MEFF M3 PRO – iOS GERÄTESICHERHEITS-SCAN

Pegasus- & Regierungs-Spyware-Erkennung

Berichtsdatum: 11/12/2025 09:47

Scan-Typ: iOS-Gerät (iPhone/iPad)

Analysiert mit: KI (GPT-4o) + Security-Datenbank

Fokus: Installierte Apps, Berechtigungen, Regierungs-Spyware (Pegasus, Predator, FinFisher)

ALLGEMEINE STATISTIK

Kennzahl	Wert	Status
Insgesamt analysierte Apps	31	■
High-Risk-Apps	0	■
Apps mit mittlerem Risiko	1	■
Apps mit geringem Risiko	30	■
Regierungs-Spyware	0	■
Malware erkannt	0	■
Verdächtige Apps	1	■■

ERKANNTE VERDÄCHTIGE DOMAINS/APPS

■ ACHTUNG: Es wurde 1 verdächtiges Element erkannt!

Die folgende Liste enthält Domains, IPs oder Anwendungen mit Risikomerkmalen. Die Elemente sind nach Schweregrad klassifiziert: KRITISCH, HOCH, MITTEL.

Element	Typ	Schweregrad	Beschreibung
Appstate	App verdächtig	■ **HOCH**	Verdächtige Aktivität erkannt

VERTIEFTE KI-ANALYSE

■ VOLLSTÄNDIGE LISTE ANALYSIERTER APPS

1. iOS System Analysis — ■ GERINGES RISIKO
   Paket: ios.system.analysis | Version: N/A
   Batterienutzung: 0.0%
   ■ Befunde:
   • I Gerät: iPhone17,1
   • I iOS-Version: Unbekannt
   • I Analysierte Dateien: 50

2. Service — ■ GERINGES RISIKO
   Paket: com.apple.Safari.SafeBrowsing.Service | Version: N/A
   Batterienutzung: 0.0%
   ■ Befunde:
   • I Name: Service
   • I Bundle-ID: com.apple.Safari.SafeBrowsing.Service

3. Imageconversionservice — ■ GERINGES RISIKO
   Paket: com.apple.photos.ImageConversionService | Version: N/A
   Batterienutzung: 0.0%
   ■ Befunde:
   • I Name: Imageconversionservice
   • I Bundle-ID: com.apple.photos.ImageConversionService

4. Appstate — ■ MITTLERES RISIKO
   Paket: com.meta.apple.diagostics.logger.appstate | Version: N/A
   Batterienutzung: 0.0%
   ■ Befunde:
   • I Name: Appstate
   • I Bundle-ID: com.meta.apple.diagostics.logger.appstate
   • II Name oder Bundle-ID enthält auffälligen Begriff: 'logger'

5. Shazam — ■ GERINGES RISIKO
   Paket: com.shazam.Shazam | Version: N/A
   Batterienutzung: 0.0%
   ■ Befunde:
   • I Name: Shazam
   • I Bundle-ID: com.shazam.Shazam

■ VOLLSTÄNDIGE LISTE ANALYSIERTER APPS

6. 2 ■ GERINGES RISIKO
Paket: io.worker.2 | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: 2
• I Bundle-ID: io.worker.2

7. Sourcing ■ GERINGES RISIKO
Paket: com.alibaba.sourcing | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Sourcing
• I Bundle-ID: com.alibaba.sourcing

8. Notificationserviceextension ■ GERINGES RISIKO
Paket: com.google.Gmail.NotificationServiceExtension | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Notificationserviceextension
• I Bundle-ID: com.google.Gmail.NotificationServiceExtension
• II Typ: Email

9. Ui ■ GERINGES RISIKO
Paket: io.flutter.1.ui | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Ui
• I Bundle-ID: io.flutter.1.ui

10. Iphoneapp ■ GERINGES RISIKO
Paket: com.internet.unicredit.iphoneapp | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Iphoneapp
• I Bundle-ID: com.internet.unicredit.iphoneapp

■ VOLLSTÄNDIGE LISTE ANALYSIERTER APPS

11. Googlemobile ■ GERINGES RISIKO
Paket: com.google.GoogleMobile | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Googlemobile
• I Bundle-ID: com.google.GoogleMobile

12. Notificationextension ■ GERINGES RISIKO
Paket: com.google.GoogleMobile.NotificationExtension | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Notificationextension
• I Bundle-ID: com.google.GoogleMobile.NotificationExtension

13. Messenger ■ GERINGES RISIKO
Paket: com.facebook.Messenger | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Messenger
• I Bundle-ID: com.facebook.Messenger
• II Typ: Social Media

14. TikTok ■ GERINGES RISIKO
Paket: com.zhiliaoapp.musically | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: TikTok
• I Bundle-ID: com.zhiliaoapp.musically
• II Typ: Social Media

15. Wetterapp ■ GERINGES RISIKO
Paket: de.wetteronline.WetterApp | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Wetterapp
• I Bundle-ID: de.wetteronline.WetterApp

■ VOLLSTÄNDIGE LISTE ANALYSIERTER APPS

16. Notificationextension ■ GERINGES RISIKO
Paket: com.burbn.instagram.notificationextension | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Notificationextension
• I Bundle-ID: com.burbn.instagram.notificationextension
• II Typ: Social Media

17. Ppclient ■ GERINGES RISIKO
Paket: com.yourcompany.PPClient | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Ppclient
• I Bundle-ID: com.yourcompany.PPClient

18. Serviceextension ■ GERINGES RISIKO
Paket: net.whatsapp.WhatsAppSMB.ServiceExtension | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Serviceextension
• I Bundle-ID: net.whatsapp.WhatsAppSMB.ServiceExtension
• II Typ: Messaging

19. WhatsApp ■ GERINGES RISIKO
Paket: net.whatsapp.WhatsApp | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: WhatsApp
• I Bundle-ID: net.whatsapp.WhatsApp
• II Typ: Messaging

20. Io ■ GERINGES RISIKO
Paket: io.flutter.1.io | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Io
• I Bundle-ID: io.flutter.1.io

■ VOLLSTÄNDIGE LISTE ANALYSIERTER APPS

21. Listener ■ GERINGES RISIKO
Paket: com.hmd.crash.listener | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Listener
• I Bundle-ID: com.hmd.crash.listener

22. Temu ■ GERINGES RISIKO
Paket: com.einnovation.temu | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Temu
• I Bundle-ID: com.einnovation.temu

23. Teams ■ GERINGES RISIKO
Paket: com.microsoft.skype.teams | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Teams
• I Bundle-ID: com.microsoft.skype.teams

24. Easy4Ip ■ GERINGES RISIKO
Paket: com.dahuaoversea.easy4ip | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Easy4Ip
• I Bundle-ID: com.dahuaoversea.easy4ip

25. Mediaservervolumecontroller ■ GERINGES RISIKO
Paket: conm.apple.mediaRemote.mediaServerVolumeController | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Mediaservervolumecontroller
• I Bundle-ID: conm.apple.mediaRemote.mediaServerVolumeController

■ VOLLSTÄNDIGE LISTE ANALYSIERTER APPS

26. 1 ■ GERINGES RISIKO
Paket: io.worker.1 | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: 1
• I Bundle-ID: io.worker.1

27. Silentphone ■ GERINGES RISIKO
Paket: com.silentcircle.SilentPhone | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Silentphone
• I Bundle-ID: com.silentcircle.SilentPhone

28. Thread ■ GERINGES RISIKO
Paket: com.meta.location.thread | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Thread
• I Bundle-ID: com.meta.location.thread

29. Shared ■ GERINGES RISIKO
Paket: caulk.messenger.shared | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Shared
• I Bundle-ID: caulk.messenger.shared

30. Partybox ■ GERINGES RISIKO
Paket: com.jbl.partybox | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Partybox
• I Bundle-ID: com.jbl.partybox

31. Instagram ■ GERINGES RISIKO
Paket: com.burbn.instagram | Version: N/A
Batterienutzung: 0.0%
■ Befunde:
• I Name: Instagram
• I Bundle-ID: com.burbn.instagram
• II Typ: Social Media

VOLLSTÄNDIGE CHECKLISTE: REGIERUNGS-SPYWARE & GEFÄHRLICHE APPS

Diese Checkliste enthält ALLE bekannten staatlichen Überwachungssysteme und gefährlichen Apps.

Das System hat geprüft, ob diese Elemente auf dem gescannten Gerät vorhanden sind. Nicht vorhandene Elemente werden mit □ markiert, erkannte Elemente (falls vorhanden) mit ■.

■ REGIERUNGS-SPYWARE

Status	Name (Spyware)	Hersteller	Beschreibung
■	Pegasus	NSO Group (Israele)	Die fortschrittlichste Spyware, eingesetzt für zielgerichtete Überwachungsoperationen (u. a. Zero-Click-Exploits)...
■	Predator	Cytrox/Intellexa (Nord Ma	Regierungs-Spyware, verkauft an europäische und nahöstliche Regierungen...
■	FinFisher (FinSpy)	Gamma Group (Germania/UK)	Kommerzieller Trojaner, eingesetzt von Polizei und Regierungsbehörden...
■	Candiru	Saito Tech (Israele)	Zero-Click-Spyware, verkauft an Regierungen, öffentlich bekannt durch Recherchen von Sicherheitsforschern...
■	Hacking Team RCS	Hacking Team (Italia)	Remote-Control-System, genutzt für staatliche Überwachung (u. a. durch Leaks bekannt)...
■	Stealth Falcon	DarkMatter (UAE)	Gezielte Spionagekampagne gegen Aktivisten in verschiedenen Ländern (öffentlich dokumentiert)...
■	Circles	NSO Group / Nice Systems	Telefon-Ortungssystem über SS7, verkauft an Regierungen/Behörden...
■	Verint	Verint Systems (USA/Israe	Plattform zur Kommunikationsüberwachung für Sicherheitsbehörden...
■	Quadream	QuaDream (Israele)	Mobile Spyware ähnlich Pegasus, verkauft an Regierungen...
■	Hermit	RCS Lab (Italia)	Mobile Spyware, in mehreren Ländern eingesetzt (öffentlich dokumentierte Fälle)...
■	Exodus	eSurv (Italia)	Italienische Spyware für Ermittlungen, z. B. installiert über manipulierte/Fake-Apps...
■	GrayKey	Grayshift (USA)	iPhone-Entsperr-Tool, genutzt von FBI und Strafverfolgungsbehörden...
■	Cellebrite UFED	Cellebrite (Israele)	Forensik-Suite zur Datenextraktion von Smartphones...
■	Pegasus Android	NSO Group	Android-Variante von Pegasus mit Zero-Day-Exploits...
■	Pegasus iOS	NSO Group	iOS-Variante von Pegasus mit Zero-Click-Exploits (z. B. iMessage/Safari)...

■■ GEFÄHRLICHE APPS & BEKANNTE MALWARE

Status	Name (App/Malware)	Kategorie	Beschreibung
■	FlexiSpy	Stalkerware	Kommerzielle Spionage-App zur Überwachung von Anrufen, Nachrichten und weiteren Daten...
■	mSpy	Stalkerware	Überwachungssoftware, oft als „Kindersicherung“ vermarktet...
■	Spyera	Stalkerware	Kommerzielle Spyware mit erweiterten Abhör-/Überwachungsfunktionen...
■	TeenSafe	Stalkerware	Monitoring-App als „Elternkontrolle“ (erhebliche Privatsphäre-/Datenschutzrisiken)...
■	Cerberus	Banking-Trojaner	Android-Trojaner, der Banking-Zugangsdaten und SMS abgreift...
■	Anubis	Banking-Trojaner	Android-Malware, die Banking-Apps und Krypto-Wallets angreift...
■	Ginp	Banking-Trojaner	SMS-Trojaner, der 2FA-Codes von Banking-Apps abfängt...
■	Gustuff	Banking-Trojaner	Banking-Trojaner mit über 100 Banking-Apps als Ziel...
■	EventBot	Infostealer	Android-Trojaner, der SMS, Kontakte und Finanzdaten stiehlt...
■	Agent Smith	Schad-Adware	Malware, die legitime Apps durch infizierte Versionen ersetzt...
■	Joker	SMS-Trojaner	Malware, die Premium-Dienste ohne Zustimmung abonniert...
■	Hiddad	Adware	Aggressive Adware, versteckt in scheinbar legitimen Apps...
■	DroidDream	Rootkit	Malware, die Root-Zugriff erlangt und Backdoors installiert...
■	GhostCtrl	RAT	Remote-Access-Trojaner, der das Gerät vollständig fernsteuert...
■	Dendroid	RAT	Android-RAT, angeboten in Underground-Foren zur Fernsteuerung...
■	OmniRAT	RAT	Remote-Administration-Tool mit erweiterten Spyware-Funktionen...
■	SpyNote	RAT	Tool/Builder zur Erstellung von Android-RATs, angeboten im Darknet...
■	DroidJack	RAT	Android-RAT mit grafischer Oberfläche für Angreifer...
■	AhMyth	RAT	Open-Source-RAT zur Fernsteuerung von Android-Geräten...
■	FakeApp Bancarie	Phishing	Fake-Apps, die Banken imitieren, um Zugangsdaten zu stehlen...

Status	Name (App/Malware)	Kategorie	Beschreibung
■	WhatsApp Fake	Trojaner	WhatsApp-Klon mit integrierter Malware...
■	Telegram Fake	Trojaner	Modifizierte Telegram-Version mit Spyware...
■	TikTok Pro Fake	Adware	Fake-App, die Premium-Funktionen verspricht, aber Adware installiert...
■	Instagram++ Fake	Malware	Instagram-Mod mit versteckter Malware...
■	Android.Xloader	Backdoor	Backdoor, die zusätzliche Schad-Payloads nachlädt...

■ HINWEISE ZUR CHECKLISTE:

• Dies ist eine vollständige und aktualisierte Liste aller bekannten Regierungs-Spyware-Systeme und gefährlichen Apps.
• Ein leeres Kontrollkästchen (□) bedeutet: Element wurde nicht erkannt.
• Ein gefülltes Kontrollkästchen (■) bedeutet: mögliche Erkennung – sofortige manuelle Verifikation erforderlich.
• Bereits ein erkanntes Element kann dringende Sicherheitsmaßnahmen erforderlich machen.
• Die Liste basiert auf öffentlich dokumentierten Recherchen u. a. von Citizen Lab, Amnesty Tech, Kaspersky, ESET und Lookout Security.

■ MVT-ZERTIFIZIERUNG (Mobile Verification Toolkit)

Dieser Bericht wurde mit Analysetechniken erstellt, die den Standards von MVT (Mobile Verification Toolkit) entsprechen – dem gleichen Tool-Ansatz, den u. a. Amnesty International zur Erkennung von Spyware wie Pegasus nutzt. Das System integriert aktualisierte Threat-Intelligence-Datenbanken sowie fortgeschrittene KI-Analyse, um eine hohe Genauigkeit in der Bedrohungserkennung zu unterstützen.

Bericht automatisch generiert durch MEFF M3 Pro – AI Traffic Analyzer

Support: support@meff-security.com