Pegasus Spyware – "A Privacy Killer"

Ajay Chawla[1]

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."[2]

INTRODUCTION

The recent Pegasus Project revelations of about half a lakh people across the world, including several in India, being targeted for cyber surveillance has firmly brought the spotlight on the Pegasus spyware, which is widely understood to be the most sophisticated smartphone attack tool. The revelations also mark the first time that a malicious remote jailbreak exploit had been detected within an iPhone.

Pegasus is a spyware (Trojan/Script) that can be installed remotely on devices running on Apple's iOS & Google's Android operating systems. It is developed and marketed by the Israeli technology firm NSO Group. NSO Group sells Pegasus to "vetted governments" for "lawful interception", which is understood to mean combating terrorism and organized crime, as the firm claims, but suspicions exist that it is availed for other purposes.

Spyware has evolved leaps and bounds in the last decade. In 2010, one would have received a suspicious email, and only upon opening the email would the malware be installed in their computer. The initial version of Pegasus, however, adopted the "mobile-first" strategy, where targeted individuals would start to receive text messages which would look like their family members sending them a link to their bank accounts, or their location, etc. In January 2016, Carmen Aristegui, an investigative journalist in Mexico, started receiving messages with suspicious links after she published an investigation into property owned by former Mexican President Enrique Pena Nieto.[3]

---

[1] Ajay Chawla, Advocate Delhi High Court, advajaychawla@gmail.com

[2] Marlon Brando, Jr. was an American movie star and political activist.

[3] https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/microsoft-exchange-email-hack-was-caused-china-us-says-2133991

Pegasus burst into global prominence in August 2016 after a failed attempt of installing it on the iPhone of Emirati human rights activist Ahmed Mansoor was detected when he received a series of SMSs promising “new secrets” about torture happening in prisons in the United Arab Emirates (UAE) if he clicked on certain URL/web links.

Mansoor got suspicious about the messages and reached out to the information controls research laboratory Citizen Lab to examine the SMSs. Citizen Lab’s investigation revealed that if Mansoor had followed the link, his phone would have been jailbroken on the spot and spyware implanted into it. Citizen Lab linked the attack to NSO Group by the IP address embedded in the text. Its report details the spyware’s abilities, and the security vulnerabilities it exploited.

Pegasus is a modular malware that can initiate total surveillance on the targeted device, as per a report by digital security company Kaspersky. It installs the necessary modules to read the user’s messages and mail, listen to calls, send back the browser history and more, which basically means taking control of nearly all aspects of your digital life. It can even listen in to encrypted audio and text files on your device that makes all the data on your device up for grabs.

The updated Pegasus spyware is a "zero-link" technology which takes advantage of zero-day vulnerabilities -- meaning the user is not required to click on any link. Zero-day vulnerabilities are referred to as newly discovered vulnerabilities within the operating software that the developer is still unaware of. Since the vulnerability is still in its "day zero", there are no patches or updates that can secure a user. Using such vulnerabilities, NSO Group -- the Israeli owner and creator of Pegasus -- sends the spyware to the target's phone, either through text message or a phone call. Since no action is required by the user, the malware instantly installs itself within the phone. Once installed, Pegasus gives NSO's "government clients" access to the target's device, bypassing even encrypted messaging apps like Signal, WhatsApp, and Telegram.

Since Pegasus hacks into the operating system, every activity within the phone can be monitored when the phone is switched on. It's as if someone is monitoring your phone activity over your shoulders. Pegasus operators can remotely record audio and video from your phone, extract phone messages, use GPS for location tracking, and

recover passwords and authentication keys without the user even noticing. It's only when a device is sent for forensic screening, and experts look into the transfer of data to and from the phone, is when a potential attack can be confirmed. The dooming fact of it all is that since Pegasus exploits zero-day vulnerabilities, there is nothing that can be done regarding such breaches unless operating system developers proactively ship out an update to your phone, aimed to protect you from hi-tech malware like Pegasus.[4]

How Pegasus works – 3 Modes

Target: Someone sends what's known as a trap link to a smartphone that persuades the victim to tap and activate — or activates itself without any input, as in the most sophisticated "zero-click" hacks.

Infect: The spyware captures and copies the phone's most basic functions, NSO marketing materials show, recording from the cameras and microphone and collecting location data, call logs and contacts.

Track: The implant secretly reports that information to an operative who can use it to map out sensitive details of the victim's life.

Who owns Pegasus?

Pegasus has been developed by the Israeli firm NSO Group that was set up on 25 January 2010.

According to an Amnesty International report, the first name initials of the founders form the acronym 'NSO'. The founders are Niv Carmi, Shalev Hulio and Omri Lavie.

NSO Group's majority ownership vests its co-founders Omri Lavie and Shalev Hulo, and the European private equity fund Novalpina Capital. An American private equity firm, Francisco Partners, holds a minority stake in the firm.[5]

[4] https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/pegasus-spyware-what-it-and-how-does-it-work-2134001
[5] https://www.newsclick.in/An-Explainer-Pegasus-Spyware

The Amnesty report citing Hulio says NSO's goal was "to develop technology that would provide law enforcement and intelligence agencies with direct remote access to mobile phones and their content – a workaround to the increasingly widespread use of encryption in the digital environment".

The Amnesty report adds that Hulio "claimed" the idea for a service and company like NSO was inspired by "a request from European authorities that were familiar with his and Omri Lavie's existing work on cell phone carrier customer service technology".

What can Pegasus do?

Unlimited access to target's mobile devices: Remotely and covertly collect information about your target's relationships, location, phone calls, plans, and activities whenever and wherever they are[6]

- Intercept calls: Transparently monitor voice and VoIP calls in real-time
- Bridge intelligence gaps: Collect unique and new types of information (e.g., contacts, files, environmental wiretap, passwords, etc.) to deliver the most accurate and complete intelligence
- Handle encrypted content and devices: Overcome encryption, SSL, proprietary protocols and any hurdle introduced by the complex communications world
- Application monitoring: Monitor a multitude of applications including Skype, WhatsApp, Viber, Facebook and Blackberry Messenger (BBM)
- Pinpoint targets: Track targets and get accurate positioning information using GPS
- Service provider independence: No cooperation with local Mobile Network Operators(MNO) is needed
- Discover virtual identities: Constantly monitor the device without worrying abou tfrequent switching of virtual identities and replacement of SIM cards

[6] https://www.firstpost.com/tech/news-analysis/pegasus-spyware-a-complete-guide-to-how-it-can-be-used-to-infiltrate-your-phone-7585931.html

- Avoid unnecessary risks: Eliminate the need for physical proximity to the target or device at any phase.

Does it Affect Other Apps?

Pegasus allows the controller to access the phone's mic and camera, but nowhere does it mention that it can affect other applications.

Yes, the controller can have access to files, images and even read encrypted messages and emails, but there is uncertainty as to whether it allows them to manipulate other applications on the phone.

It also allows access to the location data of the user and one can also read screenshots and typing feedback logs. This way the controller can know what passwords you are using to access different websites and even banking applications. To add to the above, it also provides access to contact details, browsing history, microphone recordings, and even retrieved files.[7]

Can infect both Android & Apple devices

The spyware infects Android and Apple devices too, but isn't as effective as it relies on a rooting technique that isn't 100 per cent reliable. When the initial infection attempt fails, the spyware supposedly prompts the user to grant relevant permissions so it can be deployed effectively.

What threat does it cause?

The Pegasus spyware can hack the target user's phone and access all their personal information. It can even access encrypted chats made through WhatsApp. You would be surprised to know that this spyware can also read messages, track calls, keep a check on user activity within apps, and gather their location data, and access video cameras on the phone. Not just this, the hacker can also listen through their microphones using the Pegasus spyware.

[7] https://www.thequint.com/explainers/pegasus-spyware-attack-and-affected-phones-explained

What's happening around the World?

Israeli firm NSO Group's flagship software, Pegasus, is in the news yet again this time, for being used to spy on businessmen, politicians, journalists, and in some cases, even prime ministers.

An international consortium of news outlets reported that several authoritarian governments including Mexico, Morocco and the United Arab Emirates used spyware developed by NSO Group to hack into the phones of thousands of their most vocal critics, including journalists, activists, politicians and business executives.

A leaked list of 50,000 phone numbers of potential surveillance targets was obtained by Paris-based journalism nonprofit Forbidden Stories and Amnesty International and shared with the reporting consortium, including The Washington Post and The Guardian. Researchers analyzed the phones of dozens of victims to confirm they were targeted by the NSO's Pegasus spyware, which can access all of the data on a person's phone. The reports also confirm new details of the government customers themselves, which NSO Group closely guards. Hungary, a member of the European Union where privacy from surveillance is supposed to be a fundamental right for its 500 million residents, is named as an NSO customer.

Forbidden Stories received a leaked list of 50,000 phone numbers this also includes potential targets. A review of dozens of phones confirmed the presence of the Pegasus spyware.[8]

The reporting shows for the first time how many individuals are likely targets of NSO's intrusive device-level surveillance. Previous reporting had put the number of known victims in the hundreds or more than a thousand.[9]

[8] https://www.businessinsider.in/tech/news/how-to-find-out-if-your-phone-is-infected-by-the-pegasus-spyware/articleshow/84578193.cms
[9] https://techcrunch.com/2021/07/19/toolkit-nso-pegasus-iphone-android/

2019 WhatsApp hack in India

In late 2019, it was found WhatsApp had been infiltrated to hack a number of activists, journalists, and bureaucrats in India, leading to accusations that the Indian government was involved.[10]

On October 30, 2019, WhatsApp's parent company Facebook confirmed that Pegasus was used to target Indian journalists, activists, lawyers and senior government officials. The journalists and activists were believed to have been targets of surveillance for a two-week period prior to the Lok Sabha elections. (Incidentally, several of the Indian numbers identified in the Pegasus Project revelations were added to the target list in the run up to the Lok Sabha elections as well.)

Further, the Indian IT Ministry sought a detailed response from WhatsApp on the issue. Whatsapp responded that it had alerted the Indian government about the security compromise on two occasions — once in May and again in September 2019. It verified that in all, 121 individuals had been targeted by the spyware.

Some of the Indian individuals targeted by Pegasus via Whatsapp in 2019 – academic Anand Teltumbde, Nagpur lawyers Nihalsing Rathod Jagdish Meshram, adivasi rights activist Bela Bhatia, lawyer and activist Shalini Gera, activist Rupali Jadhav, and P Pavana, the daughter of Bhima Koregaon case accused – have also been found in the latest leaked list of targets uncovered by the Pegasus Project.

A Right to Information (RTI) application was filed in October 2019 by journalist Saurav Das in which he asked whether the Indian government had purchased or given a purchase order for the Pegasus spyware.

In response, the Ministry of Home Affairs stated: "Please refer to your online RTI application dated 23.10.2019 received by the undersigned CPIO [Central Public Information Officer] on 24.10.2019. It is informed that no such information is available with the undersigned CPIO."[11]

[10] https://thewire.in/media/pegasus-project-spyware-indian-journalists
[11] https://www.newsclick.in/An-Explainer-Pegasus-Spyware

Recent Steps Taken in India:

1) ***Cyber Surakshit Bharat Initiative****:* It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.

2) ***National Cyber security Coordination Centre (NCCC):*** In 2017, the NCCC was developed to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.

3) ***Cyber Swachhta Kendra****:* In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.

4) ***Indian Cyber Crime Coordination Centre (I4C):*** I4C was recently inaugurated by the government.

a. National Cyber Crime Reporting Portal has also been launched pan India.

5) ***Computer Emergency Response Team - India (CERT-IN):*** It is the nodal agency which deals with cybersecurity threats like hacking and phishing.

6) ***Legislation****:*

- Information Technology Act, 2000.
- Personal Data Protection Bill, 2019.

What can I do to be better protected?

Although most people are unlikely to be targeted by this type of attack, there are still simple steps you can take to minimise your potential exposure — not only to Pegasus but to other malicious attacks too.

1. Only open links from known and trusted contacts and sources when using your device. Pegasus is deployed to Apple devices through an iMessage link. And this is is the same technique used by many cybercriminals for both malware distribution and less technical scams. The same advice applies to links sent via email or other messaging applications.
2. Make sure your device is updated with any relevant patches and upgrades. While having a standardised version of an operating system creates a stable base for attackers to target, it's still your best defence. If you use Android, don't rely on notifications for new versions of the operating system. Check for the latest version yourself, as your device's manufacturer may not be providing updates.
3. Although it may sound obvious, you should limit physical access to your phone. Do this by enabling pin, finger or face-locking on the device. The eSafety Commissioner's website has a range of videos explaining how to configure your device securely.
4. Avoid public and free WiFi services (including hotels), especially when accessing sensitive information. The use of a VPN is a good solution when you need to use such networks.
5. Encrypt your device data and enable remote-wipe features where available. If your device is lost or stolen, you will have some reassurance your data can remain safe.[12]

X-X-X-X-X

[12] https://www.freepressjournal.in/business/pegasus-spyware-heres-how-you-can-protect-your-phone-from-malicious-software