Mobile Device Security Analysis Report

Device Type: iOS
Target Path: /Users/simcoehall/Desktop/Merec
MVT Version: 2.6.1
Analysis Date: 2025-06-17 11:24:23.471457
IOC Files Used: 10
Total Data Sources: 21
Report Generated: 2025-06-17 11:44:43

Executive Summary

SECURITY ALERT: This forensic analysis has identified **1** potential security issues that require immediate attention. These findings indicate possible indicators of compromise (IOCs) or suspicious activities on the device.

This Mobile Verification Toolkit (MVT) analysis examined **21** different data sources from the iOS device, including 7 applications, 844 network processes, system logs, browser history, privacy permissions, location tracking data, and messaging records. Data sources analyzed: netusage, os_analytics_ad_daily, datausage, global_preferences, tcc, id_status_cache, cache_files, shortcuts and 13 others.

Key Analysis Areas:

- Applications: 7 analyzed
- SMS Messages: 70 examined
- Network Activity: Process-level traffic analysis

Device Information

Property	Value
Scan Target Path	/Users/simcoehall/Desktop/Merec
MVT Version	2.6.1
Analysis Date	2025-06-17 11:24:23.471457
IOC Files Used	10
Hash Files Used	0
Total Apps (Detailed)	7
App Store Apps	7
Sideloaded Apps	0
Network Processes	844
Total Data Sent (bytes)	1,753,171,682

Filesystem Entries	476727
Privacy Permissions	42
Location Clients	83
Browser Tracking Domains	22
Report Generated	2025-06-17 11:44:43
Device Type	iOS
Total Data Sources	21

Security Findings

■ 1 potential security issues detected:

Unknown Issues (1):

• [Unknown time] IOC: {'value': 'payload', 'type': 'processes', 'name': 'Pegasus', 'stix2_file_name': 'raw.githubusercontent.com_AmnestyTech_investigations_master_2021-07-18_nso_pegasus.stix2'}

Installed Applications Analysis

Total Applications Found: **7**
App Store Applications: **7**
Sideloaded Applications: **0**
Most Common Category: **Travel**

Application Categories:

• Travel: 2 apps
• Utilities: 1 apps
• Business: 1 apps
• Photo & Video: 1 apps
• Shopping: 1 apps
• Navigation: 1 apps

High-Risk Applications (Finance/Business/Medical):

• Duo Mobile (Business) - v4.86.0

Privacy & Permissions Analysis

Camera Access:

Third-party applications with access:
• DuoMobile

Motion & Fitness:

System applications: 1 apps

TCC Database Summary:

Total Permission Entries: **42**
Unique Services: **7**
Sensitive Permissions Found: **2**

Location Tracking Analysis

Applications with Location Access: **0**

Browser Security Analysis

WebKit Tracking Data: **22** domains

Network Activity Analysis

Total processes with network activity: **257**
Total data sent: **1,019,245,184** bytes (972.0 MB)
Total data received: **11,498,521,271** bytes (10965.0 MB)
Processes without valid bundle ID: **169**

Top Network Data Consumers:

• mobilesafari (com.apple.mobilesafari) - Total: 4152.9 MB (Sent: 522.3 MB, Received: 3630.6 MB)
• com.apple.nsurlsessiond - Total: 3341.6 MB (Sent: 12.4 MB, Received: 3329.1 MB)
• AppStore (com.apple.AppStore) - Total: 627.6 MB (Sent: 4.5 MB, Received: 623.1 MB)
• com.apple.mobileassetd.client.auto-asset-client - Total: 565.5 MB (Sent: 12.2 MB, Received: 553.3 MB)
• news (com.apple.news.widgetintents) - Total: 544.6 MB (Sent: 10.0 MB, Received: 534.6 MB)
• AppStore (com.apple.AppStore) - Total: 488.3 MB (Sent: 2.0 MB, Received: 486.3 MB)
• AppStore (com.apple.AppStore) - Total: 408.5 MB (Sent: 2.1 MB, Received: 406.3 MB)
• ios (com.google.chrome.ios) - Total: 315.5 MB (Sent: 20.7 MB, Received: 294.8 MB)
• weather (com.apple.weather.WeatherAppIntents) - Total: 180.7 MB (Sent: 3.0 MB, Received: 177.7 MB)
• com.apple.mobileassetd - Total: 133.6 MB (Sent: 6.2 MB, Received: 127.4 MB)

■ Processes without valid bundle IDs detected. These may require investigation:

• mDNSResponder - Sent: 17,849,803 bytes, Received: 19,872,439 bytes
• MISSING [follows com.apple.purplebuddy] - Sent: 0 bytes, Received: 0 bytes
• com.apple.CommCenterMobileHelper - Sent: 864,074 bytes, Received: 16,634,287 bytes
• com.apple.CommCenter - Sent: 203,690 bytes, Received: 547,344 bytes
• timed - Sent: 182,152 bytes, Received: 454,612 bytes

Messaging & Communications Analysis

SMS Messages: **70**
Call Records: **14**
Incoming calls: 0, Outgoing calls: 0
Contacts: **46**

Timeline Analysis

No significant timeline events to display.

Recommendations

[IMMEDIATE] Investigate all detected security issues flagged in this report
[IMMEDIATE] Consider isolating the device from networks until issues are resolved
[HIGH] Perform a full factory reset if compromise is confirmed
[HIGH] Change all passwords and revoke authentication tokens for accounts used on this device
[MEDIUM] Keep the device operating system updated to the latest version
[MEDIUM] Only install applications from official app stores
[MEDIUM] Regularly review and remove unused applications
[MEDIUM] Enable automatic security updates where available
[MEDIUM] Use strong, unique passwords and enable two-factor authentication
[MEDIUM] Regularly backup important data to secure, offline storage

This report was generated by the Mobile Verification Toolkit (MVT) Dashboard. MVT is developed by Amnesty International for consensual forensic analysis. For questions about this report, contact your security team.