Lookout

Mobile Risk Assessment Report for Anonymous

Prepared by Ryan Nappi Sep 15, 2015 2:22:54 PM

Anonymous

140

App-based threats encountered.

46

Threat families encountered.

METHODOLOGY

We analyzed app-based threats encountered by Lookout's global sensor network of over 70 million mobile devices, as well as the IP connections and OS versions of these devices. Using publicly-available Autonomous system (AS) numbers, Lookout correlated IP connections to AS numbers belonging to your organization, revealing mobile devices and Lookout users accessing your network(s) who have also encountered threats on their mobile devices. Please note:

Privacy

This data was aggregated anonymously and does not identify individuals

Network Security

Lookout did not infiltrate or otherwise compromise your network to obtain this data

122.77.169.**

IP Connections

IPs associated with your network(s) resulted from the network connections of both Lookout-enabled mobile devices as well as devices used by Lookout users to log-in to their accounts

Ultimately, this report reveals the app threats and potential OS threats facing mobile devices associated with your network.

APP THREATS

Lookout broadly classifies app threats using the following risk spectrum:

▲

Low Risk

- Accesses and/or exfiltrates minimal device identifier data.

◆

Medium Risk

- Exfiltrates and/or accesses device identifier data and personally identifiable data.

⬢

High Risk

- Exfiltrates and/or accesses device identifier data and personally identifiable data.
- May compromise the integrity of data encryption.
- May compromise the integrity of network security measures.

We recognize that each organization may have unique risk tolerances based on data sensitivities and compliance requirements. Lookout can work with your organization to tailor risk scoring to your specific needs.

APP THREAT ENCOUNTERS

The following app-based threats were encountered by Lookout-enabled mobile devices that either connected to your organization's network or belong to a Lookout user who connected to your network on another device.

Lookout's consumer mobile security application has a 95% self-remediation rate within 24 hours of threat encounters, so while possible, it's unlikely that these app threats were active when a device connected to your network(s). However, these devices represent only a tiny fraction of your total mobile network traffic and should serve as a baseline to understand security risk facing mobile devices on your network that are not currently protected by Lookout.

Encounter Rates by Threat Family

Risk ▼	Family	Prevalence	Risk Profile
⬢	**ActSpat** Trojan	2 devices	This application uses an ad network that will show intrusive advertisements, put shortcuts on the device's home screen, and download large files in the background. It can also send some of the user's personal information to the ad server. This can make the device run slower, use large amounts of data, and invade the user's privacy.
⬢	**AppzosThief** Trojan	1 devices	This is a legitimate application which has been modified by a third party. It collects the users WhatsApp password and contacts and sends it to a third party. This can cause sensitive information to be shared with a third party.
⬢	**TowelExploit** Exploit	1 devices	This application contains code to bypass a device's security. If the user runs this app, it may cause unwanted behavior. It is also commonly included in apps designed to give the user root permissions which may be desired by the user.
⬢	**ScarePakage** Trojan	3 devices	This application appears to be legitimate, but it is malicious. It will take control of the device, making it difficult to use any apps or to uninstall unless the user sends payment to a third party. This can make the device unusable and result

			in fraudulent charges to the user.\n
⬢	ScareMeNot Trojan	2 devices	This application pretends to be legitimate, but it is malicious. It will take control of the device, making it difficult to use any apps or to uninstall unless the user sends payment to a third party. This can make the device unusable and result in fraudulent charges to the user.
⬢	RuPaidMarket Trojan	1 devices	This app will send premium SMS without notifying you. This may cause unwanted charges on your mobile phone bill.
⬢	Fakebrows Trojan	1 devices	This program will incur premium SMS charges to download a free app.
⬢	NotCompatible Trojan	2 devices	This application claims to be a system update on installation. Instead the app will use your phone as a network proxy, allowing remote servers to send and receive traffic through your device.\n
⬢	MSpy Surveillance	1 devices	When this app receives a specially crafted SMS code, it dials a configured number, allowing the attacker to listen to audio at your phone's location. The app also allows the installer to read your text messages and emails and remotely lock or wipe the contents of your phone. If you weren't aware that this app was installed on your phone, Lookout recommends you remove it.
⬢	MadCongregant Trojan	2 devices	This application looks like a media player, but it is not. It will take over the device and claim to be law enforcement to scare the user into paying a fake fine. This can result in inability to use the device and financial loss.
⬢	JammedCart Trojan	1 devices	This application seems to be legitimate, but it is injected with malware. It runs secretly in the background and subscribes you to monthly premium services without your knowledge. This can cause unwanted charges on your phone bill.
⬢	Koler Trojan	3 devices	This application claims the device was used in some illegal activity. It prevents regular use of the device and attempts to extort money from the user to remove the application.
◆	JackeeyWallpaper Spy	1 devices	This app sends identifying information about you and your phone to a third-party server. This information includes your phone number, voicemail number, SIM card serial number, and device details.
◆	IZP Spy	2 devices	This app contains functionality to collect your browser history each time an ad is displayed and send it to a server over the Internet. This app can only do this if it has the appropriate permission to read your browser history. If it does, you may wish to uninstall this application.
◆	SofterSpy Spy	1 devices	This application looks like a system update, but is used to spy on the user. This application collects device location data, sms messages, call logs, emails, contacts, and files and sends them to a third party. It also has some basic ability to control the device, including allowing a third party to open the browser to a specific webpage. This can result in a loss of privacy.
◆	TowelRoot Root Enabler	4 devices	This application enables privileged access to the device, also called root. Root gives the user and installed apps access to actions that are normally restricted. This can allow the user or apps to modify the Android system in ways that can potentially damage a device or cause a loss of private data.
▲	SendDroid Adware	5 devices	This application may contain the SendDroid ad network. It may create "push" notification ads that appear in your notification bar, and may place shortcuts on your phone's home screen. It may not be clear to you that this application may be making these changes or displaying these ads.
▲	NULL Adware	1 devices	This pretends to be a legitimate application, but it is not. The application will secretly send device information and text messages to a third party. This can result in a loss of privacy.\n
	AdultFreedom	2 devices	This media application appears to be legitimate, but it is malicious. It will sign

▲	Toll Fraud		the device up for a content subscription without sufficient notification. This can result in unexpected charges on the device's bill.
▲	**Pirator** Toll Fraud	1 devices	This application sends private information to a third party, and may subscribe the user to premium text message services without notification. This can cause unexpected charges on the device's bill.
▲	**PlusTV** Chargeware	1 devices	This application will send premium SMS messages which will cost you money. These SMS messages may be sent without notifying you or asking for your permission. You should remove this application from your device.
▲	**RevMob** Adware	17 devices	This app may contain the RevMob ad network. It may create "push" notification ads that appear in your notification bar. It may not be clear to you that this application is creating these ads. It also may send personally identifying information, such as your email or IMSI, to RevMob's servers.
▲	**DoubleDip** Adware	2 devices	This application gives the user access to free apps that may contain malware or other adware. This app will require the user to allow ad networks to make changes to their device without adequately informing the user. It also asks for personal information without providing a privacy policy. This can cause undesired changes to the user's device and unknown use of the user's personal information.
▲	**CusmoPreload** Riskware	1 devices	This is a pre-loaded system application. It allows the device to be controlled by a remote configuration file including executing system commands, installing and uninstalling apps, killing processes, and restarting the device. This can result in a disruptive user experience.
▲	**CompromisedKey** Riskware	35 devices	This application has been signed using a compromised or debug key, which means its origin or authorship is unknown.
▲	**LetangPushAd** Adware	1 devices	This ad network is loaded as dynamic code and pushes ads to the notification bar. There are properties files that indicate the potential to charge money to the user on clicking, though no actual charges have yet been detected. Permissions on detected assessments also suggest they intend to push icon ads in the future.
▲	**SMSCapers** Chargeware	13 devices	This application appears to be an app for viewing sets of pictures or videos for 5 RMB per day. These charges may not be made clear within the app, and may result in unwanted charges on your mobile phone bill.
▲	**MoolahMedia** Adware	2 devices	This app may contain the Moolah Media ad network. It may create "push" ads that display in your notification bar, and it may not be clear to you that this application may be creating these notifications.
▲	**SwfScam** Adware	2 devices	This application tries to trick you into installing other apps. It will not provide this promised content and is instead stuffed with advertising networks.
▲	**BackgroundFace** Adware	1 devices	This pretends to be a legitimate flashlight application, but contains malicious functionality. It will secretly root the device without the user's consent. This exposes the device and the user to a greater risk of other malicious activities.
▲	**LeadBolt** Adware	17 devices	This application may contain the LeadBolt ad network. It may create "push" notification ads that appear in your notification bar, may change your browser settings or homepage, and may create shortcuts on your phone's home screen. It may not be clear to you that this application may be making these changes or creating these ads.
▲	**Winkie** Adware	2 devices	This app contains an ad network that may store and report details about calls you make to a third party server. It reports the number called, the time the call was made, and how long the call lasted for calls to specific numbers from a list provided by the server. It also uses your IMSI to identify you to the server. The IMSI is sent unencrypted over the internet.

▲	**ArmorForAndroid** Chargeware	2 devices	This is a device optimization app that uses misleading threat alerts to convince users to pay for an upgraded version of the app. The payment notice is unclear about the frequency of recurring charges for the service, which can be as often as once a day. This can result in unexpected charges on the user's credit card statement.
▲	**NoMiembros** Chargeware	1 devices	This application may not provide clear notification to the user when charging for its content. This can result in unauthorized purchases on the user's behalf.\n
▲	**Ikangoo** Chargeware	1 devices	This application will register your device with a remote server and send SMS messages to a premium number without explicit warning. This may result in unwanted charges on your mobile phone bill.
▲	**Appayable** Adware	4 devices	This application contains an ad network which collects your personal information, including but not limited to device ID, IMSI, email address, installed applications, phone number, and location. That information will then be sold to third parties in order to target ads at you.\n
▲	**PigPayer** Chargeware	1 devices	This application is a media player. It will send premium text messages without user consent. This can result in unwanted charges on the device's bill.

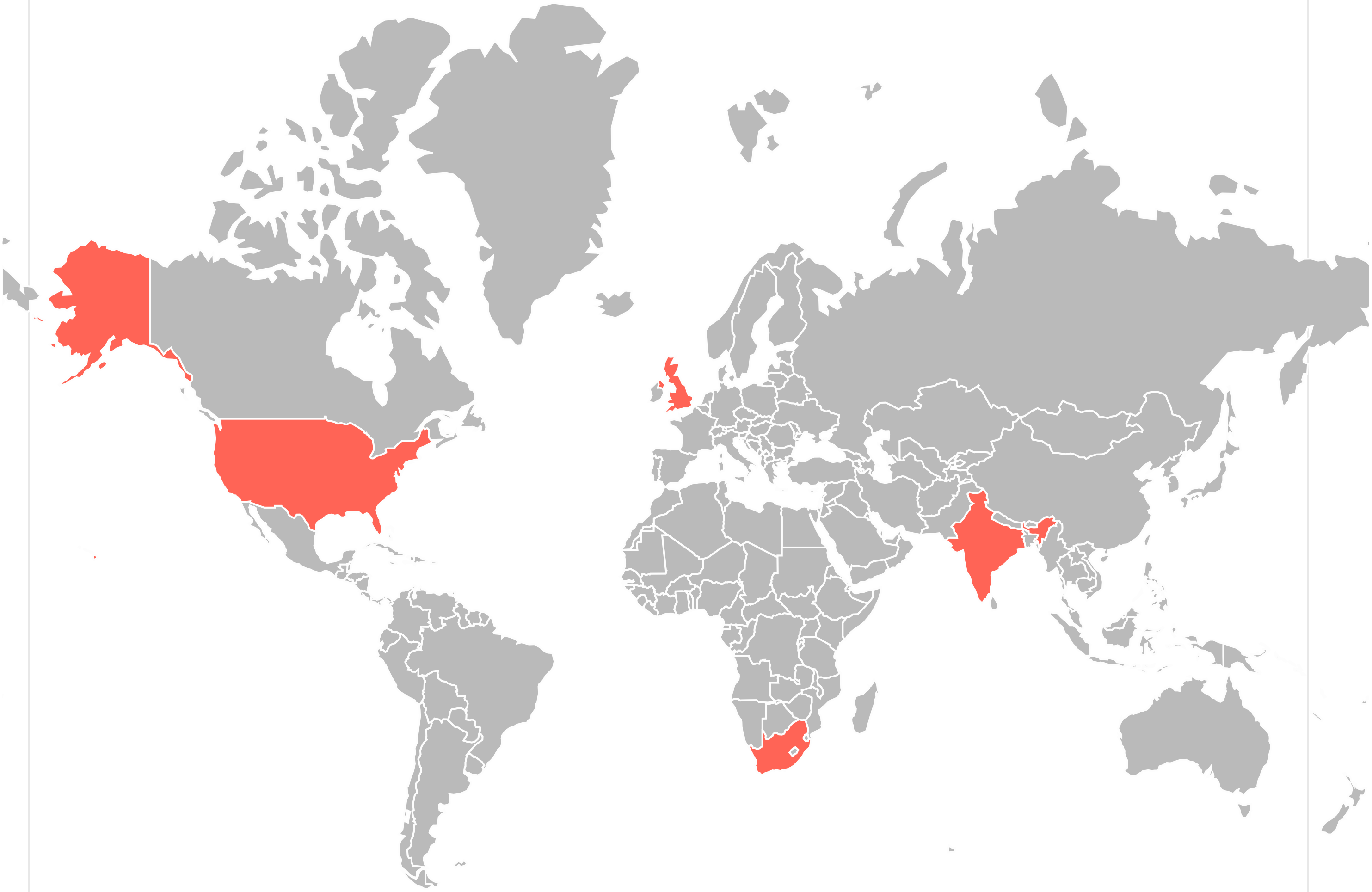
DATA LEAKS

Apps collect and transmit sensitive data to servers hosted in a wide range of geographies, raising the possibility that these exfiltration events may violate not only organizational security policy, but data protection laws as well.

Apps documented in this section exfiltrated contact and GPS location data to servers hosted in the following countries:

Server Locations for App Exfiltration of Contact and GPS Data

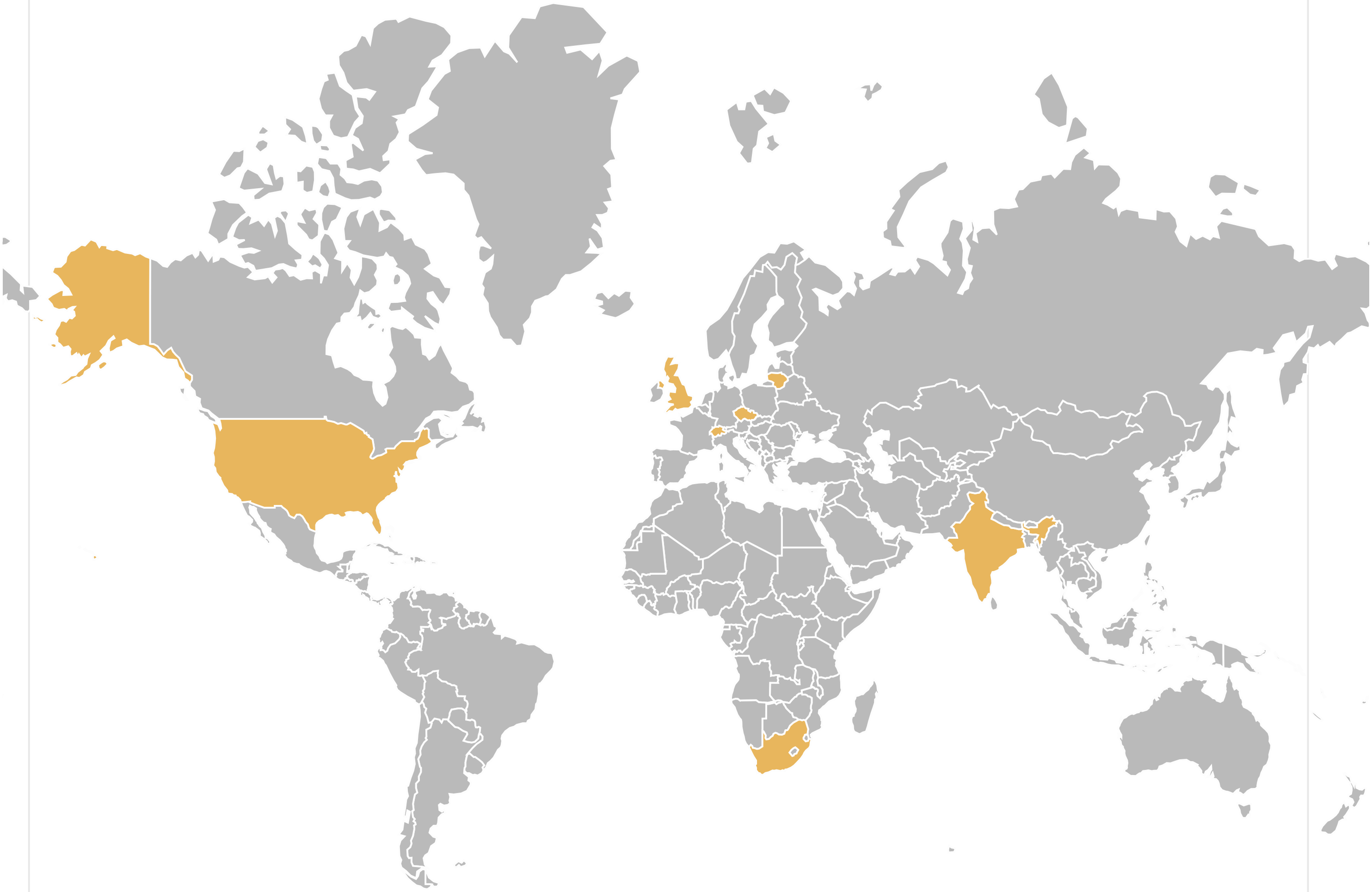
Contact Data Exfiltration



Server Locations

United States	28
South Africa	12
United Kingdom	9
India	6
Grenada	1

GPS Data Exfiltration



Server Locations

United States	234
United Kingdom	134
South Africa	62
India	12
Singapore	11
Grenada	7
Switzerland	4
Lithuania	4
Czech Republic	2

OS THREATS

Outdated operating systems may present security vulnerabilities that attackers can exploit to compromise the integrity of a device. Please note, an outdated OS version alone does not necessarily indicate device vulnerability, nor does a more recent OS version preclude attacker exploitation.

iOS Device Versions Associated with your Network(s)

OS	Version ▼	Prevalence	Prevalence Meter
🍎	8.4.1	78.13%	▬▬▬▬▬▬▬▬
🍎	8.4	3.13%	
🍎	8.3	3.13%	
🍎	8.1.1	3.13%	
🍎	7.1.2	12.50%	▬

Potential iOS Vulnerabilities

Name	Affected Version(s)	Description
Masque vulnerability	7.1.1, 7.1.2, 8.0, 8.1	This vulnerability could allow attackers to compromise jailbroken and non-jailbroken iOS devices (via provisioning profiles), replacing apps on compromised devices with trojans without detection by using the same app bundle identifier, since vulnerable iOS versions cannot identify the difference.

Android Device Versions Associated with your Network(s)

OS	Version ▼	Prevalence	Prevalence Meter

5.1.1	20.00%
5.1	2.86%
5.0.2	7.14%
5.0.1	12.86%
5.0	15.71%
4.4.4	7.14%
4.4.3	1.43%
4.4.2	12.86%
4.3	5.71%
4.2.2	4.29%
4.1.2	2.86%
4.1.1	1.43%
4.0.4	2.86%
2.3.5	1.43%
2.3.4	1.43%

Potential Android Vulnerabilities

Name	Affected Version(s)	Description

AOSP browser vulnerability	4.3 and older	This vulnerabilty affects the Android Open Source Project's (AOSP) browser and derivative mobile browsers that use AOSP's code. By directing users to a malicious webpage, it could allow attackers to access data in other open webpages in the browsing session and even hijack session cookies and take control of an online account.
Master Key vulnerabilty	4.3 and older	This vulnerability could allow attackers to modify .APK files (apps) without breaking their cryptographic signature, giving attackers the ability to maliciously update apps on devices and evade detection on devices with vulnerable OS versions