



NSO Group & Pegasus



Overview

An investigation by 17 media organizations around that world has revealed that authoritarian governments, criminal and terrorist organizations have targeted executives, human rights activists, journalists, academics, and government officials for years. While there has been heavy speculation around this being the case, a data leak of more than 50,000 phone numbers revealed a list of identified persons of interest by clients of NSO since 2016. NSO develops Pegasus, a highly advanced mobile malware that infects iOS and Android devices and enables operators to extract specific GPS coordinates, messages, encrypted chats from apps like WhatsApp and Signal, photos and emails, record calls, and secretly turn on the microphone and camera.

Recommendation for Lookout Admins

The number and variety of individuals targeted by Pegasus shows that advanced spyware and surveillanceware isn't just the concern of governments. Lookout admins should make sure the default surveillanceware and device exploitation detection policies are turned on. They should set these alerts to high priority and block the device from accessing corporate resources until the issue is resolved.

In addition, admins should enable Lookout Phishing and Content Protection to protect against attacks that deliver malicious payloads via phishing links on various messaging platforms. This will protect both managed and BYOD devices from compromise before the connection can be made and the payload is executed.

Lookout Analysis

Since its initial discovery by Lookout and Citizen Lab in 2016, Pegasus has continued to evolve. It has advanced to the point of executing on the target's mobile device without requiring any interaction by the user, which means the operator only has to send the malware to the device. Considering the number of apps iOS and Android devices have with messaging functionality, this could be done through SMS, email, social media, third-party messaging, gaming or dating apps.

Mobile devices continue to be a primary attack vector for cyber criminals. Mobile malware, surveillanceware, and ransomware can take down infrastructure and track our every move as attackers target individuals where they are most vulnerable. Business executives with access to market data, technological research, and infrastructure are highly valuable targets. As iOS and Android devices continue to be integral to our lives, they need to be secured with as much, if not more priority than any other device.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

[Click here to learn more about Lookout Threat Advisory](#)