Lookout Discovery - AzSpy

Lookout is constantly discovering and researching new threats to protect and advise our customers

Background and Discovery Timeline

Researchers recently identified a small spyware family which appears to have been created by an Azerbaijani developer. While there are not many samples of this spyware to date, it appears to be part of a new commercial Android spy platform, known as FullSpy for Android, with a user login page to monitor infected devices. The malware pretends to be an application called "Google Services" with a replica Google icon, likely in an attempt to seem innocuous. However, the applications actually contain standard surveillanceware capabilities, and various commands give the actor control over the phone, allowing for exfiltration of sensitive data.

Key Facts

1. New commercial Android spyware
2. Can pull data about device location, storage, and phone number. It also has keylogging capabilities.
3. Could be distributed via phishing or URL shorteners

Capabilities and Affected Parties

The spyware can access the phone's hardware serial number, phone number, battery status, connection type, internal and external storage availability, network operator, GPS location, Android version, and whether the device is rooted. Additionally, it has keylogger functionalities for a hardcoded list of applications like Chrome, Firefox, and Yandex browser.

Aside from uncovering the login pages to manage infected devices, Lookout also discovered another part of the infrastructure that presents itself as a well-designed site to download a program advertised as "Smart Telegram for WordPress". This site is potentially a watering hole in progress, because while the APK can be downloaded from the site, it is not found through easily clickable links, but rather by knowing the appropriate file path. This could indicate that further development is still needed, or the app is potentially distributed via deep phishing links or URL shorteners.

How Lookout Detects and Protects Against Threats like AzSpy

Lookout Security Intelligence teams leverage both static and dynamic analysis with our machine learning engine to discover new threats. The market for commercial spyware is constantly growing and appeals to more than your standard user – it has been seen in targeted nation state attacks in the past as well. The Lookout team is continuing to monitor this family's capabilities and any new samples that may be ingested.

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 Threat Advisory