Pegasus Spyware: Mechanisms of Operation, Vectors of Infection, and Countermeasures for Mobile Surveillance Defense

Dinesh Abeywickrama
Ph.D. (Reading), MBCS, MBA, BCS
siyalla@gmail.com

Abstract

Pegasus is a sophisticated commercial spyware application developed by the Israeli NSO Group, capable of transforming an infected mobile device into a covert surveillance platform. This article presents a structured overview of Pegasus spyware, examining its operational characteristics, documented deployment across 45 countries as of 2018, and its targeting of journalists, civil society members, and human rights activists. The article analyzes the three primary infection vectors — zero-day exploits, spear-phishing attacks, and physical device access — and provides evidence-based countermeasures derived from investigations conducted by the Citizen Lab and Amnesty International. The findings underscore the need for heightened digital security awareness among vulnerable populations, including media professionals and civil activists, and outline actionable defense protocols for individuals at elevated risk of mobile surveillance.

Keywords: *Pegasus, spyware, mobile surveillance, NSO Group, zero-day exploit, spear-phishing, cybersecurity, digital privacy, journalism safety, Citizen Lab, Amnesty International*

1. Introduction

The proliferation of commercial surveillance tools has raised profound concerns about the privacy and safety of journalists, political dissidents, human rights defenders, and ordinary citizens worldwide. Among the most widely documented and technically sophisticated of these tools is Pegasus — a mobile spyware application engineered by the Israeli NSO Group. Unlike conventional malware that typically targets financial data or system resources, Pegasus is explicitly designed to convert a compromised

mobile device into a comprehensive surveillance apparatus, capable of intercepting communications, tracking physical location, and activating device hardware without the owner's knowledge.

This article provides an evidence-based, structured examination of Pegasus spyware, drawing from documented investigations and academic research. It is intended to serve both as a technical reference for cybersecurity practitioners and as an accessible guide for non-specialist audiences — particularly journalists and civil society members — who face elevated surveillance risks. The article addresses: (1) the functional capabilities of Pegasus, (2) its documented global deployment, (3) the technical infection vectors through which it spreads, and (4) practical countermeasures for detection and risk mitigation.

2. Background and Context

Pegasus was developed by the NSO Group, an Israeli technology firm that describes its products as lawful interception tools sold exclusively to vetted government clients for counter-terrorism and criminal investigation purposes. However, investigations by independent research institutions — notably Citizen Lab at the University of Toronto and Amnesty International — have consistently documented the use of Pegasus against journalists, lawyers, political opponents, and human rights defenders in numerous countries.

A 2018 analysis by Citizen Lab identified active Pegasus infrastructure in 45 countries, including Mexico, Saudi Arabia, Bahrain, Morocco, Israel, the United States, and the United Arab Emirates. In these jurisdictions, investigators confirmed the use of Pegasus to monitor journalists and civil activists, raising serious concerns about the weaponization of commercial surveillance tools against civil society. In 2019, Facebook's WhatsApp revealed that Pegasus had exploited a vulnerability in its calling feature to infect approximately 1,400 devices belonging to human rights activists and journalists across roughly 20 countries (Chawla, 2021; Rudie et al., 2021).

3. Operational Capabilities of Pegasus

Once installed on a target device, Pegasus operates with a broad range of covert capabilities that span data extraction, real-time monitoring, and active hardware control. These capabilities function across Android, iOS, and BlackBerry operating systems and are designed to remain undetected by standard device users.

3.1 Data Interception and Exfiltration

Pegasus is capable of silently accessing and transmitting the following categories of data from an infected device:

- Call logs and the content of voice communications
- Messages transmitted through encrypted messaging applications (e.g., WhatsApp, Signal, Telegram)
- Email correspondence and attachments
- Real-time and historical GPS location data
- Stored files, photographs, and contacts
- Browser history and stored passwords

3.2 Hardware Activation and Environmental Surveillance

Beyond passive data collection, Pegasus possesses the ability to actively engage device hardware components:

- Remote activation of the device camera (front and rear) for silent image or video capture
- Remote activation of the device microphone to eavesdrop on ambient conversations and surroundings

3.3 Stealth and Persistence

Pegasus is engineered to evade detection. It operates without generating user-visible notifications, does not appear in the device's application list as a recognizable entry, and is typically invisible to standard antivirus or security scanning applications. Detection generally requires specialized forensic analysis by a digital security expert using purpose-built tools such as the Mobile Verification Toolkit (MVT) developed by Amnesty International's Security Lab (Rudie et al., 2021).

4. Infection Vectors

Pegasus can be installed through several technical pathways. An understanding of these vectors is essential for both risk assessment and prevention.

4.1 Zero-Day Exploit Attacks

A zero-day attack exploits an unpatched or previously unknown vulnerability in a software

application or operating system, enabling malicious code to execute without any user interaction. In the WhatsApp case documented in 2019, a vulnerability in the application's Voice over IP (VoIP) calling function was exploited: a call from an unknown number to the target device was sufficient to install Pegasus, even if the call was never answered. The call frequently did not appear in the device's call registry, eliminating a potential detection indicator.

Zero-day vulnerabilities are particularly difficult to defend against because no security patch exists at the time of exploitation. High-risk individuals in some documented cases have adopted the practice of using inexpensive, disposable mobile phones for limited periods — typically one month — before destroying and replacing them, as a non-technical mitigation strategy.

4.2 Spear-Phishing Attacks

Spear-phishing involves the targeted delivery of a deceptive message, crafted to resemble a communication that the recipient would consider legitimate and important. The message is engineered to induce the recipient to click a hyperlink or open an attachment, at which point Pegasus is downloaded and installed on the device. According to investigations by Citizen Lab and Amnesty International, such messages may be delivered via:

- SMS (Short Message Service)
- Email
- Chat messenger platforms
- Social media direct messages

The social engineering content of these messages frequently impersonates one of the following:

- Official communications from diplomatic or consular offices known to the target
- Security alerts claiming the target's device is under threat
- Employment or professional opportunity notifications
- Messages containing photographs or personal information about trusted individuals
- Notifications from financial service providers, including banks or credit card institutions

4.2.1 Defense Strategies Against Spear-Phishing

Based on guidance from Citizen Lab and Amnesty International, the following countermeasures are recommended:

- A. Sender Verification: Independently confirm the authenticity of unexpected messages through a secondary communication channel. Exercise caution with secondary-source verification, as attackers may seed false information in publicly accessible sources.
- B. Secondary Device Protocol: When a message requires inspection, use a dedicated secondary device. Keep this device deactivated and with the battery removed when not in use, and perform periodic factory resets to reduce the risk of persistent infection.
- C. URL Expansion: Before clicking shortened links (e.g., those generated by Bitly or TinyURL), use a URL expansion tool such as Urlex to inspect the actual destination URL.
- D. Alternative Browser Usage: Default web browsers (e.g., Google Chrome on Android; Safari on iOS) are known primary targets of Pegasus exploitation. Using a non-default browser can reduce exposure to browser-targeting attack vectors.

4.3 Physical Device Access

Pegasus can also be installed on a device through direct physical access. An adversary with brief, unsupervised access to an unlocked device can install surveillance software manually. This vector is particularly relevant in contexts such as border crossings, security checkpoints, or custody situations where device confiscation may occur.

5. Recommended Response Protocol for Suspected Compromise

If an individual has reason to believe that Pegasus or a similar spyware application may have been installed on their mobile device, the following immediate steps are advised:

- Discontinue use of the device immediately to prevent further data exfiltration.
- Isolate the device in a physically secure location, away from the target individual and their close contacts, to prevent ongoing environmental surveillance.
- Log out of all user accounts associated with the compromised device from a separate, clean device.
- Change all account passwords and authentication credentials from a separate, uncompromised device.
- Seek assistance from a qualified digital security expert or organization, such as Access Now's Digital Security Helpline or Frontline Defenders, for forensic examination using tools such as Amnesty International's Mobile Verification Toolkit (MVT).

6. General Preventive Measures

Beyond the specific countermeasures outlined in Section 4, the following general practices reduce the overall risk of mobile surveillance compromise:

- Keep all device operating systems and applications updated to minimize exploitable vulnerabilities.
- Avoid leaving mobile devices unattended in environments accessible to potential adversaries.
- When handing a device to authorities for inspection, power it off entirely before surrendering it.
- Use strong, complex passwords incorporating alphanumeric characters and symbols; enable full-disk encryption where available.
- Periodically review installed applications and revoke unnecessary permissions from camera and microphone access.

7. Discussion

The Pegasus case illustrates the broader challenge posed by the commercial spyware industry: the dual-use nature of surveillance technology means that tools ostensibly developed for legitimate law enforcement purposes can be — and have been — repurposed to target civil society, suppress press freedom, and undermine political opposition. The technical sophistication of Pegasus, particularly its zero-click zero-day infection vectors, places it in a category of threat that cannot be reliably neutralized through standard consumer security practices alone.

The asymmetry between attacker and defender capabilities is a central concern. State-level actors or well-resourced non-state actors who acquire access to Pegasus-level tools possess an operational advantage that is difficult for individuals to overcome through behavioral measures alone. Structural solutions — including mandatory disclosure of zero-day vulnerabilities, regulatory frameworks governing the export of surveillance technology, and investment in open-source security tooling for high-risk civil society actors — are necessary complements to individual protective measures.

8. Conclusion

Pegasus represents one of the most technically capable and extensively documented examples of commercial mobile spyware. Its documented use against journalists, human rights defenders, and civil activists in dozens of countries underscores the pressing need for digital security awareness, proactive protective measures, and institutional safeguards. This article has outlined the primary infection vectors

— zero-day exploits, spear-phishing, and physical access — and presented evidence-based countermeasures for individuals at elevated risk of mobile surveillance targeting.

Future work in this domain should focus on the development of scalable, accessible forensic detection tools for non-specialist users, as well as the establishment of international legal frameworks governing the export and use of commercial surveillance technologies. The intersection of cybersecurity, press freedom, and human rights demands a multidisciplinary response that spans technical, legal, and policy dimensions.

References

Chawla, A. (2021). Pegasus Spyware — "A Privacy Killer." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3890657

Rudie, J., Katz, Z., Kuhbander, S., & Bhunia, S. (2021). Technical analysis of the NSO Group's Pegasus spyware. In Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 747–752). IEEE. https://doi.org/10.1109/CSCI54926.2021.00188

Citizen Lab. (2018). Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries. University of Toronto. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Amnesty International. (2021). Forensic methodology report: How to catch NSO Group's Pegasus. Amnesty International Security Lab. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

NSO Group. (2021). Transparency and responsibility report. NSO Group Technologies. https://www.nsogroup.com/

Abeywickrama, D. (2021, April 10; rev. 2024, September 19). Pegasus that secretly monitors your mobile phone. Siyalla. https://www.siyalla.com/pegasus-spyware/