Lookout Discovery – Syrian Malware

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

Key Findings

1. Appears to have nation-state sponsorship from the Syrian government
2. 71 total apps were found in this campaign, all tied to the same C2 server
3. Malware delivered in malicious apps that were likely distributed via actor-operated watering holes or SMS download links.

Background and Discovery Timeline

In April 2020, Lookout released findings on a long-running surveillanceware campaign with ties to Syrian nation-state actors. The campaign appears to have started in January 2018 and targets Arabic-speaking users. Of 71 malicious Android apps tied to the command-and-control (C2) server, none were available on the Play Store, which indicates they were likely distributed via third-party app stores or actor-operated watering holes.

Tarassul Internet Service Provider, an ISP owned by the Syrian Telecommunications Establishment (STE) which has previously hosted infrastructure for the Syrian Electronic Army, owns the IP for the C2 server tied to this campaign. Tarassul also hosted the C2 server for SilverHawk, an Android malware family discovered by Lookout in the past. There is more evidence of nation-state sponsorship in the apps, which were not scrubbed of sensitive information. The apps show user-inputted names and version numbers, and repeated use of the alias "Allosh", which has been used by the Syrian Electronic Army in 22 other APKs.

Capabilities and Affected Parties

Campaigns that leverage watering hole attacks or SMS distribution are always evolving with current events. Focusing on universal interests, such as health during a pandemic, gives these types of attacks disproportionately high success rates. One app in this campaign pretended to take the user's temperature from a fingerprint while executing the malware in the background. The malware then gains access to:

- GPS Location - Installed Apps - Recording Audio - Taking Screenshots - Exfiltrating Contacts - Sending SMS - Creating Files

How Lookout Detects and Protects Against Surveillanceware Campaigns

Lookout Security Intelligence teams are continuously discovering and researching new threats to protect and advise our customers by combining static and dynamic analysis with our machine learning engine. Devices with Lookout installed can detect and be alerted to this specific campaign, and Lookout also protects against other sophisticated surveillanceware that could go undetected.

To learn more about the technical specifications of this campaign, including IOCs, read the full article here.

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