

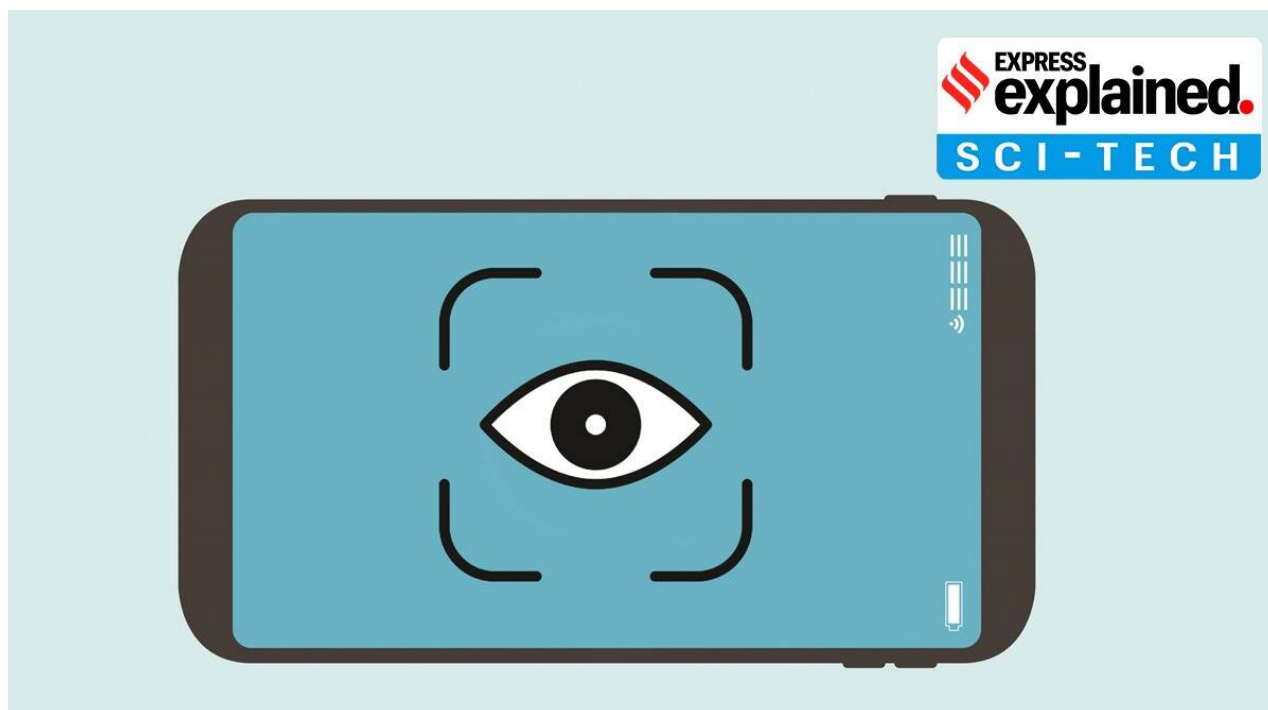
# Explained: Here's how NSO Group's spyware Pegasus infects your device

 [indianexpress.com/article/explained/pegasus-whatsapp-spyware-israel-india-7410890](https://indianexpress.com/article/explained/pegasus-whatsapp-spyware-israel-india-7410890)

July 22, 2021

Written by [Jay Mazoomdaar](#) , Edited by Explained Desk

New Delhi | Updated: July 22, 2021 8:10:05 am



Pegasus is NSO Group's flagship product (Express illustration)

In November 2019, a tech reporter from New York City photographed an interception device displayed at Milipol, a trade show on homeland security in Paris. The exhibitor, NSO Group, placed the hardware at the back of a van, perhaps suggesting convenience of portability, and said it would not work on US phone numbers, possibly due to a self-imposed restriction by the firm.

Since the Israeli cyber giant was founded in 2010, that was probably the first time an NSO-made portable Base Transceiver Station (BTS) was featured in a media report.

A BTS — or 'rogue cell tower' or 'IMSI Catcher' or 'stingray' — impersonates legitimate cellular towers and forces mobile phones within a radius to connect to it, so that the intercepted traffic can be manipulated by an attacker. The BTS photographed in 2019 was composed of horizontally-stacked cards, likely to allow interception over multiple frequency bands.

The other option is to leverage access to the target's mobile operator itself. In that scenario, an attacker would not need any rogue cell tower but would rely on the regular network infrastructure for manipulation.



Watch Video At: <https://youtu.be/Lun4CBY5ECQ>

Either way, the capability of launching ‘network injection’ attacks — performed remotely without the target’s engagement (hence, also **called zero-click**) or knowledge — gave Pegasus, NSO Group’s flagship product, an unique edge over its competitors in the global spyware market.

Pegasus is now at the centre of a global collaborative investigative project that has found that the spyware was used to target, among others, **hundreds of mobile phones in India**.

Don't miss | [The making of Pegasus, from startup to spy-tech leader](#)

## How is Pegasus different from other spyware?

---

Pegasus aka Q Suite, marketed by the NSO Group aka Q Cyber Technologies as “a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract” data “from virtually any mobile devices”, was developed by veterans of Israeli intelligence agencies.

Until early 2018, NSO Group clients primarily relied on SMS and WhatsApp messages to trick targets into opening a malicious link, which would lead to infection of their mobile devices. A Pegasus brochure described this as Enhanced Social Engineering Message (ESEM). When a malicious link packaged as ESEM is clicked, the phone is directed to a server that checks the operating system and delivers the suitable remote exploit.

In its October 2019 report, Amnesty International first documented use of ‘network injections’ which enabled attackers to install the spyware “without requiring any interaction by the target”. Pegasus can achieve such zero-click installations in various ways. One over-the-air (OTA) option is to send a push message covertly that makes the target device load the spyware, with the target unaware of the installation over which she anyway has no control.

This, a Pegasus brochure brags, is “NSO uniqueness, which significantly differentiates the Pegasus solution” from any other spyware available in the market.

Also read | [Eleven phones targeted: Of woman who accused ex-CJI of harassment, kin](#)

## **What kind of devices are vulnerable?**

---

All devices, practically. iPhones have been widely targeted with Pegasus through [Apple](#)’s default iMessage app and the Push Notification Service (APNs) protocol upon which it is based. The spyware can impersonate an application downloaded to an iPhone and transmit itself as push notifications via Apple’s servers.

In August 2016, the Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, reported the existence of Pegasus to cyber security firm Lookout, and the two flagged the threat to Apple. In April 2017, Lookout and [Google](#) released details on an [Android](#) version of Pegasus.

In October 2019, WhatsApp blamed the NSO Group for exploiting a vulnerability in its video-calling feature. “A user would receive what appeared to be a video call, but this was not a normal call. After the phone rang, the attacker secretly transmitted malicious code in an effort to infect the victim’s phone with spyware. The person did not even have to answer the call,” WhatsApp chief Will Cathcart said.

In December 2020, a Citizen Lab report flagged how government operatives used Pegasus to hack 37 phones belonging to journalists, producers, anchors, and executives at Al Jazeera and London-based Al Araby TV during July-August 2020, exploiting a zero-day (a vulnerability unknown to developers) against at least [iOS 13.5.1](#) that could hack Apple’s then-latest iPhone 11. While the attack did not work against iOS 14 and above, the report said the infections it observed were probably a minuscule fraction of the total attacks, given the global spread of the NSO Group’s customer base and the apparent vulnerability of almost all iPhone devices prior to the iOS 14 update.

### **Coronavirus Explained**

- [Which countries can Indians now visit?](#)
- [1 million kids lost a parent to Covid; 1.1 lakh in India](#)
- [2/3 Indians exposed to Covid: ICMR findings explained](#)

[Click here for more](#)

## **Does the spyware always get into any device it targets?**

---

Usually, an attacker needs to feed the Pegasus system just the target phone number for a network injection. “The rest is done automatically by the system,” says a Pegasus brochure, and the spyware is installed in most cases.

In some cases, though, network injections may not work. For example, remote installation fails when the target device is not supported by the NSO system, or its operating system is upgraded with new security protections.

Apparently, one way to dodge Pegasus is to change one’s default phone browser.

According to a Pegasus brochure, “installation from browsers other than the device default (and also chrome for android based devices) is not supported by the system”.

In all such cases, installation will be aborted and the browser of the target device will display a pre-determined innocuous webpage so that the target does not have an inkling of the failed attempt. Next, an attacker is likely to fall back on ESEM click baits. All else failing, says the brochure, Pegasus can be “manually injected and installed in less than five minutes” if an attacker gets physical access to the target device.



Also read | [2019 & now, Govt ducks key question: did it buy Pegasus?](#)

## **What information can be compromised?**

---

Once infected, a phone becomes a digital spy under the attacker’s complete control.

Upon installation, Pegasus contacts the attacker’s command and control (C&C) servers to receive and execute instructions and send back the target’s private data, including passwords, contact lists, calendar events, text messages, and live voice calls (even those via end-to-end-encrypted messaging apps). The attacker can control the phone’s camera and microphone, and use the GPS function to track a target.

To avoid extensive bandwidth consumption that may alert a target, Pegasus sends only scheduled updates to a C&C server. The spyware is designed to evade forensic analysis, avoid detection by anti-virus software, and can be deactivated and removed by the attacker, when and if necessary.

## **What precautions can one take?**

---

Theoretically, astute cyber hygiene can safeguard against ESEM baits. But when Pegasus exploits a vulnerability in one's phone's operating system, there is nothing one can do to stop a network injection. Worse, one will not even be aware of it unless the device is scanned at a digital security lab.

Switching to an archaic handset that allows only basic calls and messages will certainly limit data exposure, but may not significantly cut down infection risk. Also, any alternative devices used for emails and apps will remain vulnerable unless one forgoes using those essential services altogether.

Therefore, the best one can do is to stay up to date with every operating system update and security patch released by device manufacturers, and hope that zero-day attacks become rarer. And if one has the budget, changing handsets periodically is perhaps the most effective, if expensive, remedy.


Since the spyware resides in the hardware, the attacker will have to successfully infect the new device every time one changes. That may pose both logistical (cost) and technical (security upgrade) challenges. Unless one is up against unlimited resources, usually associated with state power.



Want to go beyond the news and understand the headlines? Subscribe to Explained by The Indian Express

 ***The Indian Express is now on Telegram. Click [here to join our channel \(@indianexpress\)](#) and stay updated with the latest headlines***

For all the latest [Explained News](#), download [Indian Express App](#).

- 
- The Indian Express website has been rated GREEN for its credibility and trustworthiness by Newsguard, a global service that rates news sources for their journalistic standards.
- 



22 Comment(s) \*

\* The moderation of comments is automated and not cleared manually by [indianexpress.com](https://indianexpress.com).