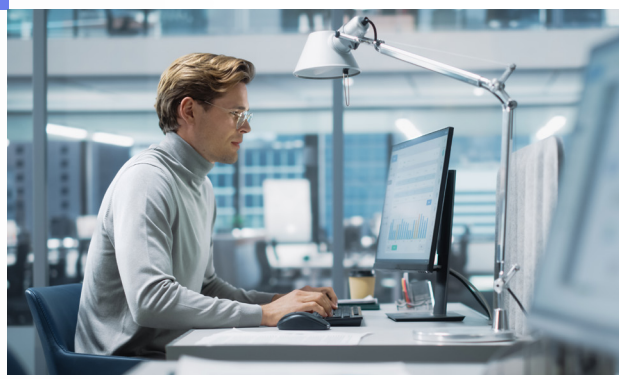
# Lookout Threat Advisory

## Your pass to cutting-edge mobile threat intelligence



### Overview

As more adversaries turn their attention to mobile platforms, keeping up with mobile threats has never been more important. Lookout is powered by the world's largest dataset that includes telemetry from over 190 million mobile apps and its analysis, and over 210 million devices running modern operating systems like iOS, Android, and ChromeOS.

Lookout is also home to the industry's leading mobile security researchers. Leveraging Lookout's data alongside insights from the Lookout Security Intelligence team will provide you with actionable intelligence on the latest mobile threats facing your organization.

### Offerings

Lookout Threat Advisory provides you with in-depth intelligence reporting, indicators of compromise (IOCs), and direct access to Lookout's mobile security researchers.

We offer a variety of packages that best suit your needs. These include access to the threat data that Lookout's own researchers use for threat hunting, comprehensive analysis of advanced malware, and bespoke research hours which you can leverage to fill your intelligence gaps on the mobile vector.

Governments as well as private organizations currently rely on Lookout to provide training on mobile threat hunting for their internal teams, and for exclusive intelligence on APT and nation-state activity undisclosed to the public.

| | Essential | Enterprise | Enterprise Premium | Enterprise Premium Plus |
|---|---|---|---|---|
| 12 mobile threat intel reports/year | ■ | ■ | ■ | ■ |
| Indicators of Compromise (IOCs) | ■ | ■ | ■ | ■ |
| Regional mobile threat data | | ■ | ■ | ■ |
| Mobile Threat Advisories | | ■ | ■ | ■ |
| Monthly status call | | | ■ | ■ |
| 100 hours of Virtual research/year | | | ■ | ■ |
| Application binaries and PCAPs | | | | ■ |
| 1 threat hunting workshop/year | | | | ■ |
| Additional custom deliverables as agreed | | | | ■ |

### Benefits

**Intelligent risk management**

Know what prevalent threats to focus on in order to make better informed security risk management decisions.

**Get ahead of the attackers**

Early visibility into mobile threat trends enables you to take protective steps before attacks occur. Lookout researchers actively identify cross-platform mobile and desktop malware campaigns. They provide actionable information such as IOCs in STIX 2 format that you can use to improve your mobile security strategy and overall security posture.

**Build stronger business cases**

Use quantified risk data to demonstrate the relevance of mobile threats and gain support for mobile security initiatives across your organization.

**Secure mobile infrastructure**

For mobile network operators and organizations responsible for the security of entire mobile fleets, Lookout Threat Advisory services offer critical, actionable insights that allow you to make better investments in protecting your mobile infrastructure.

## Monthly global threat report

As part of Lookout Threat Advisory services, Lookout provides a monthly mobile threat report. This in-depth intelligence report provides complete context on multiple APTs, nation state and crimeware campaigns conducted using mobile malware. The report provides malware reverse engineering analysis, command and control IOCs, targeting, OSINT details, and attribution when achievable.

BouldSpy

Lookout researchers discovered an Android surveillanceware family that Lookout has named BouldSpy. Lookout researchers assess with moderate confidence that BouldSpy is employed by FARAJA (Law Enforcement Command of the Islamic Republic of Iran) to surveil victims with activity from 2020 to 2022. BouldSpy collects a wide variety of information from its victims, including accounts, files, contacts, call logs, SMS logs, microphone recordings, call recordings, screenshots, photos taken from the camera on command, keylogs, location, network and device information, clipboard content, browser history, and installed apps. BouldSpy can remotely enable or disable Wi-Fi, encrypt arbitrary files, take photos, take screenshots, take audio recordings, open arbitrary web pages via browsers on the device, attempt to gain admin rights, change passwords on enumerated accounts, or send SMS messages.

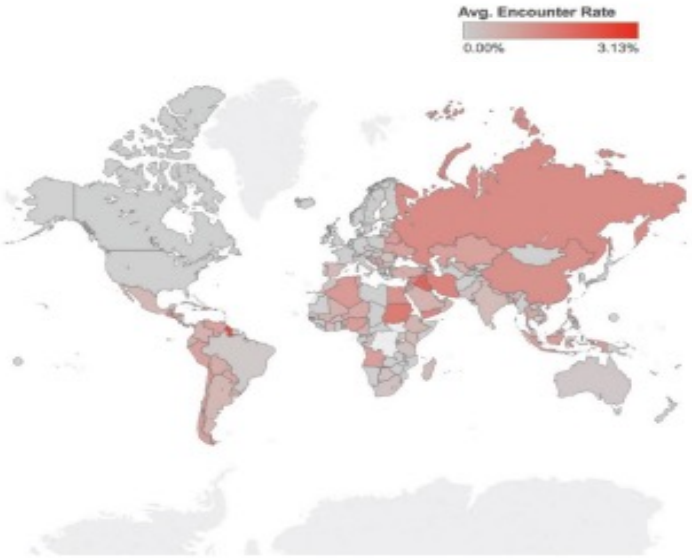
BouldSpy appears to be fairly early in development based on the relatively small number of samples as well as operational security oversights such as unencrypted command and control (C2) traffic, hardcoded plaintext C2 infrastructure details, a lack of string obfuscation, failure to conceal or remove intrusion artifacts, or others.

**Overview**
A BouldSpy sample from September 2022 trojanizes a legitimate Android CPU benchmarking app named CPU-Z, developed by French company CPUID1. The sample, 5168610b73f50661b998e95a74be25bfe749b6ef, implements the CPU-Z app's intended functionality, while running surveillance actions in the background within packages com.android.call service.core and com.android.callservice. manager. These packages are common across all the newer BouldSpy variants, with older test versions (such as 75a6c724f43168346b177a60c81ca179a436246f) simply named com.android.callservice without trojanizing legitimate applications. BouldSpy is named for a class called BoulderApplication which contains C2 , locale, and SSL configurations. Lookout researchers discovered three other trojanized BouldSpy samples sharing the same com.android.callservice package and the same C2 websocket, http://192.99.251[.]51:3000.

These samples are shown in the table below.

| Package Name | App Title | SHA-1 |
|---|---|---|
| ir.andromedads.interestcalculator | محاسبه سود و وام | af999714aec75a64529c59f1e8de4c669adfa97a |
| ir.andromedads.interestcalculator | محاسبه سود و وام | 965d118cb80ccdbc6e95e530a314cb4b85ae1b42 |
| com.devnied.currency.pro | Currency converter pro | f3b135555ae731b5499502f3b69724944ab367d5 |
| com.devnied.currency.pro | Currency converter pro | 43a92743c8264a8d06724ab80139c0d31e8292ee |

***Table 1:*** *List of trojanized BouldSpy samples*




Lookout researchers actively track over 130 malware families tied to more than 65 APT and nation-state threat actors, as well as more than 1,200 crimeware and commodity families. On average, we identify mobile APT malware and campaigns six months before public disclosure by other entities. In many cases we provide exclusive intelligence on threats that are both undetected and unattributed by other threat intelligence organizations.

## Customized to fit your needs

In addition to our monthly reporting, Lookout Threat Advisory offers customization options such as virtual research hours, in-person workshops, and access to malware binaries and packet capture data to truly augment your security team's capabilities.

This catered service provides high quality IOCs and direct access to our mobile experts to minimize false positives and enable your team to focus on what really matters. Our personalized offering acts as a force multiplier for your SOC or threat intelligence team by providing the mobile perspective with necessary resources and training opportunities to enable them to deal with mobile threats confidently.

## Why Lookout?

Lookout Mobile Endpoint Security ensures continuous security and compliance on every device, leveraging a large data set fed by more than 215 million devices, and the analysis of over 190 million mobile apps. Lookout empowers your organization to adopt secure mobility without compromising productivity by providing the visibility IT and security teams need. To learn how you can secure your mobile fleet today, contact us at sales@lookout.com.

Lookout®

## About Lookout

Lookout, Inc. is the endpoint-to-cloud cybersecurity company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo