Threat advisory: Mobile spyware continues to evolve

By Jamf Threat Labs

Archived: 2026-04-05 14:09:02 UTC

Introduction

Jamf Threat Labs has been studying the ongoing use of sophisticated spyware, including indicators previously attributed to NSO Group's Pegasus, to target iPhones used by high-risk individuals. Over a period of six months, Jamf Threat Labs investigated multiple mobile devices belonging to different individuals and organizations that showed unique indicators of compromise (IOCs) and evidence of active spyware campaigns.

This advisory is intended to highlight the active use of spyware against workers in a variety of regions and to share research with the security community that can help with the ongoing monitoring of these exploits.

To protect the organizations and individuals that have been targeted, we have anonymized certain details, but that does not change the findings; all other findings remain intact for analysis.

Research led by Nir Avraham.

What we know

- Targeted spyware has been identified in attacks around the globe
    - Users in multiple regions have been impacted by spyware over the past six months
    - The instances have each involved individuals at high risk of targeted attacks
    - Each attack scenario has yielded unique indicators of compromise

    - Variations in the compromised hardware and software indicate that new exploits continue to be discovered as security patches are issued, expanding the population of vulnerable devices
- Apple is actively monitoring devices for compromise
    - Apple notified one of the compromised users working with Jamf Threat Labs and confirmed unusual activity on the device
    - Not all users impacted by spyware have been contacted by Apple, illustrating the challenges with maintaining a comprehensive list of IOCs and with extracting relevant data remotely
- High-risk individuals and organizations do not consistently execute full investigations as a result of threat indicators or user-reported issues
    - Some organizations pursue complete investigations in response to threat indicators to confirm attacks
    - Some organizations decide to wipe devices upon seeing initial IOCs without performing a full analysis on the device
    - Inconsistent investigations and data collection hinders timely and comprehensive research on emerging attacks

Verifying a mobile spyware infection

The first device we will examine is an iPhone 12 Pro Max that was used as the daily communications tool by a human rights activist based in the Middle East. We will subsequently refer to this as the Middle East iPhone.

A known IOC

Analysis from Jamf Threat Labs revealed traces of the “libtouchregd” process. According to Amnesty International, this process name is an IOC associated with the Pegasus spyware.

While another threat actor purposefully reusing the same process name for misattribution can never be entirely ruled out, it is unlikely in the case of the Middle East iPhone for the following reasons:

- Another threat actor would not want to name their processes the same name since this can lead to an unwanted discovery of an attack and destroy the exploit chain used in the attack.
- Jamf Threat Labs has determined that the attack on the device from the Middle East happened three months *before* the publication of Amnesty International’s IOCs. Therefore, the chances of a third party mimicking the process identified in the Amnesty report prior to publication is reduced significantly.

Therefore, our analysis strongly suggests that the same threat actor that was described by the Amnesty International blog is behind the attack on the Middle East iPhone.

Indicator of possible exploitation via crash log analysis

The Middle East iPhone also yielded additional indicators of compromise via subsequent analysis of the `com.apple.CrashReporter.plist` file.

The `com.apple.CrashReporter.plist` file is located within a root folder on iOS (/private/var/root/Library/Preferences/). This plist serves as a configuration file for the system daemon,

ReportCrash.

Under normal operating conditions, applications are not granted permission to access or modify this file. Alteration of this file could potentially impede the reporting of crash report logs to Apple. Additionally, the existence of the file is rare for normal users.

In rare cases that this file exists legitimately, it will keep state for urgentSubmission crash reports and have contents similar to the following example. This example illustrates that there have been 5 crash logs classified as urgentSubmission, with the last submitted on Thursday, March 9, 2023 (19425 days since Jan 1 1970).

The system daemon ReportCrash defines urgentSubmission. On Beta versions of iOS all crash logs are considered urgentSubmission. Otherwise, ReportCrash reserves its usage for the reporting of rare and critical events (see below).

Analysis of the ReportCrash daemon on iOS 16.2 leads us to believe that only crash logs that meet a strict set of criteria will be classified as urgentSubmission. These conditions include:

- Special types of reports, such as probGuard and quarantine.
- Undefined behavior detected by the UBSan, a tool utilized by LLVM to detect issues at runtime.
- A specific snapshot error code, as the snapshot mechanism is utilized to maintain the integrity of the file system.
- Various overflow alerts from the libsystem_c library.

Ultimately, Jamf Threat Labs treats the existence of these urgent submission reports as an indicator of exploitation requiring follow-on device analysis.

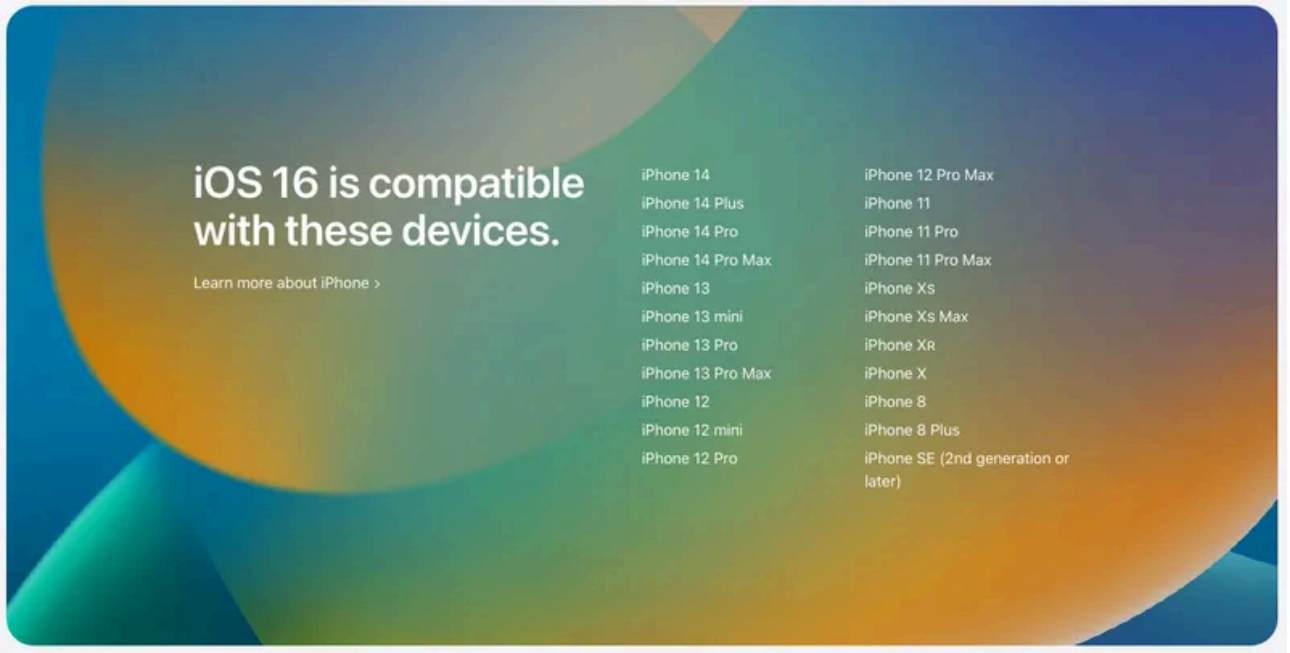
Official notification

In late 2022, the targeted user of the Middle East iPhone received a threat notification from Apple, notifying them of a potential attack and recommending that the device be updated to iOS 16.2. Following the update, the user engaged with security researchers to better understand the attack timeline and details.

Upon investigation, the Middle East iPhone proved to be a treasure trove for our analysis given the compounded set of compromise indicators and the clear association with Pegasus. These findings have allowed Jamf Threat Labs to build a more robust profile on a device with “proven” compromise status.

Analyzing spyware targeting older iPhones

The second device we will showcase is an iPhone used by a journalist in Europe working for a global news agency. We will subsequently refer to this as the Europe iPhone. It is noteworthy that this device was an iPhone 6s, a device that is no longer supported with the latest iOS version.



New IOC discovery via filesystem analysis

Like the Middle East iPhone, the Europe iPhone showed evidence of critical system crashes as indicated by the existence of a `com.apple.CrashReporter.plist` file discussed in detail above.

Even more suspiciously, the Europe iPhone included files found at an atypical location within iPhone's strict filesystem. Furthermore, at least one file at this location is clearly masquerading as a built-in binary: /private/var/containers/appconduitd_helper. Based on this path and filename, we have strong reason to believe this may be a new indicator that can be used to assess if a device has been targeted by this threat actor. We have also notified Apple of this potential new indicator.

While we have seen similar activities across other targeted devices, we cannot conclusively determine that the Europe iPhone was compromised by a specific threat actor. Based on previous infections by a threat actor that shares striking similarities, we estimate that the Europe iPhone was targeted using a commercial tool.

iPhone 6s and Unsupported Devices

The continued targeting of older devices, such as the iPhone 6s, serves as a reminder that malicious threat actors will exploit any vulnerabilities in an organization's infrastructure, attacking wherever possible.

Apple occasionally releases updates to prior iOS versions to back-port critical security fixes to older devices. iOS 15.7.5 was released on April 10, 2023, which is the latest iOS version available for iPhone 6s at the time this blog was published. It is important to note that not all vulnerabilities are addressed on prior iOS versions for legacy devices, and newer security mitigations may not be back-ported either. Additionally, these security patches often trail updates issued for current OS versions (iOS 15.7.5 contained security fixes that Apple patched three days earlier in iOS 16.4.1). As a result, threat actors can continue to exploit unpatched vulnerabilities that have been patched on newer supported devices, potentially giving attackers more time and more information to gain remote access to targeted devices.

As a general best practice, we strongly recommended upgrading outdated devices to newer iPhone or iPad models that are running the latest available updates and operating system versions.

Recommended actions

Modern spyware is very advanced and, as evidenced by the continued evolution of commercial spyware, continues to leverage zero-day vulnerabilities in both old and new devices to ensure any user can be effectively targeted.

Though the attacks through commercial spyware are expensive to operate, any individual or organization with mobile devices that are used to access sensitive data should take action to implement a layered set of defenses to insulate from attack.

Jamf Threat Labs recommends that organizations:

- Ensure all devices are running the most current operating system and have all available security patches applied.
- Keep all applications, both business oriented and personal, up-to-date and fully patched; mobile application vulnerabilities are easily exploited and frequently overlooked by security teams.
- Run security software to monitor for suspicious activity and report alongside all other endpoint monitoring dashboards, ensuring that mobile devices are treated with the same attention and urgency as desktops, laptops and servers.
- Monitor communications for suspicious downloads, command & control indicators and data exfiltration; utilize automated policy controls to block known bad activity before it can cause further damage.
- Educate high-risk users about the symptoms of spyware, which can include performance issues and frequent crashes. Encourage them to reach out to their security team if they observe any of these issues to maximize the extraction of IOCs from their device.
- Encourage high-risk users to use Lockdown Mode, which is designed to protect devices against extremely rare and highly sophisticated cyber attacks.
- Implement a security monitoring process that includes mobile telemetry analysis and stay up-to-date on known IOCs related to mobile spyware.

Learn more about how you can engage Jamf Threat Labs within your organization.
