# Lookout Discovery - ArmaSpy

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

### Background and Discovery Timeline

Lookout researchers recently investigated the ArmaSpy surveillance family, which appears to have been targeting Iranian users since late 2016 with new samples discovered as recently as mid-2019. The interest in ArmaSpy came from the observation of the application's ability to create a unique contact on the user's device named HAMRAHAVVAL, the brand name of Mobile Telecommunication Company of Iran (MCI), as an attempt to blend into the user's device. Multiple Iranian phone numbers were associated with this contact in the various samples of the family and were discovered to be part of command and control infrastructure acting as designated SMS servers.

### Key Facts

1. Surveillanceware primarily targeting Iranian users. It's also capable of intercepting 2FA.
2. Found in malicious versions of Google, Flashplayer, and adult content applications.
3. Overlapping C2 infrastructure with OilRig threat group.

### Capabilities and Affected Parties

ArmaSpy's capabilities have increased over time, with the most recent samples containing 20 unique commands that one would expect from surveillanceware, such as retrieving browser history, downloading files, and taking a photo whenever the device is unlocked. Additionally, the actor can enable data usage and WiFi by simply sending SMS messages with predefined phrases in them. Those phrases can be customized per sample, likely allowing the actor to tailor the SMS messages to the target in order to avoid suspicion. A specific phrase over text also sets up a regex character sequence to detect digits in a string, theoretically allowing the malware to intercept 2FA codes the user might receive via SMS.

Primarily, ArmaSpy is found in malicious versions of apps such as Google, Flashplayer, and adult content apps. Interestingly, one of the C2 domains that ArmaSpy samples communicate back to resolves to an IP that simultaneously resolved to a domain that was part of known OilRig infrastructure, a threat group with suspected Iranian origins that has targeted Middle Eastern and international victims since 2014.

## How Lookout Detects and Protects Against Threats like ArmaSpy

Lookout Security Intelligence teams leverage both static and dynamic analysis with our machine learning engine to discover new threats. While ArmaSpy is a smaller and more targeted family, its unique heuristics and code structure are being analyzed against our data corpus of 170 million devices in order to get the most accurate understanding of the malware's presence and evolution. Devices with Lookout installed have been protected against ArmaSpy since May 2019. Lookout also protects against other sophisticated malware that could normally go undetected.

### 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