Source : www.thehindu.com Date : 2021-07-21

PEGASUS ISSUE

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Pegasus can infect both iOS and Android mobile phones, and turn them into surveillance devices | Photo Credit: Reuters

According to an investigative report by a consortium of media outlets, thousands of activists, journalists and political leaders across the world were targeted by clients of an Israeli spyware maker NSO Group. Over 300 Indians including two serving ministers in the Modi government, three opposition leaders, journalists, rights activists, and businessmen are said to a part of the leaked list of possible targets.

(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)

At the heart of the hack is a powerful spyware called Pegasus, which uses zero day vulnerability in the operating systems (OS) to enter into a targeted individual's phone. Using this exploit, Pegasus can infect both iOS and Android mobile phones, and turn them into surveillance devices.

How Pegasus attacks?

Pegasus has evolved from using spear-phishing, a process where an attacker tricks the target to click on a malicious link sent via text message or email, to a more sophisticated method of attack called zero-click attacks. This new form of attack has made the software one of the most dangerous spyware that threatens individual's privacy.

What are Zero-click attacks?

As the name suggests, the attack does not require any action by the targeted phone's user. It can remotely infiltrate a device with the help of spyware.

To gain entry, the software identifies zero-day vulnerabilities, meaning flaws in the OS that are not identified yet and hence have not been patched. Instead of exploiting human error, it banks on flaws in the software and hardware system to gain access to a device.

All the hacker does is simply make a WhatsApp call and that initiates access to the OS by launching the code. After planting the malware, Pegasus alters call log so that the user has no knowledge of what happened.

"When an iPhone is compromised, it's done in such a way that allows the attacker to obtain so-called root privileges, or administrative privileges, on the device," Claudio Guarnieri, who runs Amnesty International's Berlin-based Security Lab told *The Guardian.* "Pegasus can do more than what the owner of the device can do."

NSO Group found three zero-day vulnerabilities in iOS, which allowed them entry into the system, cybersecurity firm Incognito Security explained.

Earlier, such attacks were possible only in jailbroken iPhones. Now, Pegasus, by itself, jailbreaks an iOS device without user's knowledge.

Jailbreak is a process used to gain root access to an iOS device. By doing it, an iPhone is freed from the dependence of Apple as its exclusive source for apps.

Also Read | Explained | Target list of Israeli hack-for-firm widens

In Android, a method of rooting, called framaroot, was developed to gain control over a non-iOS device. Google termed the Android version of Pegasus as Chrysaorand and had set up security update patches.

Amnesty International noted that despite issuing security updates, Android and iOS devices were breached.

Exploiting already installed software, such as iMessage, is another attractive method as it increases the number of devices that can be hacked further.

What Pegasus does?

Once the spyware enters the device, it installs a module to track call logs, read messages, emails, calendars, internet history, and gather location data to send the information to the attacker. If the hacker is unable to find zero-day flaws in the system to infiltrate, they can install Pegasus manually in a device or over a wireless transceiver.

The spyware hides intelligently using built-in self-destruct capabilities. If Pegasus fails to connect with its command-and -control server for more than 60 days, it self-destructs and removes all traces.

Also Read | New online platform maps Pegasus spread

If it detects that it was installed on the wrong device or sim card, it will again self-destruct.

Zero-click attacks are hard to detect as it is linked directly to the OS. To stay safe, users must ensure that the software and apps in the device are updated, and that any app in use is directly installed from Google Play Store or Apple’s App Store. Users must also avoid clicking links in email, text or message that does not look reputable.

Our code of editorial values

Twitter, Google, Microsoft and Photoshop maker Adobe urged the U.S. Congress to come together to protect Dreamers, with Google saying they wanted DACA to be "cemented" into law.

Josh Giegel, the chief executive and co-founder of Virgin Hyperloop foresees us zipping between cities in minutes.

END