

iVerify.

Matthias Frielingsdorf

Placeboed Apples
A New Way to Hunt Spyware on iOS

OBTSv8 - Oct 17th, 2025

helthydriver

Who am I



1. Co-Founder and VP of Research at iVerify
2. iOS Malware and Exploitation
3. Basketball and Board Games

helthydriver

Whats the Job of an iOS Threat Hunter?

Whats the Job of an iOS That Hunter?

Whats the Job of an iOS Thread Hunter?

 +  = 





+



=







+



=





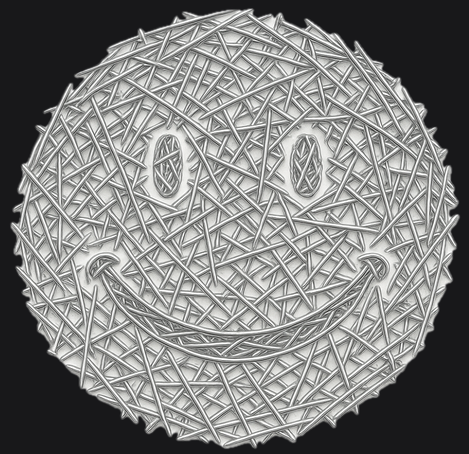






2021 2022 2023 2024 2025





+



=







Today

1. iOS Malware Overview & Detailed Behavior
2. iOS Malware Simulation
3. Demo

Why Malware Simulation?

1 Finding new IOCs



2 Understanding Spyware



3 Quality Check Detections



Study Malware Behavior

Samples ☣️



If you want to donate:

matthias@iverify.io | helthydriver

A Malware Attack Example

Infiltration

Code Execution

Exit

Attack Process → Sandbox Escape → Privilege Escalation → Implant → Exfiltration → Clean-Up* → Exit Device

Crashes | Logs | Files | Network

Logs | Crashes | Processes | Networks | Files

*Earlier Attacks also had Persistency Modules

<=2021 Pegasus Exploit



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

Infection Vector

iMessage

Detection & Technical Analysis

Citizen Lab, Amnesty, Google Project 0

Attribution

NSO

IOCs

URLs
Emails
Processes
Files

Targets

Journalists
Politicians
Human Rights Activists

Detection

Forensic Analysis

CVEs

CVE-2021-30860

ForcedEntry Attack Example



Infiltration

Code Execution

Exit

Attacking iMessage → Sandbox Escape → Privilege Escalation → Implant → Exfiltration → Clean-Up → Exit Device

Crashes | Logs | Files | Network

Logs | Crashes | Processes | Networks | Files

2021 Pegasus Clean Up / Hiding

1. Launch from /private/var/db/com.apple.xpc.roleaccountd.staging
2. Half-Delete Entries in DataUsage.sqlite
3. Stalls Shutdowns
4. Deletes Crashlogs and iMessages

2022 Pegasus Clean Up / Hiding

1. Launch from /private/var/db/com.apple.xpc.roleaccountd.staging*
2. Delete Shutdown.log entries
3. Helper spawns from /private/var/tmp
4. Disguises as System Processes - com.apple.WebKit.Networking

***Full Path - /private/var/db/com.apple.xpc.roleaccountd.staging/com.apple.WebKit.Networking**

On Shutdown.log

1. Useful for Pegasus 2021 - 2022 and Predator 2021 detections.
2. Keeps historic data of all shutdown on the device
3. Pegasus 2022 started to clean it (but failed once again)
4. iOS 26 changes the behavior
    1. Shutdown.log entries are now only kept for the last reboot
    2. Make sure you collect a sysdiagnose before updating!
    2. Otherwise you are losing any chance of investigation :/

2023 Pegasus BLASTPASS Exploit



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

Infection Vector

HomeKit
iMessage

Detection & Technical Analysis

Citizen Lab & Amnesty & iVerify

Attribution

NSO

IOCs

HomeKit Account
iMessage Attachment

Targets

Journalists

Detection

Forensic Analysis

CVEs

CVE-2023-41061
CVE-2023-41064

BLASTPASS Attack Example



Infiltration

Code Execution

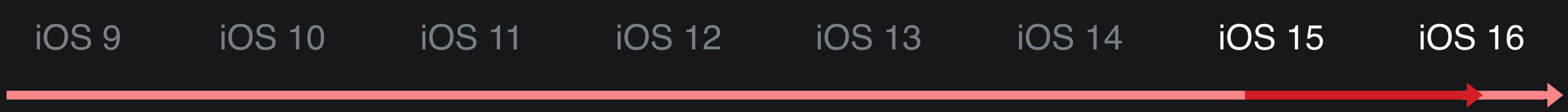
Exit

Attacking HomeKit → Attacking iMessage → Privilege Escalation → Implant → Exfiltration → Clean-Up → Exit Device

Crashes | Logs | Files | Network

Logs | Crashes | Processes | Networks | Files

2023 Operation Triangulation



Infection Vector

iMessage

Detection & Technical Analysis

Kaspersky

Attribution

Unknown

IOCs

Processes

Files

URL

Emails

Targets

Kaspersky

Detection

Network &
Forensic Analysis

CVEs

CVE-2023-32434

CVE-2023-32435

CVE-2023-41990

CVE-2023-38606

Operation Triangulation

Infiltration

Code Execution

Exit

Attacking iMessage → Attacking Safari → Privilege Escalation → Implant → Exfiltration → Clean-Up → Exit Device

Crashes | Logs | Files | Network

Logs | Crashes | Processes | Networks | Files

2023 Operation Triangulation - Clean-Up

1. Delete Crashlogs
2. Delete iMessage Attachments
3. Remove Traces from iMessage related Databases
4. Disguises as normal System Process (BackupAgent)
5. Spawns System Processes for Cleanup (imagent)

2023 Predator v2



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

Infection Vector

WebKit (0-Click)

Detection & Technical Analysis

Citizen Lab & Google TAG & Amnesty Tech

Attribution

Intellexa (Cytrox)

IOCs

Processes
Files

Targets

Former
MP of Egypt
EU Commission

Detection

Forensic &
Infrastructure Analysis

CVEs

CVE-2023-41991
CVE-2023-41992
CVE-2023-41993

Predator 2023

Infiltration

Code Execution

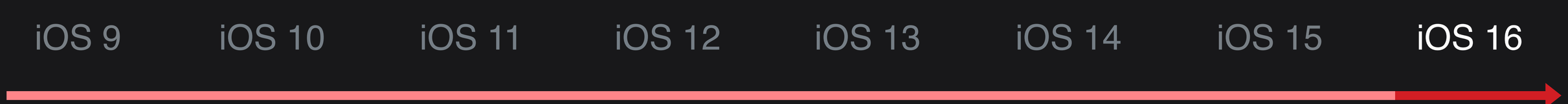
Exit

Attacking WebKit → Privilege Escalation → Implant → Exfiltration → Clean-Up → Exit Device

Crashes | Logs | Files | Network

Logs | Crashes | Processes | Networks | Files

2023 NoClip



Infection Vector

WebKit

Detection & Technical Analysis

Google TAG

Attribution

PARS Defense

IOCs

Unknown

Targets

Potentially Turkey

Detection

Web-Server Analysis

CVEs

CVE-2023-42916
CVE-2023-42917

```
__int64 __fastcall AgentEntry(RemoteProcessExecCtx *rproc)
{
  __int64 _18; // [xsp+18h] [xbp+8h]

  pwnCitizenLab(rproc, 1);                      // remove forensics traces
  pwnAppList(rproc, 1);                         // List all apps
  pwnCitizenLab(rproc, 1);
  pwnDeviceInfo(rproc, 1);                      // Device info
  pwnCitizenLab(rproc, 1);
  pwnLocationDbs(rproc, 1);                     // GPS
  pwnCitizenLab(rproc, 1);
  pwnStockApps(rproc, 1);                       // Data from stock apps (e.g. iMessages)
  pwnCitizenLab(rproc, 1);
  pwnContainers(rproc, 1);                      // SMS, call history, contacts
  pwnCitizenLab(rproc, 1);
  pwnThumbnails(rproc, 1);                      // All photos as thumbnails
  pwnCitizenLab(rproc, 1);
  pwnWifiInfo(rproc, 1);                        // Wifi info
  pwnCitizenLab(rproc, 1);
  pwnLessPriorityContainers(rproc, 1);          // less important db
  pwnCitizenLab(rproc, 1);
  pwnStockMailApp(rproc, 1);                    // emails
  pwnCitizenLab(rproc, 1);
  pwnTwitterDB(rproc, 1);                       // twitter
  if ( ((_18 ^ (2 * _18)) & 0x4000000000000000LL) != 0 )
    __break(0xC471u);
  return pwnCitizenLab(rproc, 1);
}
```



2023 NoClip

Infiltration

Code Execution

Exit

WebKit → Sandbox Escape → Privilege Escalation → Implant → Exfiltration → Clean-Up → Exit Device

Crashes | Logs | Files | Network

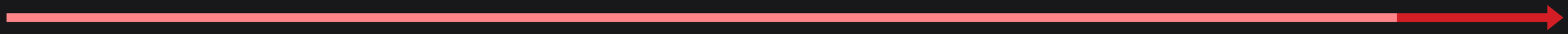
Logs | Crashes | Processes | Networks | Files

2023 NoClip Clean-Up Steps

1. Run pwnCitizenLab Function after every exfiltration
2. Delete all Crashlogs
3. Delete Unified Logs
4. Delete Aggregates (“90 Days Analytics Files”)
5. Clean Application, Identity and Launchd Logs
5. …

2025 Graphite

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



Infection Vector

iMessage

Detection & Technical Analysis

CitizenLab, Meta

Attribution

Paragon

IOCs

Small Pretzel
IPs

Targets

Journalists
Activist
Business

Detection

Apple Notifications
Meta Alerts

CVEs

CVE-2025-43200

Graphite

Infiltration

Code Execution

Exit

Attacking iMessage → Sandbox Escape → Privilege Escalation → Implant → Exfiltration → Clean-Up → Exit Device

Crashes | Logs | Files | Network

Logs | Crashes | Processes | Networks | Files

Is this all?

Exploited CVEs without Attribution

CVE-2023-5217

CVE-2024-23296

CVE-2024-23225

CVE-2025-31201

CVE-2025-31200

CVE-2023-42824

CVE-2025-24201

CVE-2025-24085

CVE-2023-42916

CVE-2023-42917

CVE-2024-44309

CVE-2024-44308

https://mythicalbeasts.dfrlab.org/

Infiltration

Implant

iOS Commercial Spyware Behavior

	Pegasus		Predator		Operation T	NoClip	Graphite
	2021	2023	2021	2023	2023	2023	2025
Crashes	✓	✓	✓	✓	✓	✓	✓
Emails	✓	✓			✓		✓
Files	✓	✓			✓		
URL			✓		✓	✓	
Process	✓	✓	✓	✓	✓	?	?
Files	✓	?	✓	✓	✓	✓	?
Network	✓	?	✓	✓	✓	✓	✓
Clean-Up	✓	✓	✓	✓	✓	✓	?

Infiltration

Implant

iOS Commercial Spyware Behavior

	Pegasus		Predator		Operation T	NoClip	Graphite
	2021	2023	2021	2023	2023	2023	2025
Crashes	✓	✓	✓	✓	✓	✓	✓
Emails	✓	✓			✓		✓
Files	✓	✓			✓		
URL			✓		✓	✓	
Process	✓	✓	✓	✓	✓	?	?
Files	✓	?	✓	✓	✓	✓	?
Network	✓	?	✓	✓	✓	✓	✓
Clean-Up	✓	✓	✓	✓	✓	✓	?

iVerify.

Today

1. iOS Malware Overview & Detailed Behavior
2. iOS Malware Simulation
3. Demo

Wishlist for Simulation

Infiltration		Min. Requires
Crashes	(Repeatedly) Crashing a process	App or Extension
Logs	Creating Unified Logs entries	App
Files	iMessage Attachments	Privileged Process or Mac*
Network	Domain and IP Connections	App

Wishlist for Simulation

	Code Execution	Min. Requires
Crashes	Panic the Kernel	Vulnerability
Logs	Creating Unified Logs entries	App
Files	/private/var/tmp*	Privileged Process
Networks	Domain and IP Connections	App
Processes	Process in privileged path	Privileged Process
CleanUp	Deleting files in privileged locations	Privileged Process

Additional Requirements

1. As little device wide changes as possible
2. Easy Interface
3. Running repeated consistent simulations
4. Allowing for flexible extensions
5. Supporting the latest iOS Version 🙏

Jailbreak ll Privilege Escalation ll Corellium

Palera1n

Pro

1. Support iOS 18
2. Running Privileged Processes
3. Easy Install and Shell Environment
4. Hooking Frameworks

Cons

1. Only iPad 7
2. Disabled Security Mitigations
3. Many Device Wide Changes
4. Only arm64

TrollStore



Pro

1. No device wide changes
2. Running Privileged Processes
3. Based on CVE-2023-41991
4. Supports arm64e
5. Intact Security Mitigations

Cons

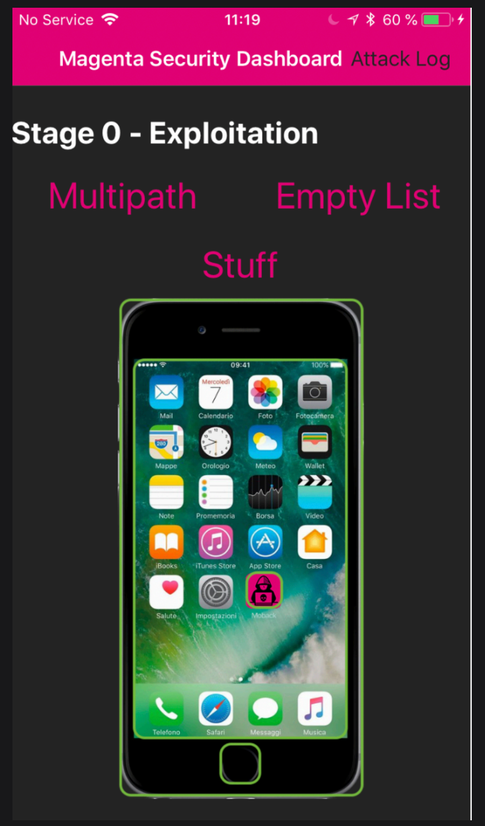
1. Only 17.0, <16.7
2. Limited Hooking

*🙌 @opa334, @alfiecg_dev and others - https://github.com/opa334/TrollStore

Previous Work / Inspiration

Master Thesis: iOS Operating System Exploit Detection (2019)

1. Used a public exploit for tfp0*
2. Used QiLin** for privilege escalation
3. Supported iOS 11 - 12.1.2
4. Terrible Code Quality and outdated



*🙌 Jonathan Levin - https://newosxbook.com/QiLin/

** 🙌 Ian Beer + Brandon Azad

Previous Work / Inspiration

Patricks Talk on “Making oRAT … Go!” (OBTS v6)

1. Build a custom backend
2. Simulated the backend API Handler to dynamically analyze oRAT

*🙌 Patrick Wardle - https://speakerdeck.com/patrickwardle/making-orat-go?slide=6

Previous Work / Inspiration



SeaShell

1. Uses TrollStore
2. No commit since September 2024 :/
3. Python based, includes implant
4. Extensible and remote access

🙌 https://github.com/EntySec/SeaShell



Custom App it is!

Implementation



Malware Simulator

1. Uses TrollStore
2. App to run simulations
3. Privileged Helper for anything that needs root
4. Reduced Entitlements from Predator Sample

https://iverify.io/blog/trust-broken-at-the-core

Compilation



Malware Simulator

1. Build Privileged Helper
2. Include Helper in App Bundle, add to TSRootBinaries, Archive
3. Export, Unpack, Use ldid for fake signing with Entitlements, Pack to .tipa
4. AirDrop to device with TrollStore
5. Profit

Supported Simulations



Pegasus 2021

1. File IOCs
2. Process Name

Predator 2022

1. File IOCs
2. Process Name

Supported Simulations



Pegasus 2023

1. HomeKit Crashes
2. MessagesBlastDoor Service Crashes
3. Stage 2: /p/v/db/com.apple.xpc.roleaccountd.staging/…
4. Use Stage 2 Process to clean-up Crashes

Supported Simulations



Random Simulations

1. Spawn Processes (ProcessBadA, ProcessMadB, ProcessTadC, …)
2. Drop Files to /private/var/tmp/process_name*
3. Delete Files
4. Run network calls to domain + domain/process_name
5. Crash Process at end

Results for “ProcessBadA”



Sysdiagnose after a run

```
matthiasfrielingsdorf@MatthiasMBPro4 Crashes % grep -l -i -r "ProcessBadA" .
./stacks-2025-10-15-163134.900.ips
./ProcessBadA-2025-10-15-155054.ips
./stacks-2025-10-15-163134.ips
./stacks-2025-10-15-163135.ips
./Analytics-Never-2025-10-16-020802.0005.ips.ca
./ProcessBadA-2025-10-15-160656.ips
./ProcessBadA-2025-10-15-163216.ips
./Analytics-Daily-2025-10-16-020802.0004.ips.ca
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Signpost/000000000000007a.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/35/F5163BA86B36888957109C0CDC49AA
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/3C/6FF40D2BB735F09793A85F8959D7EA
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/C1/16FB24DCB63E1EBD20B2D1B7364650
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/7B/AD6F957013344EA5DB8F9FBC76E938
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/01/1C3672DF413355A4E2AAE05C941054
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Persist/0000000000000b92.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Persist/0000000000000b91.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_14-30-28+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/7A/1F1E380035376AA8334B3C781882F9
```

Results for “ProcessBadA”



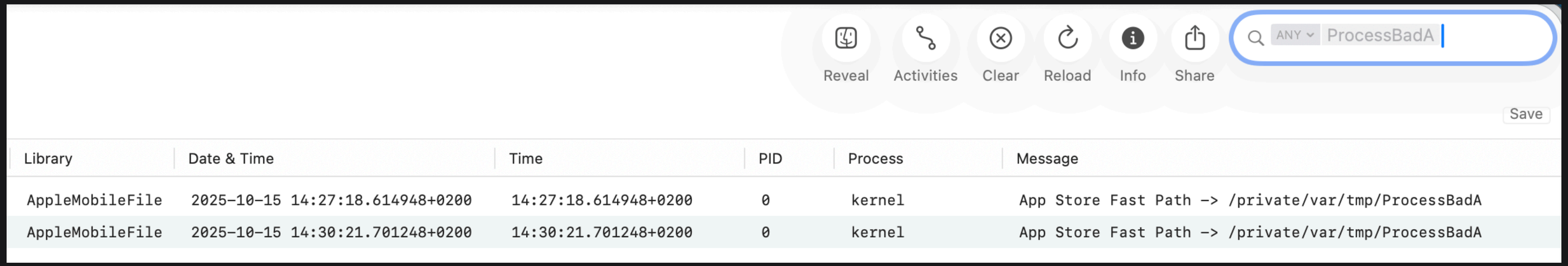
Sysdiagnose during a run

```
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/spindump-nosymbols.txt
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/taskinfo.txt
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/logs/powerlogs/powerlog_2025-10-15_16-32_5F141D97.PLSQL
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/summaries/crashes_and_spins.log
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/summaries/diagnostic_summary.log
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/ps.txt
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/ps_thread.txt
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/0D/887F0BA7C0316C851FB8F2417098D8
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Signpost/000000000000007a.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/35/F5163BA86B36888957109C0CDC49AA
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/3C/6FF40D2BB735F09793A85F8959D7EA
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/FC/80149715E334548A1D013A8F317B1E
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/C1/16FB24DCB63E1EBD20B2D1B7364650
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/7B/AD6F957013344EA5DB8F9FBC76E938
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/logdata.LiveData.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/01/1C3672DF413355A4E2AAE05C941054
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Persist/0000000000000b94.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Persist/0000000000000b95.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Persist/0000000000000b93.tracev3
./DiagnosticLogs/sysdiagnose/sysdiagnose_2025.10.15_16-31-34+0200_iPhone-OS_iPhone_19A348/system_logs.logarchive/Persist/0000000000000b92.tracev3
```

Results for “ProcessBadA”



Unified Logs



Library	Date & Time	Time	PID	Process	Message
AppleMobileFile	2025-10-15 14:27:18.614948+0200	14:27:18.614948+0200	0	kernel	App Store Fast Path -> /private/var/tmp/ProcessBadA
AppleMobileFile	2025-10-15 14:30:21.701248+0200	14:30:21.701248+0200	0	kernel	App Store Fast Path -> /private/var/tmp/ProcessBadA

Results for “ProcessBadA”



osanalyticsaddaily.plist

f65b5fafc69bbd3c60be019c6e938e146825fa83 — f6

```
1  // !!! BINARY PROPERTY LIST WARNING !!!
2  //
3  // The pretty-printed property list below has been created
4  // from a binary version on disk and should not be saved as
5  // the ASCII format is a subset of the binary representation!
6  //
7  {   netUsageBaseline = {
8          ACCFeatureAudioProductService = ( @2023-08-09 15:55:29 +0200, 367161, 117986, 16243, 4533 );
9          AppStoreService = ( @2023-08-09 17:34:40 +0200, 414358, 77449, 132936, 27504 );
10         AssetCacheLocato = ( @2023-08-16 17:13:06 +0200, 1509627, 601120, 677, 370 );
11         AssetCacheLocatorService = ( @2023-08-09 15:29:01 +0200, 1651964, 638835, 0, 0 );
12         CallHistorySyncHelper = ( @2023-08-09 15:28:55 +0200, 115783, 18267, 0, 0 );
13         CategoriesService = ( @2023-09-21 14:59:02 +0200, 111431, 22223, 15520, 4249 );
14         CommCenter = ( @2023-08-09 15:28:55 +0200, 3209887, 163970, 38889582, 5648745 );
15         CommCenterMobileHelper = ( @2023-08-09 15:28:55 +0200, 277067545, 4710551, 1419349, 50083 );
16         DTServiceHub = ( @2023-08-10 14:09:02 +0200, 8720961, 13131524, 0, 0 );
17         EnforcementService = ( @2023-09-04 14:08:55 +0200, 16104, 5379, 24004, 8238 );
18         IMTransferAgent = ( @2023-10-27 15:09:43 +0200, 261556, 43297, 8010, 1558 );
19         OTACrashCopier = ( @2024-11-06 16:42:32 +0100, 197318, 85201, 0, 0 );
20         ProcessBadA = ( @2025-10-15 15:50:54 +0200, 182984, 48214, 0, 0 );
21         StatusKitAgent = ( @2023-08-09 15:28:55 +0200, 387904, 58559, 0, 0 );
```

Results for “Pegasus 2021”



Shutdown.log

```
After 0.87s, these clients are still here:
        remaining client pid: 584 (/private/var/db/com.apple.xpc.roleaccountd.staging/rlaccountd/1B678799-D232-3A3E-8B1F-6A950D3C592C)
        remaining client pid: 583 (/private/var/containers/Bundle/Application/DA3595B6-3C09-4986-A85D-39367324DD27/threat-simulator.app/mosim_helper/1
        remaining client pid: 477 (/usr/libexec/afcd/FC233EAC-A31E-3868-AA25-9D7B0E457072)
        remaining client pid: 438 (/System/Library/PrivateFrameworks/HealthPluginHost.framework/healthappd/69C9327C-5E8B-35EC-8034-608CCD6BAA9E)
        remaining client pid: 376 (/usr/libexec/heartbeatd/C5A4AAE8-B5BD-309C-9AAF-14382D02A525)
        remaining client pid: 368 (/usr/libexec/duetexpertd/5AA86ADE-7FA8-3716-AAED-C0844FC8D483)
        remaining client pid: 241 (/System/Library/PrivateFrameworks/MapsSupport.framework/mapspushd/80410380-C70B-379D-A208-379A35CD2A1C)
        remaining client pid: 94 (/System/Library/Frameworks/CoreTelephony.framework/Support/CommCenter/6D8DBACC-4AC7-3773-819B-35A4DC6BB629)
        remaining client pid: 49 (/usr/libexec/remoted/F0E57647-3CF1-3FFD-99AA-16CA10D1B6F8)
        remaining client pid: 0 (/kernel/B0841348-0448-39A5-BA2B-F99C7CC3D28A)
After 0.87s, these clients are still here:
        remaining client pid: 0 (/kernel/B0841348-0448-39A5-BA2B-F99C7CC3D28A)
```

Implemented Simulations

Infiltration		Min. Requires
Crashes	(Repeatedly) Crashing a process	App or Extension
Logs	Creating Unified Logs entries	App
Files	iMessage Attachments	Privileged Process or Mac*
Network	Domain and IP Connections	App

Implemented Simulations

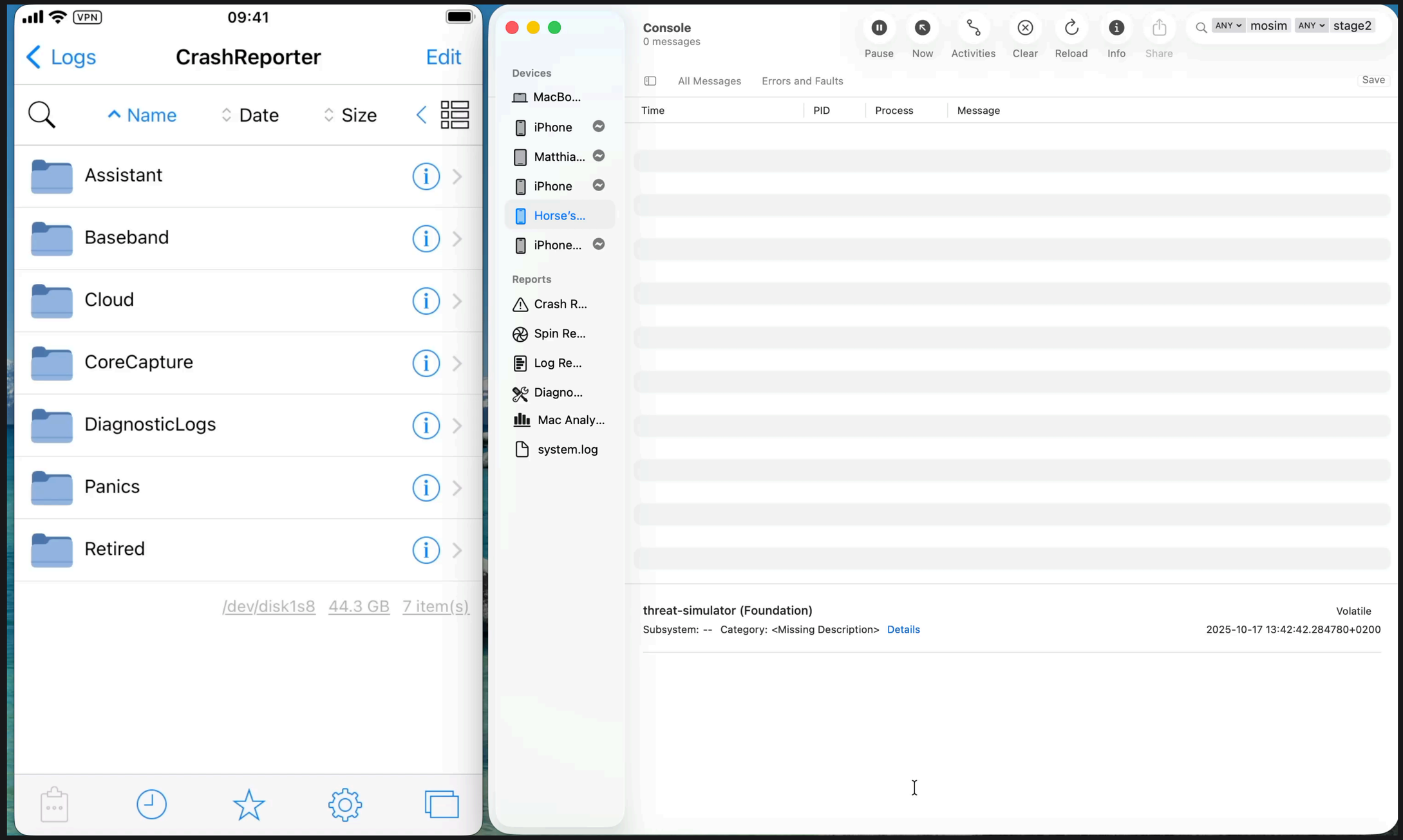
	Code Execution	Min. Requires
Crashes	Panic the Kernel	Vulnerability
Logs	Creating Unified Logs entries	App
Files	/private/var/tmp*	Privileged Process
Networks	Domain and IP Connections	App
Processes	Process in privileged path	Privileged Process
CleanUp	Deleting files in privileged locations	Privileged Process

Today

1. iOS Malware Overview & Detailed Behavior
2. iOS Malware Simulation
3. Demo

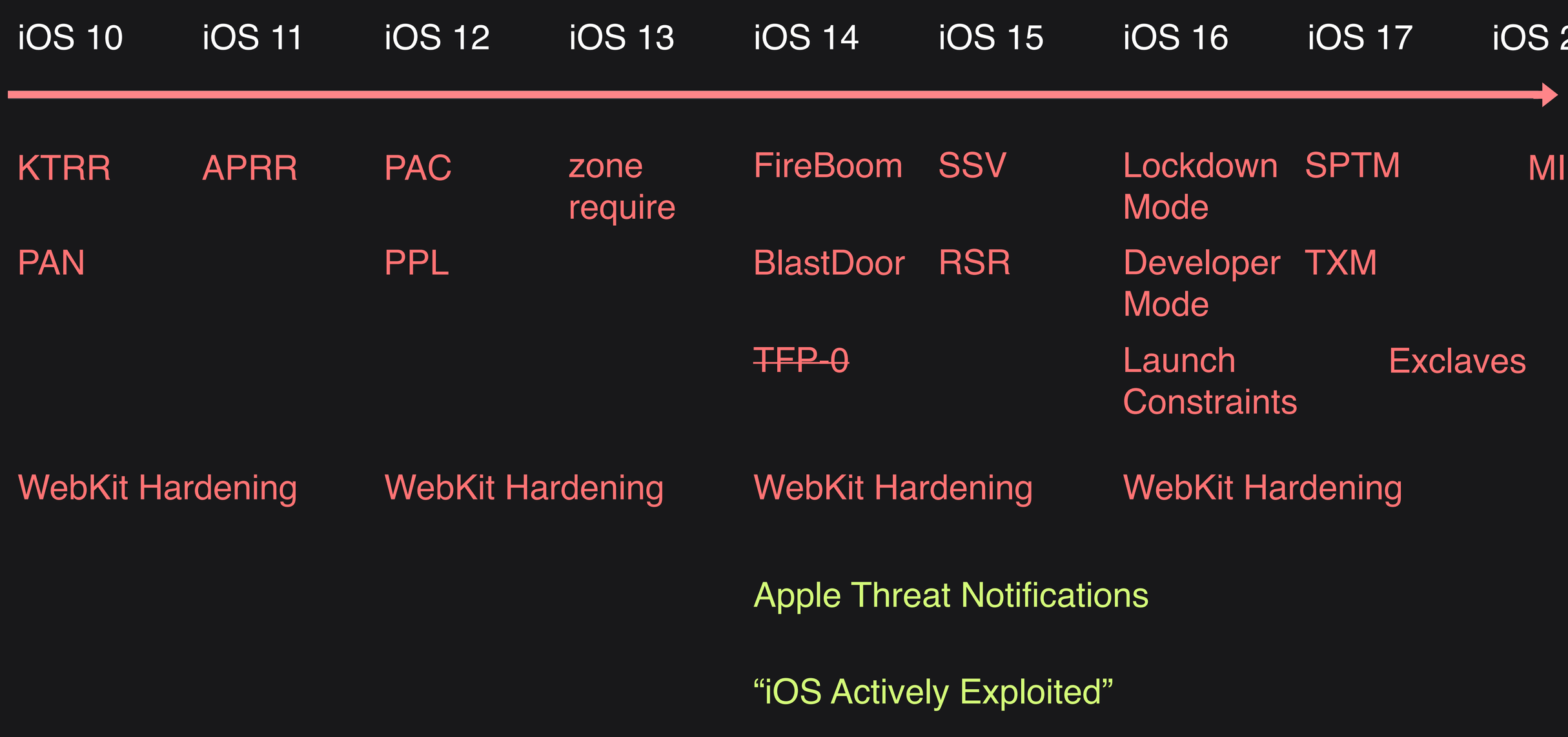


Demo Time!


09:41
Logs
CrashReporter
Edit
Name
Date
Size
Assistant
Baseband
Cloud
CoreCapture
DiagnosticLogs
Panics
Retired
/dev/disk1s8 44.3 GB 7 item(s)
Console
0 messages
Pause
Now
Activities
Clear
Reload
Info
Share
ANY mosim ANY stage2
All Messages
Errors and Faults
Save
Devices
MacBo...
iPhone
Matthia...
iPhone
Horse's...
iPhone...
Reports
Crash R...
Spin Re...
Log Re...
Diagno...
Mac Analy...
system.log
Time
PID
Process
Message
threat-simulator (Foundation)
Volatile
Subsystem: -- Category: <Missing Description> Details
2025-10-17 13:42:42.284780+0200

iOS Mitigation and Detections - 2025

Prevention
Notification
Detection



State of Malware Detection - 2024

Apple	Companies & Individuals	Defensive Community
(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	Security Hygiene	Exchange & Knowledge Transfer

State of Malware Detection - 2025

Apple	Companies & Individuals	Defensive Community
(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	Security Hygiene	Exchange & Knowledge Transfer



SRD for Malware Analysis???

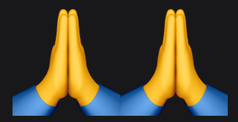


🙏



Endpoint Security Framework for iOS





One more thing…

What if…



We use the simulator to build our own ESF?



Demo Time!


9:41
Threat Viewer
MalwareSimula...

Infiltration

Implant

iOS Commercial Spyware Behavior

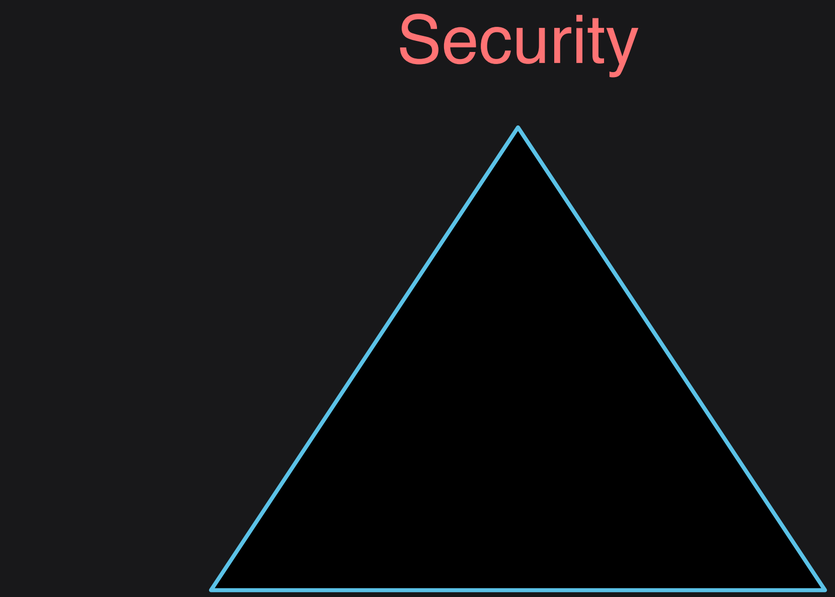
	Pegasus		Predator		Operation T	NoClip	Graphite
	2021	2023	2021	2023	2023	2023	2025
Crashes	✓	✓	✓	✓	✓	✓	✓
Emails	✓	✓			✓		✓
Files	✓	✓			✓		
URL			✓		✓	✓	
Process	✓	✓	✓	✓	✓	?	?
Files	✓	?	✓	✓	✓	✓	?
Network	✓	?	✓	✓	✓	✓	✓
Clean-Up	✓	✓	✓	✓	✓	✓	?

Flag with basic ESF
Detection with ESF
Flag w/o ESF

iOS Commercial Spyware Behavior

	Pegasus		Predator		Operation T	NoClip	Graphite
	2021	2023	2021	2023	2023	2023	2025
Crashes	✓	✓	✓	✓	✓	✓	✓
Emails	✓	✓			✓		✓
Files	✓	✓			✓		
URL			✓		✓	✓	
Process	✓	✓	✓	✓	✓	?	?
Files	✓	?	✓	✓	✓	✓	?
Network	✓	?	✓	✓	✓	✓	✓
Clean-Up	✓	✓	✓	✓	✓	✓	?

Security vs Privacy vs Visibility



This is delicate balance that Apple needs to find.