Predator & Pegasus

Overview

In the latest on state-sponsored mobile surveillanceware, two Egyptians were successfully targeted and spied on with both Predator spyware, which is developed by Cytrox, and NSO Group's Pegasus. Predator is a new piece of mobile surveillanceware that appears to use a similar attack chain as Pegasus and, like Pegasus, can target individuals on both iOS and Android. Predator is reported to be developed by the group Cytrox. They are part of Intellexa, which on its website says it's "an EU based and regulated company, with six sites and R&D labs throughout Europe" and is known to compete with NSO in the surveillanceware market.

In this case, Predator was delivered to the targets through a malicious WhatsApp link. After initialization is complete, both the iOS and Android versions of Predator call out for additional loader filed from the command-and-control server. Persistence doesn't appear to be an issue on Android, but on iOS Predator will download a function that takes advantage of iOS' shortcuts automation and triggers the exploit whenever one of 44 apps is opened. This is presumably how the spyware silently reinstalls itself in the background.

Lookout Coverage and Recommendation for Admins

To ensure coverage against these attacks, 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

The mobile surveillanceware market is growing with more opportunity for smaller groups or less-known groups to emerge. 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. 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