Apple iPhone Spyware Attacks:

Understanding the Threat and How to Stay Safe

Office of Information Technology
Division of Information Security
DECEMBER 2025

In recent years, Apple iPhones, widely considered among the most secure consumer devices, have increasingly come under scrutiny due to sophisticated spyware attacks. These attacks, often targeting high-profile individuals, journalists, activists, and ordinary users alike, have raised significant concerns about privacy, surveillance, and digital security. While Apple continues to strengthen its defenses, spyware threats are evolving just as rapidly. Since the Indian Health Service (IHS) mostly uses Apple iPhones, this article explores the nature of iPhone spyware attacks, notable incidents, spyware malicious software that tracks work-related devices, and user options to protect themselves.

What is iPhone Spyware?

Spyware is malicious software designed to infiltrate a device and collect data without the user's knowledge or consent. In the context of iPhones, spyware can:

- Monitor messages, emails, and calls
- Track location
- Activate the camera and microphone
- Harvest passwords and other sensitive information

Unlike typical malware, which often requires user interaction (clicking on a malicious link), advanced spyware targeting iPhones may use zero-click exploits, with no user action, to compromise the device. Zero-click techniques are a form of cyber attack that allows a system to be compromised without any action from the victim. These techniques exploit vulnerabilities in software or hardware to gain unauthorized access to a device or network.

Notable Spyware Attacks on iPhones

1. Pegasus Spyware

Developed by the Israeli company NSO Group, Pegasus is the most infamous spyware related to iPhone attacks. First discovered in 2016, it has been used to survey journalists, human rights activists, and political figures worldwide.

Pegasus can exploit vulnerabilities in iOS via zero-click techniques such as those involving iMessage or FaceTime, and once installed, it can completely compromise the device.

In 2021, investigations revealed that Pegasus was used to target over 50,000 phone numbers, including heads of state, opposition leaders, and journalists.

2. ForcedEntry Exploit

In 2021, cybersecurity researchers at Citizen Lab uncovered ForcedEntry, a zero-click iMessage exploit used to deploy Pegasus spyware. Apple patched this vulnerability with iOS 14.8, underscoring a constant game of cat and mouse between attackers and defenders.

3. Triangulation Campaign

In 2023, Kaspersky reported a sophisticated attack through a campaign targeting the iPhones of company employees. Using an invisible iMessage with a malicious attachment, attackers were able to gain control over devices without any user interaction. The Apple iPhone spyware could persist even after a reboot and was designed to be stealthy and difficult to detect.

4. Mercenary Spyware

Apple has sent alerts to iPhone users in 100 countries, and recommends they enable Lockdown Mode. Apple has detected mercenary spyware attacks on select iPhones and issued Threat Notifications to those affected. If Apple detected a targeted mercenary spyware attack against your iPhone," it reads the subject of the message sent from ***threat-notifications@email.apple.com*** via email and iMessage. To confirm if it's genuinely from Apple, you can sign in to ***account.apple.com*** and look for a notification up top.

Mercenary spyware attacks are well-funded zero-click attacks often associated with state-sponsored actors. These attacks target specific iPhones, extract information, and vanish. Journalists, activists, politicians, and diplomats are often victims.

How Spyware Attacks Exploit Work-related Devices

Advanced spyware attacks on iPhones often leverage:

- **Zero-day vulnerabilities:** Unknown flaws in iOS that are exploited before Apple is aware or has issued a fix.
- **Zero-click exploits:** Require no interaction from the user; a malicious code is embedded in a message that triggers automatically when received.
- **Privilege escalation:** Once inside the device, spyware elevates its permissions to gain full control.

These techniques are typically part of Advanced Persistent Threats, long-term, highly targeted attacks often backed by state actors.

How to Protect Your iPhone

While no device is 100% immune to spyware, users can take precautions:

1. **Update regularly:** Always install the latest iOS updates to patch known vulnerabilities. Update them when IHS Information Technology personnel inform you that an update is available.
2. **Take physical security measures:** Set up a strong passcode/personal identification number on your Government-furnished Equipment (GFE) device to prevent unauthorized access. This serves as the first line of defense in case your device is lost or stolen. Never share your device passcode/personal identification number.
3. **Be cautious with links and attachments:** Avoid clicking suspicious links or opening files from unknown sources.
4. **Enable two-factor authentication:** Add a layer of security to your Apple ID.
5. **Check device analytics:** Look for unusual activity or diagnostics suggesting unauthorized access.
6. **Avoid jailbreaking:** This removes built-in security features and makes your device more vulnerable. Download only IHS-approved apps from the “Apps Catalog” on your GFE.

Conclusion

Spyware attacks on iPhones are a stark reminder that no system is completely secure. The combination of valuable personal data and a widespread user base makes iPhones a prime target for sophisticated attackers. While Apple continues to raise the bar on security, vigilance, awareness, and proactive measures remain essential for users, especially those in sensitive roles. In an increasingly surveilled digital landscape, understanding the threat is the first step toward maintaining your privacy and security.

NOTE: The links and products in this document are for informational purposes only, and do not signify an endorsement.

For questions or further information, please contact the IHS Office of Information Technology, Division of Information Security, at cybersecurity@ihs.gov. You must immediately report all lost, stolen, or compromised GFE mobile devices to your Area ISSO or the IHS Cybersecurity Operations Center (CSOC) at incident@ihs.gov. If immediate contact is not possible, users should contact the IHS IT Service Desk (888-830-7280) within 24 hours of the reported loss.