Source : www.thehindu.com Date : 2019-11-02

IN WHATSAPP BREACH, FOLLOW THE MONEY TRAIL

Relevant for: Security Related Matters | Topic: Role of Media and Social Networking Sites in internal security challenges

On October 30, multiple Indian media publications revealed that a spyware called Pegasus (made by an Israeli firm, NSO) was used to compromise phones of multiple activists, journalists and lawyers. The phones were reportedly compromised by using vulnerability in WhatsApp which allowed the Pegasus spyware software to be installed in a target's phone by initiating a WhatsApp voice call with the target. Once installed, the spyware is able to track the activities of multiple user applications in the target's phone including messages, mails, audio calls, browser history, contacts, and so on. This also includes data (audio and text) that is exchanged via end-to-end encrypted systems such as WhatsApp. This specific vulnerability in WhatsApp has now been patched.

WhatsApp has now filed a lawsuit against the Israeli firm in a U.S. federal court in San Francisco, alleging that the Israeli group had targeted WhatsApp users and is seeking a permanent injunction banning NSO from using its service. NSO disputed the allegations levelled by WhatsApp and said in a statement that the sole purpose of NSO was to provide technology to licensed government intelligence and law enforcement agencies to help them fight terrorism and serious crime. After it was revealed that Indian citizens were spied upon using Pegasus, the Indian government has sought an explanation from WhatsApp by November 4. There was also much outrage on social media with questions being asked of the Indian government and calls to boycott WhatsApp.

While the government has tried to shift the focus to WhatsApp, it is misleading the population at large by doing so. To understand this aspect, one needs to first understand how Pegasus exactly works and how it is able to track every activity on a target's phone, and how WhatsApp is not the only gateway for Pegasus. In July and August 2016, there were multiple attempts to infect the phone of a Mexican health researcher with Pegasus by sending repeated messages that were emotionally stirring. These messages claimed various things such as his daughter had met with an accident with a link to the hospital she was admitted to, or that his wife was cheating on him with a link to a supposedly leaked photo. In all cases, the links were essentially exploit links, clicking on which would have installed Pegasus on the target's phone. In fact, Citizen Lab which has investigated several cases of Pegasus infections around the world, including the ones in India, has shown through its research as to how social engineering is a very common strategy to deliver the most sophisticated spyware.

So, how is Pegasus able to spy on every aspect of your phone? Pegasus does so by exploiting vulnerabilities in the phone's operating system. Smartphones have operating systems (OS) much like the desktops and laptops we use. While Android phones use a modified version of the famous open source operating system Linux, iPhones use a mobile operating system called iOS which was created by Apple. Lookout, which is a cybersecurity company, had partnered with Citizen Lab to investigate the 2016 case and had found that the Pegasus software had exploited three zero-day vulnerabilities in iOS to successfully attain privileged user access of the phone. A zero-day vulnerability is a flaw in a software or hardware that is previously unknown to the party responsible, which in this case is Apple. In the specific case of 2016, upon clicking on the link, the Pegasus software was first able to exploit a vulnerability in the Safari browser which is the default browser in an iPhone, and then execute a Stage 2 code which was able to jailbreak the target's iPhone to gain privileged user access. In the present case with WhatsApp, a specially crafted call was used to trigger a buffer overflow, which in turn was used to take control of the device.

The Android version of Pegasus spyware is called Chrysaor Malware and was found on about three dozen devices in 2017 according to a blog by Google. The Android version of Pegasus installs as an application on your phone, and uses a known root technique called framaroot. Rooting an Android phone enables one to get privileged user (root) access, and thus allowing the spyware to monitor various activities.

From social engineering to exploiting user apps such as WhatsApp or Safari and then eventually using the vulnerabilities in the underlying mobile operating system, NSO employs various techniques to target and take control of a user's phone. The Google Play Store and the Apple App store house thousands of apps, many of which could have undiscovered vulnerabilities, and could potentially be exploited by firms such as NSO to target individual users. Thus, we are barking up the wrong tree by focusing solely on WhatsApp. However, when an application like WhatsApp, the most used chat app, has a serious vulnerability, then the impact is much more widespread.

From a user point of view, to ensure security of your devices, it is important to keep phones updated — both the applications and the firmware. Many smartphone users often disable automatic updates in order to save on data, but this also prevents security updates from being installed on the phones. It is extremely important to be self-aware about one's digital security, as a compromise in that could lead to a situation of total surveillance.

Finally, the question that needs to be asked is who in India can afford millions of dollars to target phones of select individuals. Pegasus is a state-of-the-art spyware, and NSO charges an exorbitant sum for its product and services. According to a 2015 contract, between the National Communications Authority of Ghana, Africa, NSO, and a local reseller, NSO was paid $8 million for the Pegasus spyware and associated services. Similarly, Mexican Federal agencies have reportedly purchased $80 million worth of spyware from NSO, from 2011 to 2017. As a company, NSO has offered services to various clients, and helped them hack a victim's phone through a variety of methods. The government needs to investigate who in India can afford to hire NSO and is interested in targeting select activists, lawyers and journalists, especially when NSO itself claims that it sells the software only to government agencies. The usual whataboutery about this being an attempt to defame the government is not going to be enough this time around.

Pratik Sinha is co-founder Alt News, and formerly a software engineer who worked over a decade in wireless and embedded systems

Move smoothly between articles as our pages load instantly.

A one-stop-shop for seeing the latest updates, and managing your preferences.

We brief you on the latest and most important developments, three times a day.

*Our Digital Subscription plans do not currently include the e-paper ,crossword, iPhone, iPad mobile applications and print. Our plans enhance your reading experience.

Support quality journalism - Subscribe to The Hindu Digital

Please enter a valid email address.

How an idea for a ‘perfect Mumbai feature story’ failed to materialise

Subscribe to The Hindu now and get unlimited access.

Already have an account? Sign In

Sign up for a 30-day free trial. Sign Up

Support The Hindu's new online experience.

Already a user? Sign In

END