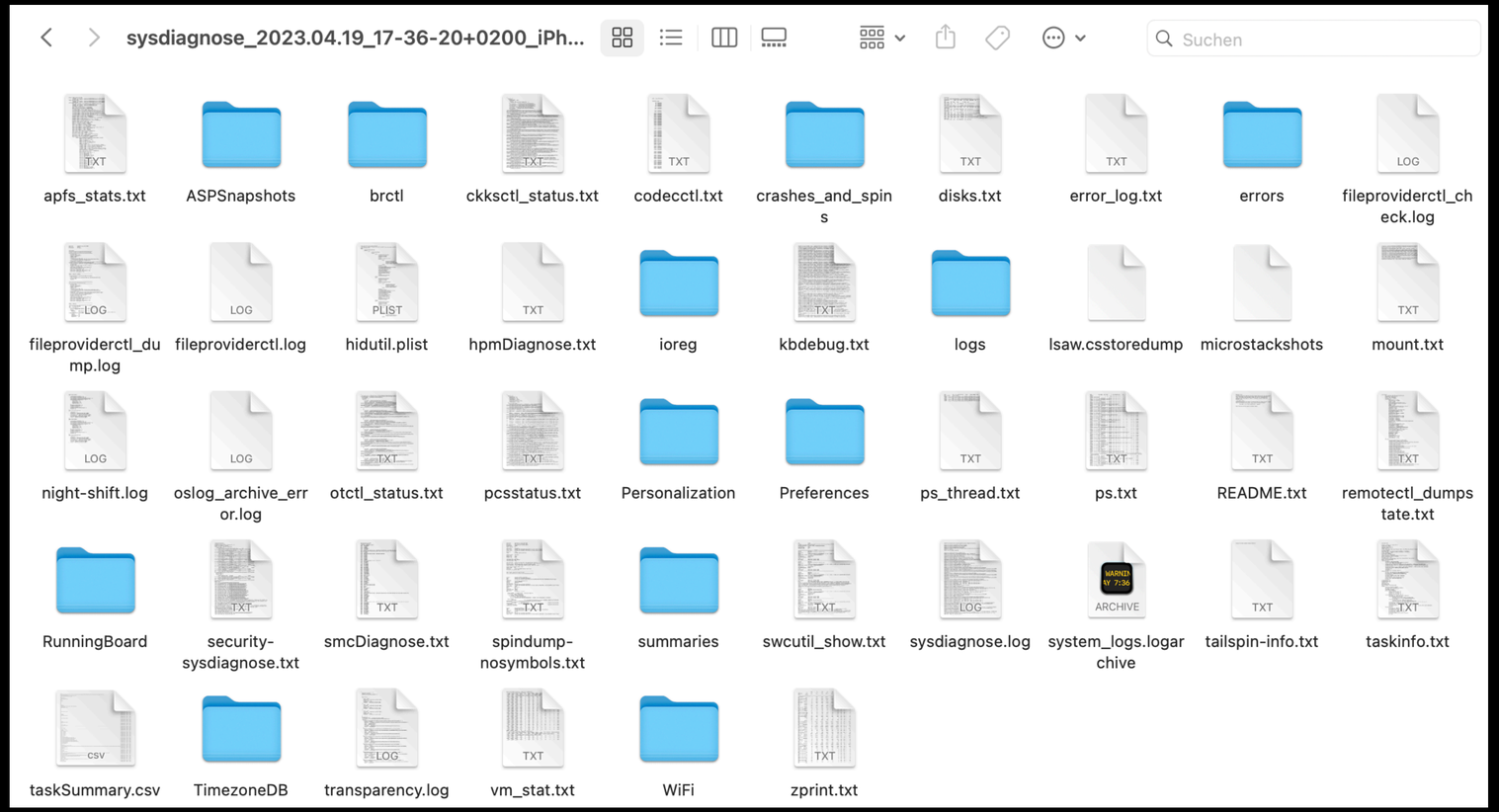
sysdiagnose file is roughly 100 - 500 MB of data

You can sent the file via share dialog or
- sync with iTunes
 (~/Library/Logs/CrashReporter/MobileDevice/)
- copy crashlogs with libimobiledevice



Forensic Data - Sysdiagnose

Lets have a look:



Forensic Data - Sysdiagnose

Contains basically everything interesting you want to look at ;)
- Process Names
- Mount / Partition Information
- App Names, Updates & Uninstalls
- Information on Backups

Excellent Paper available at: http://www.for585.com/sysdiagnose

Tools to parse sysdiagnose data:
https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts
https://github.com/abrignoni/iLEAPP

4. Detection Capabilities - Forensics - Data

Method	App List	Crash Logs	Files	Network	Processes
App*			✓**	✓	
MDM	✓				
Companion	✓	✓		✓	
Backup	✓		✓	✓	✓
Sysdiagnose	✓	✓	✓	✓	✓

* Under the assumption of a sandboxed app ** Only for known file path

4. Detection Capabilities - Forensics - Malware

Malicious	App*	MDM	Companion	Forensic
Apps		✓	✓	✓
Profiles		✓	✓	✓
Known Implants	✓**			✓
Unknown Implants				✓

* Under the assumption of a sandboxed app ** Only for known file path

5. Synthesis - Bringing it all together

Manual vs. (Semi) - Automatic Detections

	Automatic		Semi - Automatic	
Malicious	App*	MDM	Companion	Forensic
Apps		✓	✓	✓
Profiles		✓	✓	✓
Known Implants	✓**			✓
Unknown Implants				Manual ✓

* Under the assumption of a sandboxed app ** Only for known file path

Manual vs. (Semi) - Automatic Detections

All the tools are available to detect our known malware samples

- some: can be detected automatically
- all: can be detected semi-automatically with a companion app / forensic analysis

There are manual tools available to detect unknown malware samples if
- a device is infected
- a proper forensic & sysdiagnose analysis is executed

Status Quo - Implementation

Most companies will only do the automatic detections (MDM + App) as this is available and known

To improve we need:
- companion apps and tools to support analysis
- skilled people that can do an analysis
- people to train other people in malware detection
- to make data extraction and analysis easier

What to do if your phone be.a.es w.i.d.y

Contact an expert:

Apple recommends in their threat notifications:
https://securityplanner.consumerreports.org/tool/emergency-resources

Amnesty International & CitizenLab are known to be experts in the field.
Feel free to contact us at Trail of Bits / iVerify
https://www.iverify.io/contact /

6. Improving the detection

Improving Jailbreak Detection - 2023

Reporting …

„Jailbreak“ detected

One event triggers detection

Better Reporting

Don’t detect Jailbreaks, detect mal. behavior!

Every event is reported for analysis

Differentiate active & inactive Jailbreaks

App Jailbreak vs. Boot Jailbreak

Validate findings (iOS Version, Device Type…)

Improving Malware Detection

Apple	Companies	iOS Experts + Defensive Companies
(Code Quality and Exploitation)	Crash log & Forensic Analysis	Crash log & Forensic Analysis
Endpoint security capabilities	Companion App	Training on Malware detection
FileSystem and Process Access	Monitoring network traffic	Set Focus on Malware Detection

Further Research

Combining EMM / MTD with Crash Log & Forensic Analysis

Combining iOS and macOS Agents

iOS Backups / FileSystem / Syslog Data

Conclusion

Apple’s walled garden raises the bar for exploitation every year

We need more focus on malware detection

Improvements have to be make on several levels

It is not possible to detect _new_ malware with an app on the device

We need more companion apps for forensic analysis

We need more training & skilled people

Conclusion

„…The capability to target and monitor the private activities of entire populations in real time.“

Ian Beer (2019)

Additional Information + Contact Data

Spyware Information (Twitter)

Contact me on

Twitter

LinkedIn

Thank you!