Objective by the Sea v6.0
The Mac Security Conference

Poisoned 🍏🍎 - How do we find them?

Matthias Frielingsdorf, 12.10.2023

Who am i?

Matthias Frielingsdorf

VP of Research - iVerify

Research of iOS Malware & Mobile Device Security

Twitter | X | Discord @helthydriver

Today

- **Recap**
- Updates on iOS Malware discovered in 2023
- Steps to discover iOS Malware (Forensic Analysis)
- Demo: Creating Forensic Artifacts
- Analysis
- Conclusion

Conclusion

- Apple’s walled garden raises the bar for exploitation every year
- Malware != Jailbreaks
- Typical jailbreak detection is aimed at user jailbreaks
- It is not possible to detect [unknown] exploits & malware with an app on the device
- Improvements have to be make on several levels
- No one can fight this problem alone!

Some Research Ideas

- Combining EMM / MTD with Crash Log & Forensic Analysis
- Combining iOS and macOS Agents
- iOS Backups / FileSystem dumps contain a lot of data…

iOS CVEs - „actively exploited“

CVE-2016-4657	CVE-2019-6217	CVE-2021-30883	CVE-2021-30869	CVE-2023-42827	CVE-2023-32373
CVE-2016-4655	CVE-2019-7286	CVE-2021-1870	CVE-2021-1879	CVE-2023-42827	CVE-2023-28209
CVE-2016-4656	CVE-2019-7287	CVE-2021-1782	CVE-2021-30761	CVE-2023-41991	CVE-2023-32409
CVE-2017-2505	CVE-2020-27930	CVE-2021-30762	CVE-2022-22587	CVE-2023-41993	CVE-2023-37450
CVE-2017-7064	CVE-2020-27950	CVE-2021-30663	CVE-2022-22674	CVE-2023-41992	CVE-2023-5217
CVE-2017-13861	CVE-2020-27932	CVE-2021-30661	CVE-2022-22675	CVE-2023-23529	CVE-2023-42824
CVE-2018-4438	CVE-2021-31010	CVE-2021-30665	CVE-2022-32917	CVE-2023-28205	CVE-2023-41064
CVE-2018-4122	CVE-2021-30858	CVE-2021-1871	CVE-2022-32894	CVE-2023-28206	CVE-2023-41061
CVE-2018-4442	CVE-2021-30807	CVE-2021-30983	CVE-2022-32893	CVE-2022-42827	CVE-2023-32434
CVE-2019-6225	CVE-2021-30666	CVE-2021-30860	CVE-2022-22620	CVE-2022-42856	CVE-2023-32435

iOS CVEs - „actively exploited“

CVE-2016-4657	CVE-2019-6217	CVE-2021-30883	CVE-2021-30869	CVE-2023-42827	CVE-2023-32373
CVE-2016-4655	CVE-2019-7286	CVE-2021-1870	CVE-2021-1879	CVE-2023-42827	CVE-2023-28209
CVE-2016-4656	CVE-2019-7287	CVE-2021-1782	CVE-2021-30761	CVE-2023-41991	CVE-2023-32409
CVE-2017-2505	CVE-2020-27930	CVE-2021-30762	CVE-2022-22587	CVE-2023-41993	CVE-2023-37450
CVE-2017-7064	CVE-2020-27950	CVE-2021-30663	CVE-2022-22674	CVE-2023-41992	CVE-2023-5217
CVE-2017-13861	CVE-2020-27932	CVE-2021-30661	CVE-2022-22675	CVE-2023-23529	CVE-2023-42824
CVE-2018-4438	CVE-2021-31010	CVE-2021-30665	CVE-2022-32917	CVE-2023-28205	CVE-2023-41064
CVE-2018-4122	CVE-2021-30858	CVE-2021-1871	CVE-2022-32894	CVE-2023-28206	CVE-2023-41061
CVE-2018-4442	CVE-2021-30807	CVE-2021-30983	CVE-2022-32893	CVE-2022-42827	CVE-2023-32434
CVE-2019-6225	CVE-2021-30666	CVE-2021-30860	CVE-2022-22620	CVE-2022-42856	CVE-2023-32435

Today

- Recap
- **Updates on iOS Malware discovered in 2023**
- Steps to discover iOS Malware (Forensic Analysis)
- Demo: Creating Forensic Artifacts
- Analysis
- Conclusion

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

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/

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/

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/

2023 - Operation Triangulation

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

Infection Vector

Homekit, iMessage,
FindMy

Targets

Kaspersky

Detection & Technical Analysis

Kaspersky

CVEs

Kernel	CVE-2023-32434
WebKit	CVE-2023-32435

Detection

Network & Forensic Analysis

IOCs

Processes
Links

Attribution

???

https://securelist.com/operation-triangulation/109842/
https://securelist.com/find-the-triangulation-utility/109867/
https://securelist.com/triangledb-triangulation-implant/110050/

2023 - Pegasus v4

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

Infection Vector

PassKit, iMessage

Targets

Journalists

Detection & Technical Analysis

CitizenLab

CVEs

ImageIO CVE-2023-41064
Wallet CVE-2023-41061

Detection

Forensic Analysis

IOCs

Files?
Processes?
Crashes?

Attribution

NSO

https://citizenlab.ca/2023/09/pegasus-infection-of-galina-timchenko-exiled-russian-journalist-and-publisher/

2023 - Predator v2

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

Infection Vector

WebKit (0-Click)

Targets

President of EU Parliament, Former MP of Egypt

Detection & Technical Analysis

CitizenLab, Amnesty International, Google TAG

CVEs

Kernel	CVE-2023-41992
Security	CVE-2023-41991
WebKit	CVE-2023-41993

Detection

Forensic Analysis
Network Analysis

IOCs

Files?
Processes
Links

Attribution

Intelexa, Cytrox

https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/
https://www.amnesty.org/en/documents/act10/7245/2023/en/
https://blog.google/threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-egypt/

2023 Predator Validation Steps

1. Check Running Processes from /private/var/mp
2. Check for Log Monitoring
3. Check Location
4. Check if Developer Mode is enabled
5. Check for Jailbreaks
6. Check for „unsafe“ Processes
7. Check for Proxies
8. Check for additional root Certificate Authorities

https://citizenlab.ca/2023/10/predator-spyware-targets-us-eu-lawmakers-journalists/

Today

- Recap
- Updates on iOS Malware discovered in 2023
- **Steps to discover iOS Malware (Forensic Analysis)**
- Demo: Creating Forensic Artifacts
- Analysis
- Conclusion

Detecting Mercenary Spyware: Target Data

Sample	App List	Crash Logs	Files	Network	Processes
2019		✓	✓	✓	✓
Hermit	✓	✓	✓	✓	✓
jamf Report			✓		✓
Reign		✓	✓	✓	✓
Pegasus		✓	✓	✓	✓
Predator		✓	✓	✓	✓
Operation Triangulation		✓		✓	✓

Detection Capabilities - App & MDM

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

Detection Capabilities - Companion

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

Detection Capabilities - Backup

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

Detection Capabilities - Sysdiagnose

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

Detection Capabilities vs. Target 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

Forensic Data - Analyzing Backups

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 - 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

Create Backups with: iTunes, Finder, iMazing, libimobiledevice…

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

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

https://github.com/EC-DIGIT-CSIRC/sysdiagnose (Good for Malware Analysis!)

New!

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

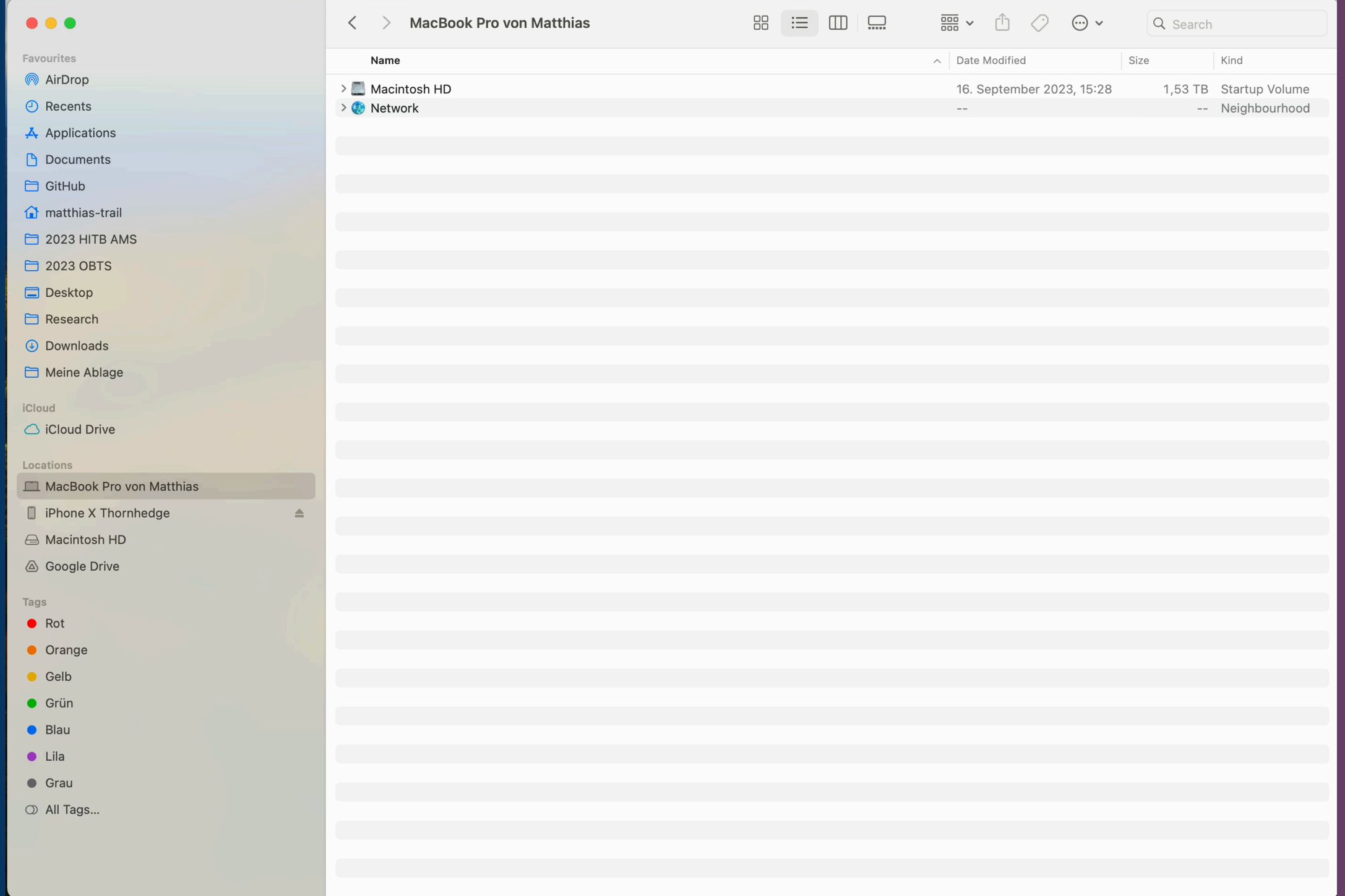
Today

- Recap
- Updates on iOS Malware discovered in 2023
- Steps to discover iOS Malware (Forensic Analysis)
- **Demo: Creating Forensic Artifacts**
- Analysis
- Conclusion

How to - iTunes Backup - Forensic Analysis

1. Connect your iPhone (Trust)
2. Open Finder and select your iPhone
3. Turn on Encryption (Please remember the complex password!!!)
4. Take a Backup
5. Run mvt to decrypt the backup
6. Run mvt to analyze the decrypted backup

Demo - iTunes Backup

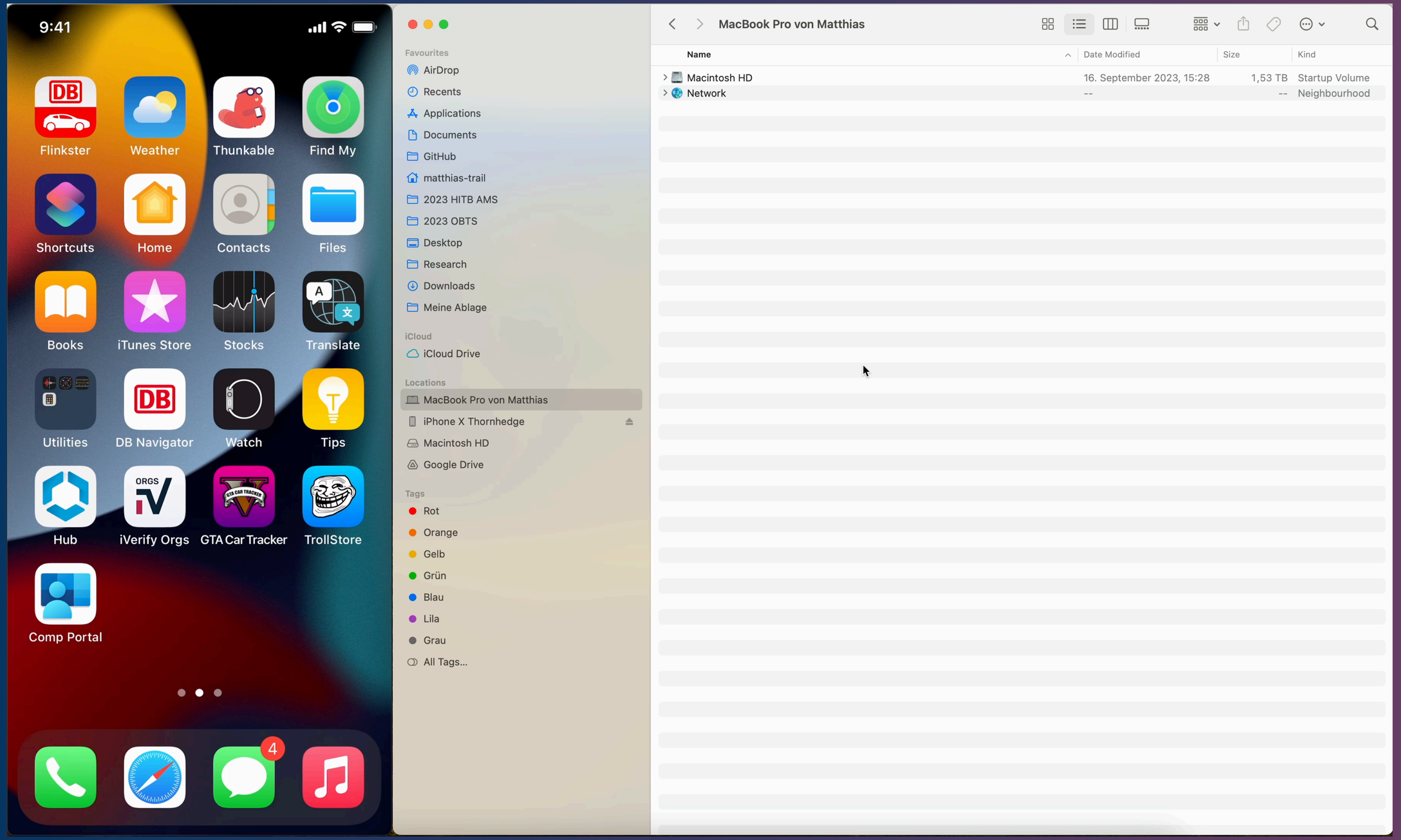

MacBook Pro von Matthias
Search
Favourites
AirDrop
Recents
Applications
Documents
GitHub
matthias-trail
2023 HITB AMS
2023 OBTS
Desktop
Research
Downloads
Meine Ablage
iCloud
iCloud Drive
Locations
MacBook Pro von Matthias
iPhone X Thornhedge
Macintosh HD
Google Drive
Tags
Rot
Orange
Gelb
Grün
Blau
Lila
Grau
All Tags...
Name
Date Modified
Size
Kind
Macintosh HD
16. September 2023, 15:28
1,53 TB
Startup Volume
Network
--
--
Neighbourhood

How to - Sysdiagnose - Forensic Analysis

1. Run sysdiagnose on your iPhone*
2. Wait until it is finished
3. Connect your iPhone (Trust)
4. Sync your iPhone with Finder
5. *Stored in: ~/Library/Logs/CrashReporter/MobileDevice/*
6. *Analyze with EU-CSIRT Tools*

* https://it-training.apple.com/tutorials/support/sup075

Demo - Sysdiagnose


9:41
Flinkster
Weather
Thunkable
Find My
Shortcuts
Home
Contacts
Files
Books
iTunes Store
Stocks
Translate
Utilities
DB Navigator
Watch
Tips
Hub
iVerify Orgs
GTA Car Tracker
TrollStore
Comp Portal
Favourites
AirDrop
Recents
Applications
Documents
GitHub
matthias-trail
2023 HITB AMS
2023 OBTS
Desktop
Research
Downloads
Meine Ablage
iCloud
iCloud Drive
Locations
MacBook Pro von Matthias
iPhone X Thornhedge
Macintosh HD
Google Drive
Tags
Rot
Orange
Gelb
Grün
Blau
Lila
Grau
All Tags...
MacBook Pro von Matthias
Name
Date Modified
Size
Kind
Macintosh HD
16. September 2023, 15:28
1,53 TB
Startup Volume
Network
--
--
Neighbourhood

Today

- Recap
- Updates on iOS Malware discovered in 2023
- Steps to discover iOS Malware (Forensic Analysis)
- Demo: Creating Forensic Artifacts
- **Analysis**
- Conclusion

Manual vs. (Semi) - Automatic Detections

	Automatic		Semi - Automatic	
Malicious	App*	MDM	Companion	Forensic
Apps		✓	✓	✓
Profiles		✓	✓	✓
Known Merc. Spyware	✓**			✓
Unknown Merc. Spyware				Manual ✓

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

Challenges with Forensic Analysis

- Sysdiagnose takes 10 - 15 Minutes in total
- iTunes Backups may take **hours** depending on the size and USB
- Both need user interaction
- Both need experts to analyze for unknown bugs
- Public analysis tools require some knowledge of IT (Python..)
- Typical forensic trainings don’t include iOS Malware analysis
- Forensic experts or organizations that can do the analysis are scarce

Mobile Forensics Hygiene / Guidelines for targeted Persons

1. Install the latest OS Version always as soon as possible!
2. Do a first encrypted Backup
3. Do sysdiagnose weekly / monthly sysdiagnose
4. Do follow-up Backups with the same Mac (faster, cause incremental)
5. Check iCloud.com / iMessage for Apple Security Notifications
6. If your iPhone behaves weird?
    1. Do another sysdiagnose
    2. Restart your iPhone

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

Contact an Expert!

Feel free to contact us at iVerify
https://www.iverify.io/contact

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

Amnesty International & CitizenLab are also known to be experts in the field.

Thats it…

One more Thing!

2023 Predator Validation Steps

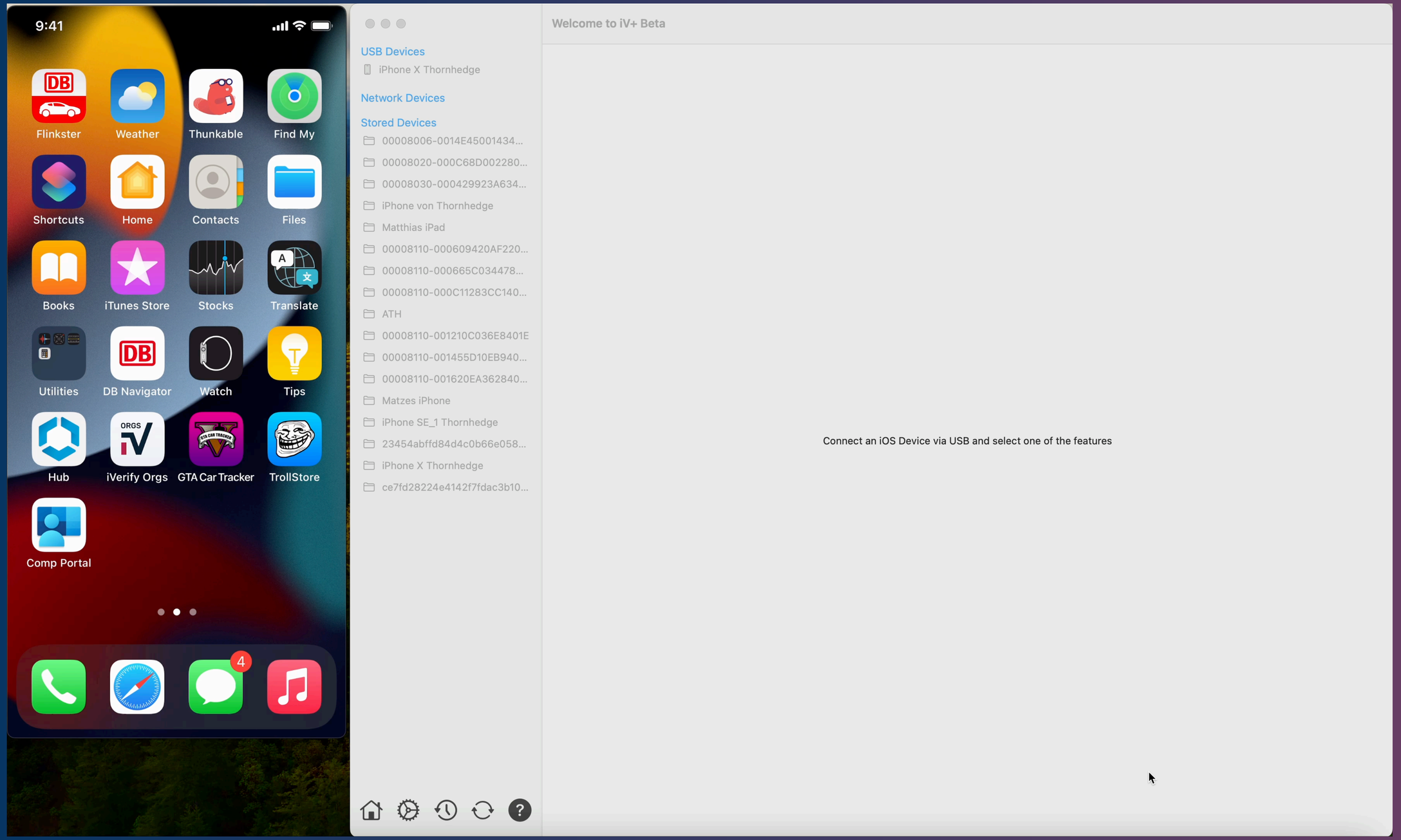
1. Check Running Processes from /private/var/mp
2. Check for Log Monitoring
3. Check Location
4. **Check if Developer Mode is enabled**
5. Check for Jailbreaks
6. Check for „unsafe“ Processes
7. Check for Proxies
8. Check for additional root Certificate Authorities

https://citizenlab.ca/2023/10/predator-spyware-targets-us-eu-lawmakers-journalists/

Developer Mode

- Security Features introduced in iOS 16
- User needs to turn it on in the Settings App
- Includes tools that are made available for debugging
- Might give access to some interesting data ;)
- **What if we turn Developer Mode on to prevent from Predator?**
- **Pro**
  - Insights into telemetry data, Prevention of Predator infection
- **Cons**
  - Allows to build easier Exploits, Enables Side-loading (with User Interaction)

Demo - Developer Mode


9:41
Flinkster
Weather
Thunkable
Find My
Shortcuts
Home
Contacts
Files
Books
iTunes Store
Stocks
Translate
Utilities
DB Navigator
Watch
Tips
Hub
iVerify Orgs
GTA Car Tracker
TrollStore
Comp Portal
4
USB Devices
iPhone X Thornhedge
Network Devices
Stored Devices
00008006-0014E45001434...
00008020-000C68D002280...
00008030-000429923A634...
iPhone von Thornhedge
Matthias iPad
00008110-000609420AF220...
00008110-000665C034478...
00008110-000C11283CC140...
ATH
00008110-001210C036E8401E
00008110-001455D10EB940...
00008110-001620EA362840...
Matzes iPhone
iPhone SE_1 Thornhedge
23454abffd84d4c0b66e058...
iPhone X Thornhedge
ce7fd28224e4142f7fdac3b10...
Welcome to iV+ Beta
Connect an iOS Device via USB and select one of the features

Today

- Recap
- Updates on iOS Malware discovered in 2023
- Steps to discover iOS Malware (Forensic Analysis)
- Demo: Creating Forensic Artifacts
- Analysis
- **Conclusion**

Improving Malware Detection

Apple	Companies	iOS Experts + Defensive Companies
(Code Quality and Exploitation)	Crash log & Forensic Analysis	Crash log & Forensic Analysis
Endpoint security capabilities	Strategy for targeted Persons	Training on Malware detection
FileSystem and Process Access	Monitoring network traffic	Set Focus on Malware Detection
Security Research Devices		

Conclusion

- We got 4 different samples of Mercenary Spyware reported in 2023!
- We got multiple reports on infections this year high ranking politicians, managers, journalists
- **Its not getting better, its getting worse :/**

- Mercenary Spyware can be detected by manual forensic analysis but not prevented
- Forensic Analysis works, but it has its challenges that we need to solve
- Do Backups and Sysdiagnose to support the analysis

Some courtesy info

Scan your iPhone / iPad for Malware here at OBTS
Today - Coffee Break - Before the Conference Room
Tomorrow - 09:15 - 10:00 - Before the Conference Room

Sign up for the iVerify+ Beta at:
https://tinyurl.com/StopPegasus

Training on iOS Forensic Malware Analysis:
https://www.blackhat.com/eu-23/training/schedule/index.html#ios-threat-hunting---lets-catch-a-pegasus-virtual-33906

Conclusion

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

Ian Beer (2019)

Thanks

Contact me on:

Spyware Information (Twitter)

Twitter

LinkedIn

iVerify+ Beta

OBTS v5: https://objectivebythesea.org/v5/talks/OBTS_v5_mFrielingsdorf.pdf
HITB AMS 2023: https://conference.hitb.org/hitbsecconf2023ams/session/poisoned-apples-current-state-of-ios-malware-detection/

iVerify.

Additional Material

Book Recommendation:

Pegasus - How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy

By: Laurent Richard and Sandrine Rigaud

ISBN: 9781250858689