

## Israeli Spyware Pegasus

### Why in news?

- Cyber-attack reports are emerging from a collaborative investigation by journalists from around the world, including from India's The Wire, titled the 'Pegasus Project'.
- Accordingly, over 300 verified Indian mobile telephone numbers were targeted using spyware made by the Israeli firm, NSO Group.

### What is Pegasus?

- Pegasus is also known as Q Suite.
- It is marketed by the NSO Group also known as Q Cyber Technologies, as a world-leading cyber intelligence solution.
- [NSO Group Technologies is an Israeli technology firm.]
- It enables law enforcement and intelligence agencies to remotely and covertly extract data "from virtually any mobile device."
- It was developed by veterans of Israeli intelligence agencies.

### How was it earlier?

- Until early 2018, NSO Group clients primarily relied on SMS and WhatsApp messages.
- They use these mediums to trick targets into opening a malicious link, which would lead to infection of their mobile devices.
- This is described as Enhanced Social Engineering Message (ESEM).
- In its October 2019 report, Amnesty International first documented the use of 'network injections.'
- This enabled attackers to install the spyware "without requiring any interaction by the target". This is called zero-click installation.

### How is Pegasus different from other spywares?

- Pegasus can achieve such zero-click installations in various ways.
- The over-the-air (OTA) option is to send a push message covertly that makes the target device load the spyware.
- The target remains unaware of the installation and has no control over it.
- This is "NSO uniqueness, which significantly differentiates the Pegasus solution" from any other spyware available in the market.

## What kind of devices are vulnerable?

- All devices, practically, are vulnerable to Pegasus intervention.
- iPhones have been widely targeted with Pegasus.
- It is done through Apple's default iMessage app and the Push Notification Service (APNs) protocol upon which it is based.
- WhatsApp has, in 2019, blamed the NSO Group for exploiting a vulnerability in its video-calling feature.
- In December 2020, a Citizen Lab report flagged how government operatives used Pegasus.
- They used it to hack 37 phones belonging to journalists, producers, anchors, and executives at Al Jazeera and London-based Al Araby TV.
- [Citizen Lab - an interdisciplinary laboratory based at the University of Toronto]

## How does it work?

- 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.
- And the spyware is installed in most cases.
- In some cases, though, network injections may not work.
- E.g., remote installation fails when the target device is not supported by the NSO system, or its operating system is upgraded with new security protections.
- Next, an attacker is likely to fall back on ESEM click baits.
- All else failing, Pegasus can be "manually injected and installed in less than five minutes" if an attacker gets physical access to the target device.

## What kinds of information are at risk?

- 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.
- It receives and executes instructions and sends back the target's private data.
- These may include 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.
- It can also be deactivated and removed by the attacker, when and if necessary.

### **What precautions could be taken?**

- Apparently, one way to dodge Pegasus is to change one's default phone browser.
- 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.
- 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 it 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.
- Changing handsets periodically is perhaps the most effective, but expensive, remedy.
- [Since the spyware resides in the hardware, the attacker will have to successfully infect the new device every time it is changed.]

**Source: The Indian Express**

