Pegasus for Android: The Other Side of the Story Emerges

By Lookout

Published: 2017-04-03 · Archived: 2026-04-05 15:57:22 UTC

Today, Lookout and Google are releasing research into the Android version of one of the most sophisticated and targeted mobile attacks we've seen in the wild: Pegasus.

Read the full technical analysis here

A "cyber arms dealer" named NSO Group developed the Pegasus malware, which jailbreaks or roots target devices to surveil specific targets. Last summer, after being tipped off by a political dissident in the UAE, Citizen Lab brought Lookout in to further investigate Pegasus. In August 2016, Lookout, with Citizen Lab, published research about the discovery of the iOS version of this threat. What we discovered was a serious mobile spyware operation that has since been reportedly used to target Mexican activists, according to The New York Times.

Google calls this threat Chrysaor, the brother of Pegasus. For simplicity, we'll reference this as Pegasus for Android. Names aside, the threat is clear: NSO Group has sophisticated mobile spyware capabilities across a number of operating systems that are actively being used to target individuals.

Lookout enterprise and personal customers are protected from this threat.

Finding the threat

In the course of researching the iOS threat, Lookout researchers mined our comprehensive dataset and located signals of anomalous Android applications. We have sophisticated and valuable insight into what is happening in the mobile ecosystem at any given point in time. Without the Lookout Security Cloud, Pegasus for Android most likely would not have been found.

After looking into these signals, we determined that an Android version of Pegasus was running on phones in Israel, Georgia, Mexico, Turkey, the UAE, and others.

What it does

The Android version performs similar spying functionality as Pegasus for iOS, including:

- Keylogging
- Screenshot capture
- Live audio capture
- Remote control of the malware via SMS

- Messaging data exfiltration from common applications including WhatsApp, Skype, Facebook, Twitter, Viber, Kakao
- Browser history exfiltration
- Email exfiltration from Android's Native Email client
- Contacts and text message

It self-destructs if the software feels its position is at risk. Pegasus for Android will remove itself from the phone if:

- The SIM MCC ID is invalid
- An "antidote" file exists
- It has not been able to check in with the servers after 60 days
- It receives a command from the server to remove itself

It's clear that this malware was built to be stealthy, targeted, and is very sophisticated.

How it's different from the iOS version

The biggest distinction between the iOS and Android versions of Pegasus is the Android version does not use zero-day vulnerabilities to root the device.

In the course of researching the Pegasus for iOS, Lookout discovered three vulnerabilities Pegasus used to jailbreak the target device, and install and run the malicious software. We called these three "Trident."

Pegasus for Android does not require zero-day vulnerabilities to root the target device and install the malware. Instead, the threat uses an otherwise well-known rooting technique called Framaroot. In the case of Pegasus for iOS, if the zero-day attack execution failed to jailbreak the device, the attack sequence failed overall. In the Android version, however, the attackers built in functionality that would allow Pegasus for Android to still ask for permissions that would then allow it to access and exfiltrate data. The failsafe jumps into action if the initial attempt to root the device fails.

This means Pegasus for Android is easier to deploy on devices and has the ability to move laterally if the first attempt to hijack the device fails.

Contacting the target

Lookout alerted Google to the presence of the malware and worked with the Google Security team to understand the overall threat. Google has since sent a notification to potential targets with information about remediating the threat.

Anyone who believes they may have come into contact with Pegasus for Android or iOS should contact Lookout Support.

We have provided our full, technical research in a report Pegasus for Android:Technical Analysis and Findings of Chrysaor. If you are interested in the detailed story behind how we found Pegasus for Android and exactly what it does, read the full report here.
