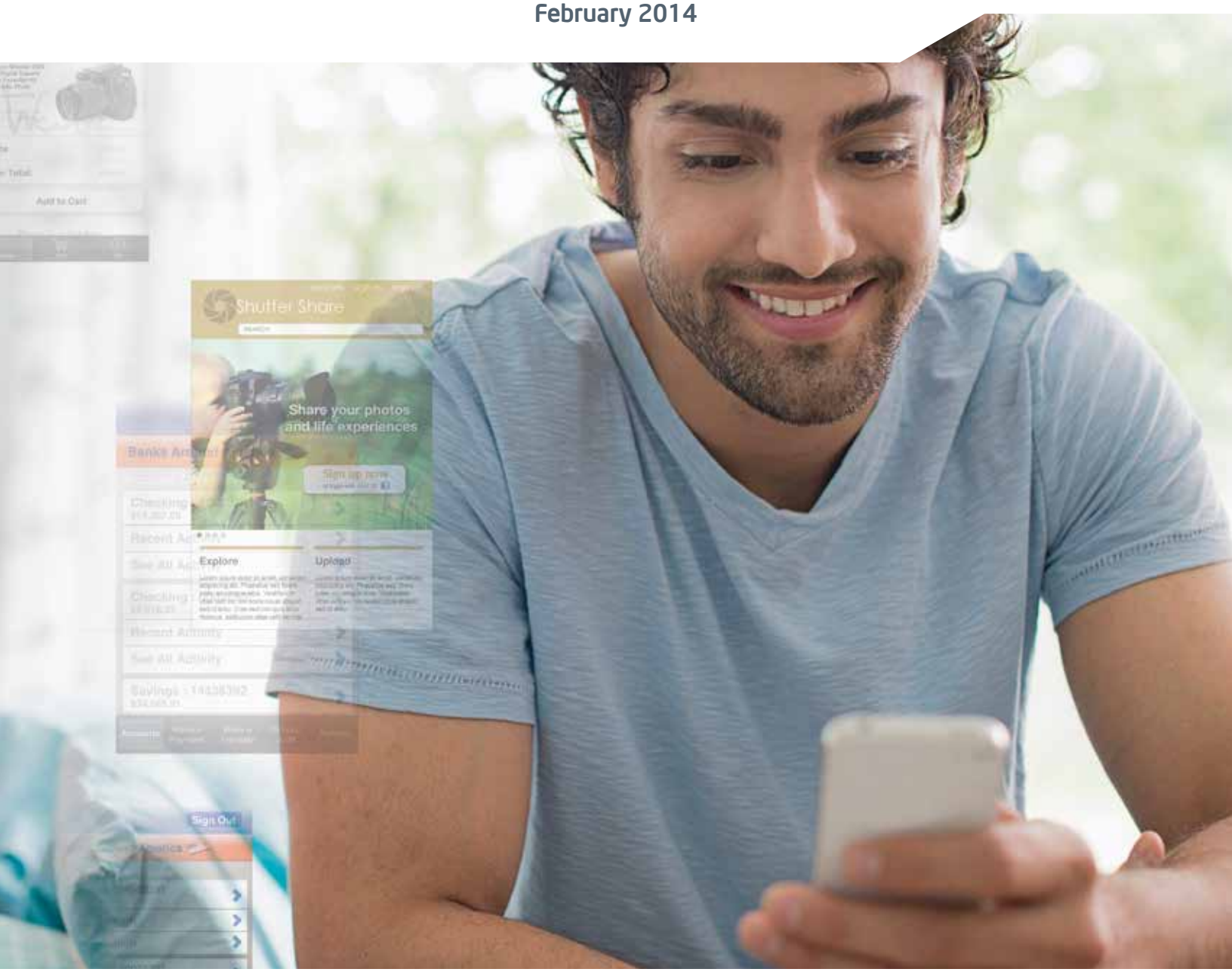
Who's Watching You?

McAFEE MOBILE SECURITY REPORT

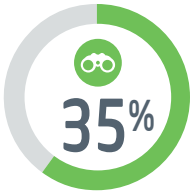
February 2014



intel Security

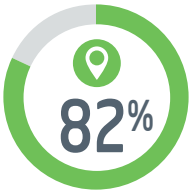
Table of Contents

MALWARE IS FAR MORE LIKELY
than the average app to collect what tasks and apps you are using, plus your phone and SIM card numbers



OF THE MOST PRIVACY-THREATENING APPS
also contain malware

ANDROID MALWARE ALMOST TRIPLED
from 2012 to 2013, with more collection of handset information, premium SMS scams, fraud, downloaders, and installers



OF APPS TRACK YOU
they know: when you use Wi-Fi and data networks, when you turn on your device, and your current and last location

ON THE UPSIDE, ROOT EXPLOITS HAVE FALLEN, perhaps because operating systems are getting more secure

Overview

In this third mobile security trends report, McAfee finds that privacy-invading apps dominate the landscape, some containing malware, and many leveraging ad libraries. As we analyzed the behavior and permissions of thousands of Android apps, we found that 82% of apps track you, and 80% of apps collect location information.

These apps might be considered today's personal "Space Invaders." However, privacy is an individual concept. The perception of privacy changes depending on your culture, age group, disposable income, and technology comfort level. So we looked at the scores and worked to identify the apps that seem to be the most aggressive about data collection.

While ad libraries may serve legitimate business purposes, subsidizing content that consumers want, they can also facilitate over-sharing of information with mobile apps. In a few cases, they go hand in hand with malware. We found that Adsmogo and LeadBolt are two ad libraries that we found seldom appear without malware. However, as with successful app stores, malware authors include successful ad libraries because of the volume of users. We should not conclude that ad libraries are innately bad.

Malicious software isn't just distributed in apps. It also comes in websites and emails. Premium SMS Trojans, FakeInstaller, and AdWoLeaker remained the most prevalent problems in the second half of 2013. Over the last year, we have tracked a gradual increase in invasive attacks, including data and SMS fraud.

We've learned about these trends as we have helped keep people safe. McAfee® Mobile Security continues to block risky downloads, scan files for malware, locate lost phones, and block undesired content including spam, malicious text messages, and nuisance calls.

The Stakes are High

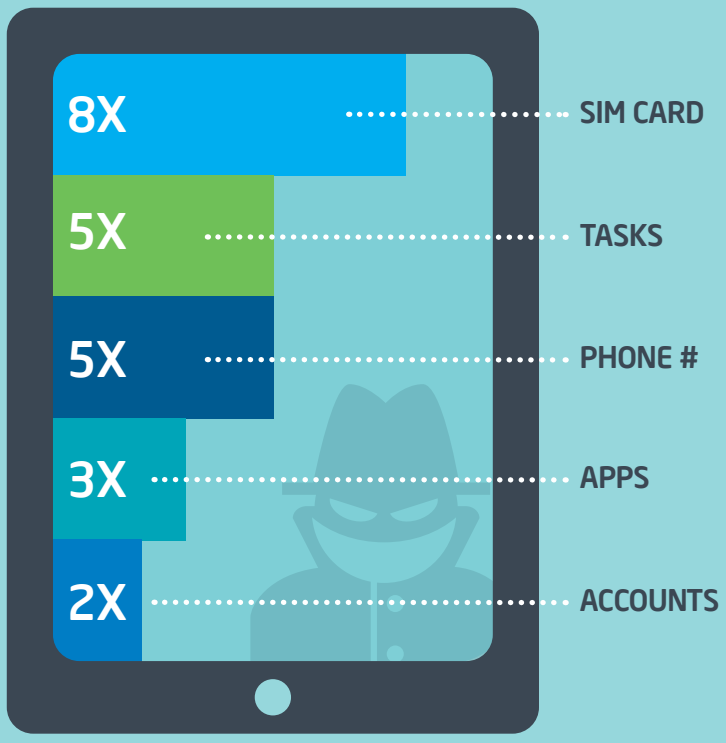
Your mobile device can share all sorts of personal information about you—with honest businesses and with criminals.

82% OF ANDROID APPS and 100% of malware track your network use, when you use your device, and your location

35% OF THE MOST privacy-threatening apps also contain malware

MALWARE IS FAR MORE LIKELY than the average app to collect invasive information: what tasks and apps you are using, plus your phone and SIM card numbers

HOW MUCH MORE VALUABLE IS YOUR DATA TO A CRIMINAL THAN AN HONEST DEVELOPER?



CHOOSE WISELY

THESE ARE SOME OF THE PERMISSIONS TO WATCH

GET_TASKS
Why? To eavesdrop on your life, or evade defenses

READ_PHONE_STATE
Why? To track you—and their bot clients—through your device

ACCESS_FINE_LOCATION or ACCESS_COARSE_LOCATION
Why? To pinpoint you and track your travels

GET_ACCOUNTS
Why? To manage accounts so they can log in or authenticate to certain accounts

READ_SMS or RECEIVE_SMS or RECEIVE_MMS OR SEND_SMS
Why? To commit fraud or steal from your bank

4 OUT OF 5
APPS WANT TO KNOW
WHERE YOU GO

What Have You Got to Lose?

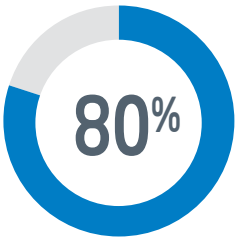
We looked at how often apps track you, your device, and your personal life. Of the things apps can track, location may be the most intimate information these apps collect.

- Your exact location (GPS, longitude, and latitude)
- Your general location (Wi-Fi or cell tower)
- Your last known location

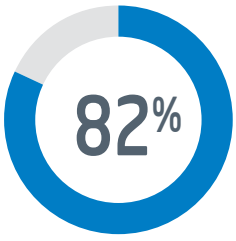
APPS COLLECT YOUR INFORMATION

MOST APPS COLLECT DETAILED INFORMATION ABOUT WHERE YOU GO AND WHAT YOU DO WITH YOUR DEVICE

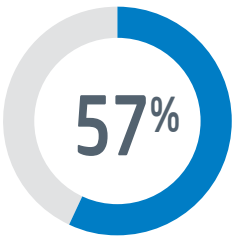
82%	64%	59%	55%	26%	26%
READ YOUR DEVICE ID	KNOW YOUR WIRELESS CARRIER	TRACK LAST KNOWN LOCATION	CONTINUOUSLY TRACK LOCATION	READ THE APPS YOU USE	KNOW YOUR SIM CARD NUMBER



COLLECT LOCATION

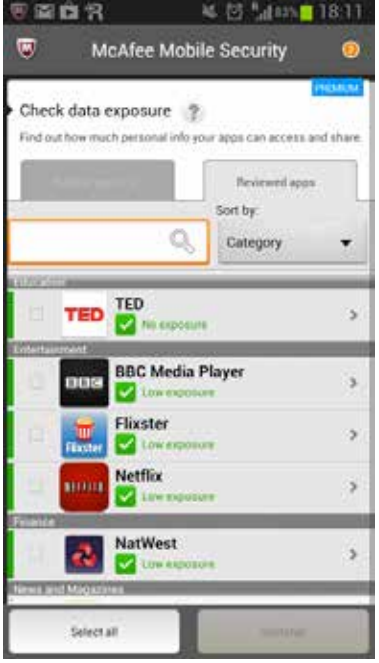


TRACK SOMETHING

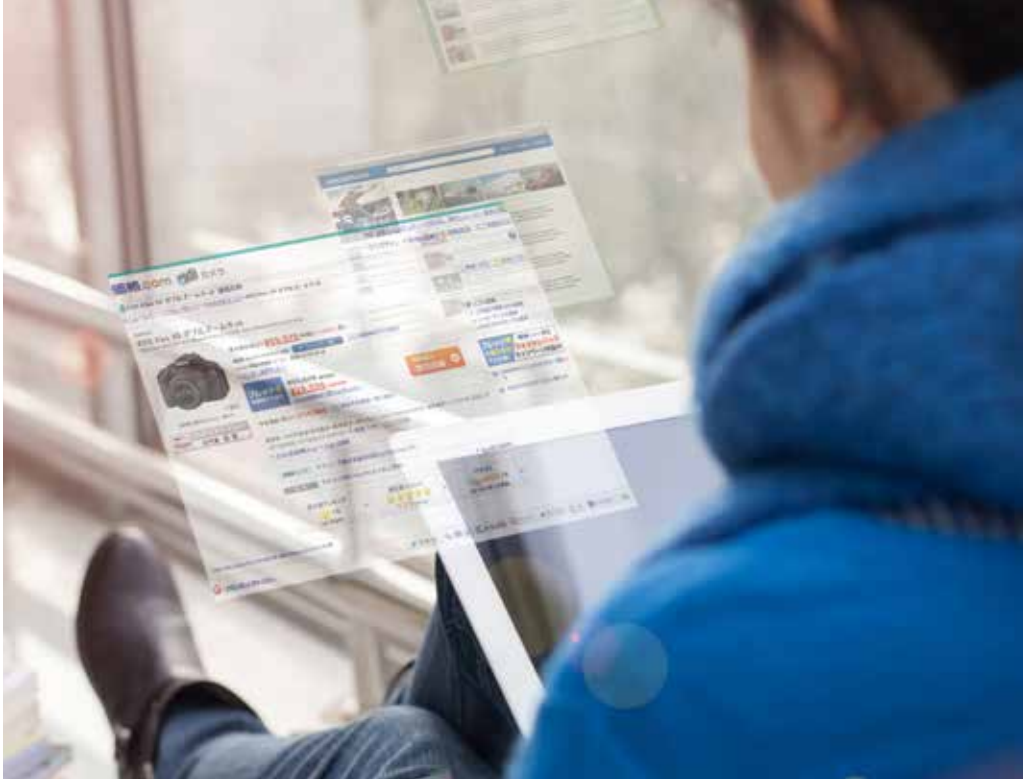


TRACK WHEN YOU USE YOUR PHONE

36%
KNOW YOUR ACCOUNT INFORMATION



McAfee Mobile Security users can see details on app sharing behavior



Is Your App Over Sharing?

The McAfee mobile research team has a scoring system to evaluate these data invasions. Of course, some apps need some of this information, so we consider the app category and other data points before we worry—or tell you to worry—too much.

McAfee maintains a reputation database for mobile apps. When an app behaves significantly differently than others in its category, we may increase the riskiness reflected in its privacy "sharing" score. The higher the score, the more private data it shares. A low score, within each category and for each app, means the app collects very little information or behaves the way a user would expect it to, based on the description of the app.

We think these are the most worrisome permissions:

- **Apps that read your subscriber ID** from your device (vs. device utilities that do so or apps that read just your IMEI, which isn't tied to you)
- **Anything that gets your precise location** (vs. Wi-Fi network or cell tower)
- **Anything that reads or tracks text messages**, which can contain private messages and online banking transaction authorization numbers

TECH TIP

Many apps use your unique device identifier (IMEI, MEID, ESN, or IMSI) to track you—and their bot clients—through your device. Watch for an app requesting the READ_PHONE_STATE permission. Starting with Android OS 1.6 (Donut), apps must explicitly ask for this permission.

Space-Invading Apps

When we dug into the Top 10 most space-invading apps in our collection—those with sharing scores of 20 or higher—we found they all:

READ YOUR DEVICE ID

TRACK YOUR LAST KNOWN LOCATION

KNOW YOUR SPECIFIC LOCATION

KNOW YOUR WIRELESS CARRIER

These details add precision to geographic tracking, placing a device and its user in a specific location. This information can legitimately be used by ad libraries to geo-target ads. However, for spyware, it provides location data that crooks add to other stolen data to expand their profile of the victim. We also believe this data helps botnets keep track of their bots.

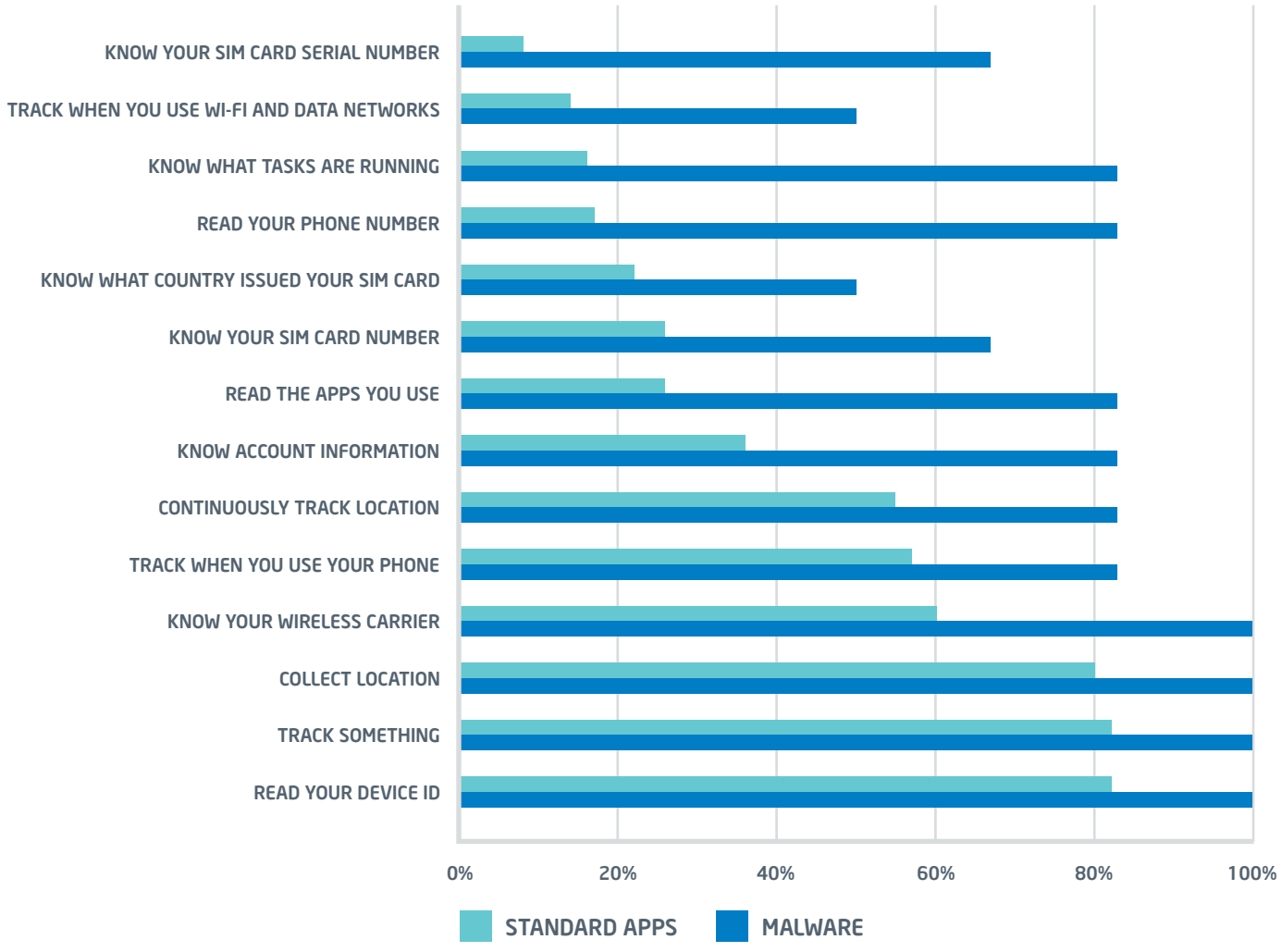
Aggressive Data Collection + Malware

While we have many privacy-invading apps, a relatively small number also contain malware. Malware includes Trojans that can download other software or perform unwanted activities without your consent, and suspicious programs, such as spyware.

We used our research data to see what was different between collections of malware and the world of mobile apps generally. We saw some big differences!

MALWARE COLLECTS MORE

MALWARE IS MUCH MORE LIKELY THAN A STANDARD APP TO MONITOR YOUR TASKS AND APP USAGE AND COLLECT IDENTIFYING INFORMATION.



Malware uses the most common abusive permissions. In addition, malware is far more likely than generally-abusive apps to:

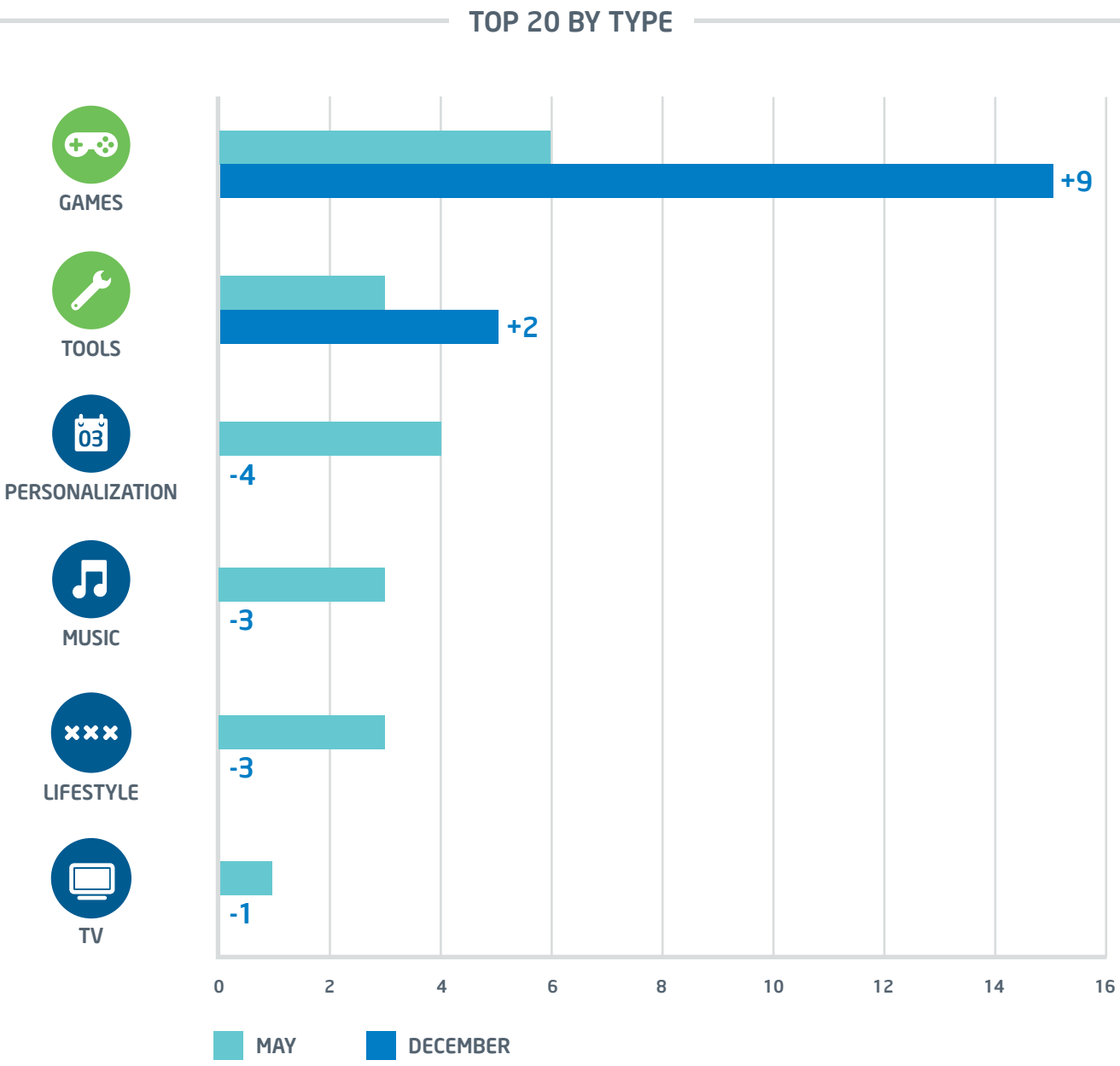
- Know what tasks are running
- Read your phone number
- Know your SIM card serial number
- Know the apps you use

This information might help a bot herder, an attacker running a botnet, to keep track of all his individual bots. The serial number gives a unique identifier to each device. The phone number gives an idea of the geographic region for the infected device, as well as the ability to contact the victim, for example through a spam SMS message.

Knowledge of the apps and running tasks would be useful if the botnet owner wanted to see if antivirus software were installed, or otherwise profile the victim and harvest more information. If he can discover antivirus software, for example, he can then tell his malware to maneuver around or interfere with that defense.

Which Apps are Abusing?

When we compared today's top malware to our previous report, we found games dominated any opposition, and tools had become a popular tool for attackers. No other category was relevant.



WHICH APPS ARE ABUSING?

The higher the score, the more data the app collects.

What does the malware do? Suspicious means it misbehaves, a PUP is a nuisance program or spyware, a Trojan usually installs other malware.

Behavior outside what is normal for its category gets our attention.

APP NAME (PACKAGE)	PRIVACY SCORE	MALWARE CLASSIFICATION	CATEGORY NAME	CATEGORY SCORE
com.sr.DeathSniper02	26	Suspicious	Games	7
com.kamitu.drawsth.standalone.free.android	25	Suspicious	Games	8
com.omgbrews.plunkunlockedIt	25	Suspicious	Games	8
com.bslapps1.gbc	21	Suspicious	Games	7
com.idoing.sniper	21	PUP	Games	7
vStudio.Android.Camera360	21	Suspicious	Tools	7
com.spy.camera.proversion	20	PUP	Tools	9
com.rechild.advancedtaskkiller	17	Suspicious	Tools	4
com.topsurgerygames.Knee.Surgery	17	Trojan	Games	7
com.bestcoolfungames.antsmasher	16	Trojan	Games	7
org.orangenose.games	14	Suspicious	Games	9
com.feelingtouch.gnz	13	PUP	Games	7
com.feelingtouch.gnz.realistic	13	PUP	Games	7
com.feelingtouch.zombiex	13	Suspicious	Games	7
com.stargames.volume.booster	13	PUP	Tools	9
com.outfit7.talkingtom2free*	12	Suspicious	Games	7
com.outfit7.tomlovesangelafree*	12	PUP	Games	7
com.outfit7.talkingnewsfree*	9	PUP	Games	7
com.solverlabs.worldcraft	9	Suspicious	Games	7

* These are malicious, "trojanized" versions of popular legitimate apps, so the package names are the same as the honest ones.

50% OF THE TIME, LEADBOLT IS ASSOCIATED WITH MALWARE

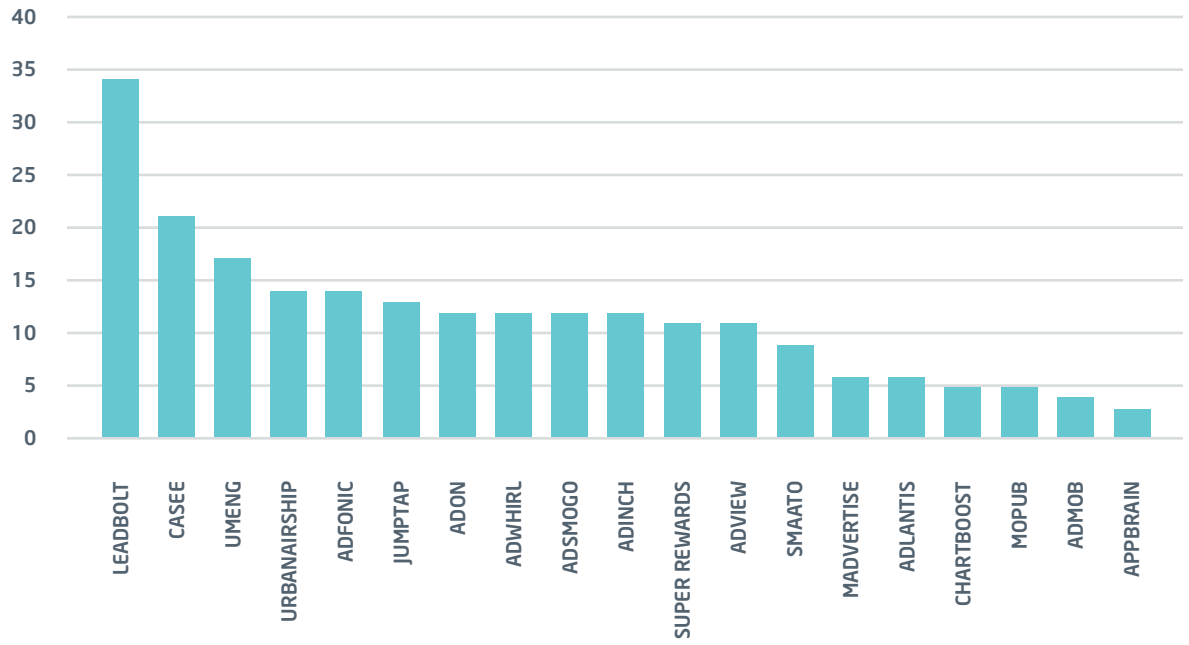
Ad Libraries Love You—And What You Do

For ad libraries: Your privacy is their price for permitting you to engage with mobile devices without prohibitive fees. The data collected enables retailers to target you with ads, coupons, and promotions based on your demographics and location.[1] The more precise the targeting, the less ad clutter you have to deal with, and the more likely you are to click or cash in the coupon displayed on your device. So targeting is really a win-win, but targeting takes data. And trust.

A few ad libraries had privacy scores worse than the worst app.

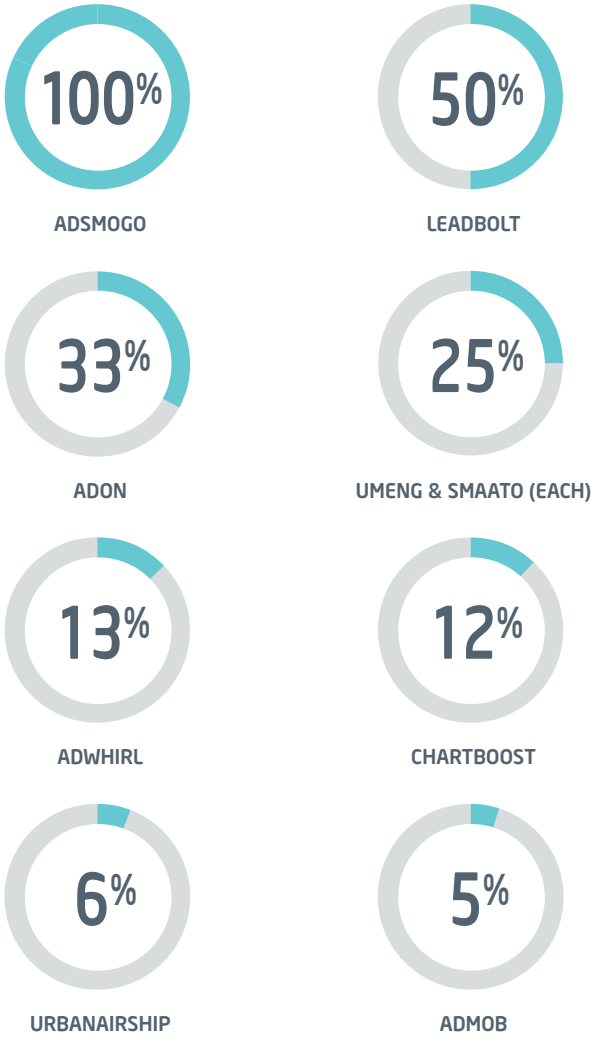
AD LIBRARIES' PRIVACY SCORES

LEADBOLT IS THE WORST OFFENDER WHEN IT COMES TO INVADING YOUR PRIVACY

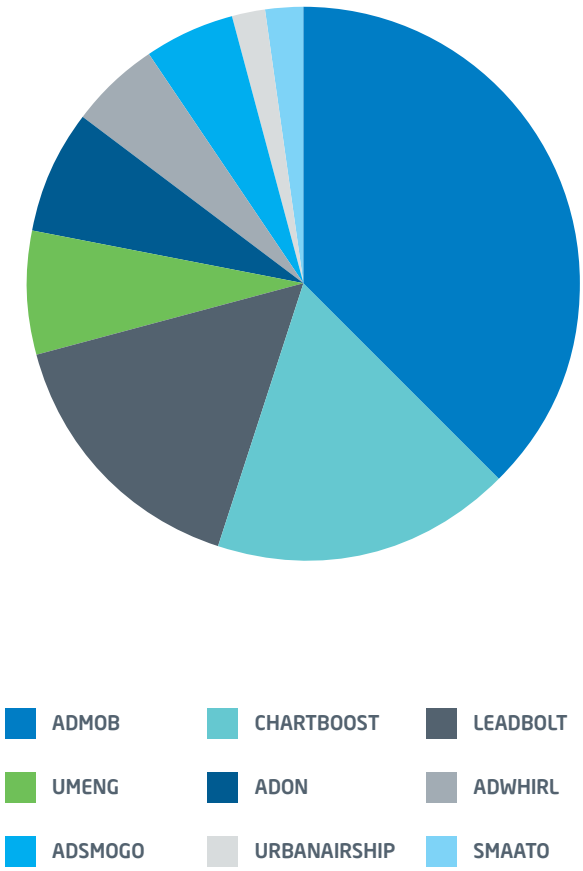


1 https://developers.google.com/mobile-ads-sdk/docs/

SOME AD LIBRARIES SELDOM APPEAR, EXCEPT BROUGHT TO YOU BY MALWARE



THE MOST POPULAR LIBRARIES ARE ALSO FAVORITES OF MALWARE AUTHORS



When we look across the analysis, we see that invasive data collection and malware don't correlate perfectly. Some ad libraries collected data aggressively, but were not used very often by malware authors. We also had ad libraries with very low (that means good!) privacy scores, but a track record of being associated with malware: Admob and Chartboost.

The activities and usage of ad libraries are both beneficial and problematic. This is clearly an area where the industry must continue to work on protecting consumers in order to maintain consumer trust.

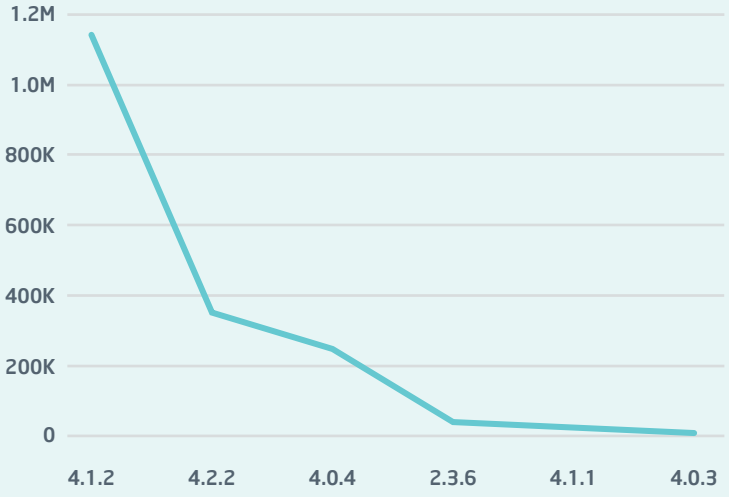
Malware Marches On

Privacy abuse and ad libraries aren't the only thing to worry about when it comes to mobile devices.

We continue to see lots of mobile malware—in apps, emails, and web pages. The highest volumes of infections are in the newest releases, which have been adopted by about half of the market.[2]

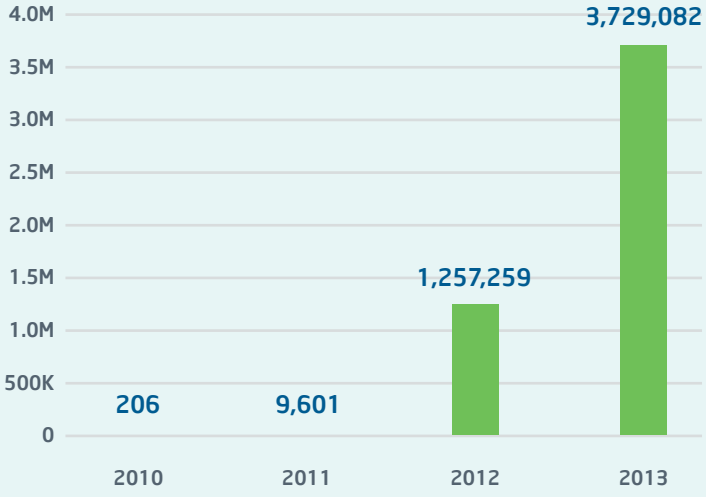
Overall, we saw the total Android "zoo" of malware rise 197% between December 2012 and December 2013.

THE MORE RECENT ANDROID OSes HAVE THE MOST MALWARE



Source: McAfee Labs

THE ZOO OF ANDROID MALWARE ALMOST TRIPLED IN 2013



Source: McAfee Labs

Beginning with the McAfee Labs Threats Report: Third Quarter 2013, we switched our reporting of mobile malware from a malware family count to a unique sample count (hash count). We did that for two reasons. First, we want the method that we use for mobile malware to be consistent with the way we report malware in general. Second, by reporting the total number of variants instead of the total number of mobile malware families, we present a better measure of overall malware affecting mobile devices.

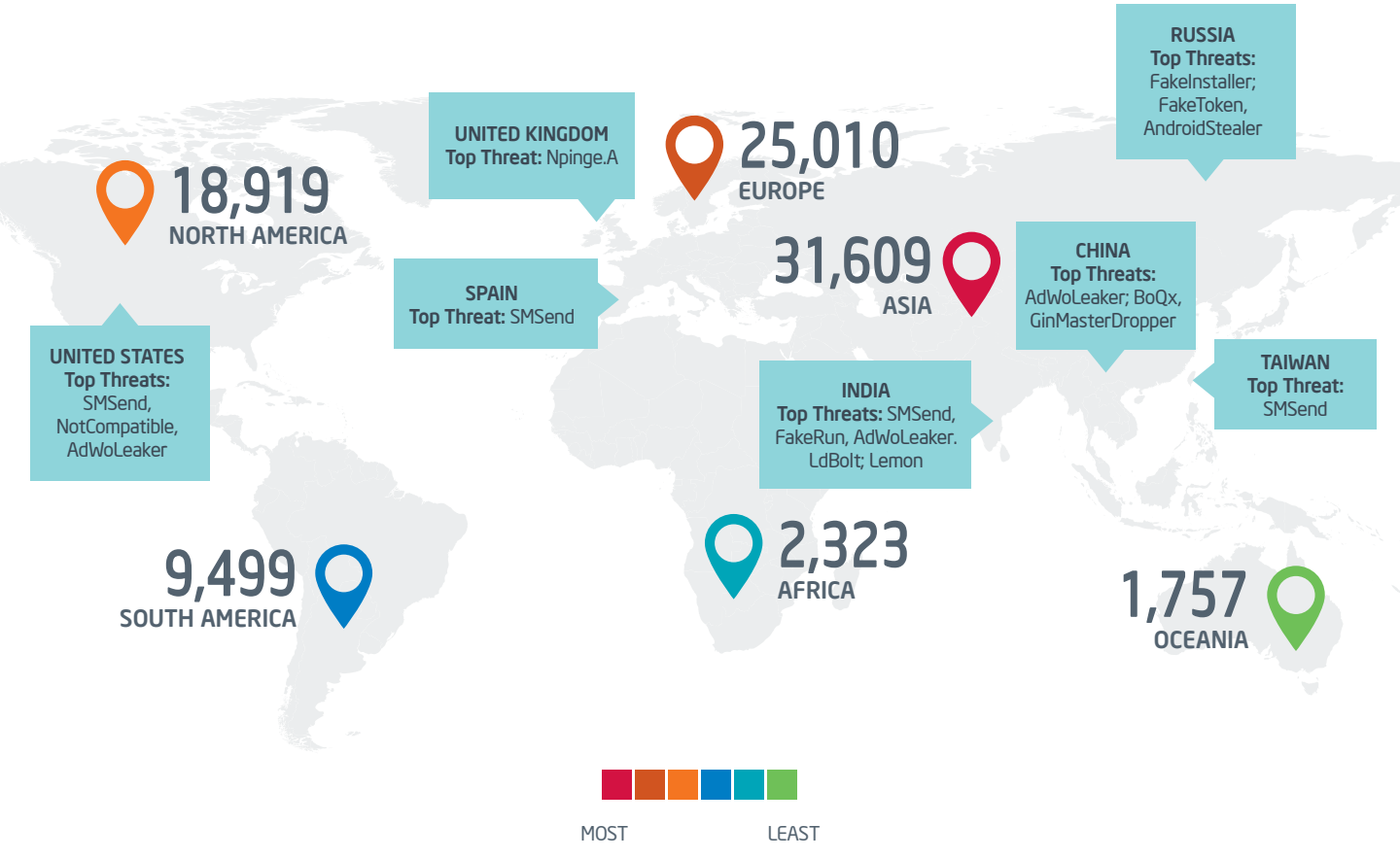
2 http://developer.android.com/about/dashboards/index.html

1ST
THE UNITED STATES WAS THE INDIVIDUAL COUNTRY WITH THE HIGHEST MALWARE COUNT

Some of the most intriguing malware in our latest research included:

- SMS Trojans used in spam, phishing, and harassment
  - Android/SMSend
  - Android/FakeInstaller
- Exploit/MasterKey.A. tricks the Android verification system
- Drive-by downloads / social engineering to plant Fake Antivirus
- Political activists using malware

MOST MALWARE

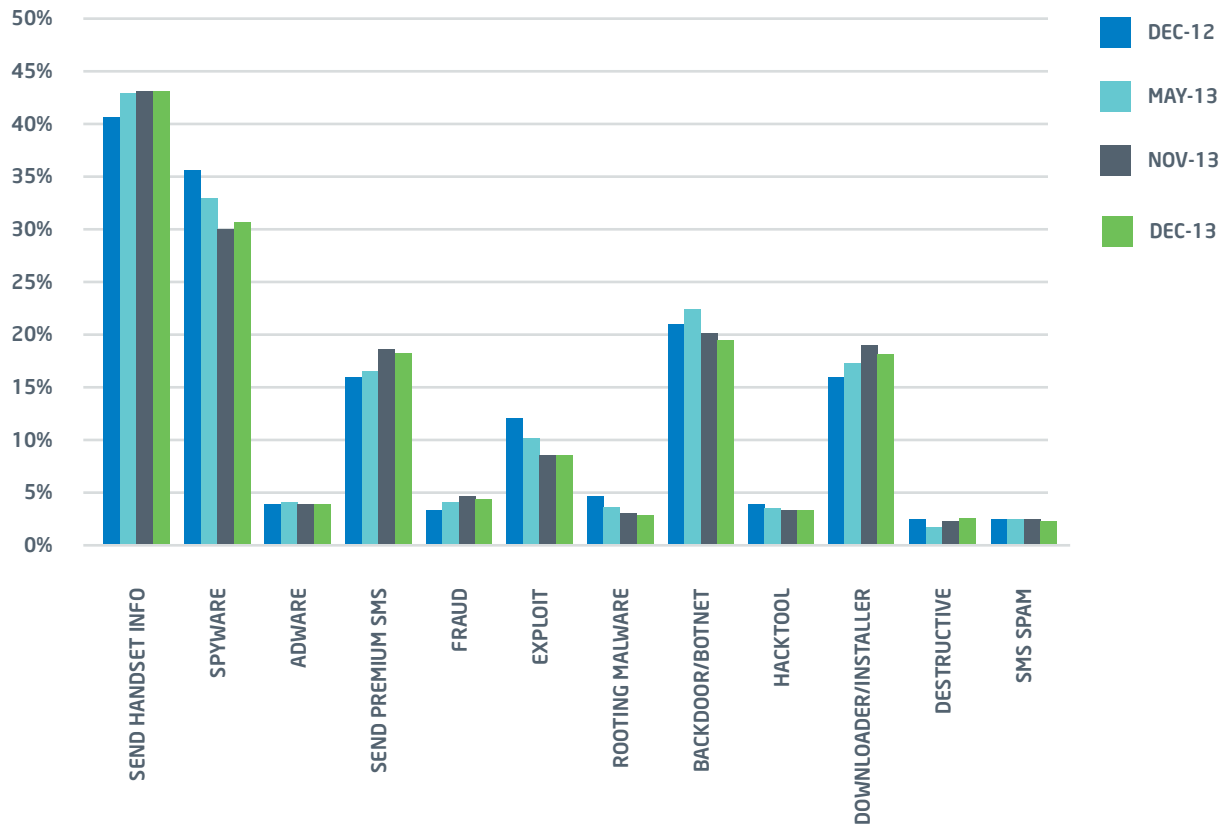


Malware Behavior

Digging into malware trends, we see that malicious software behavior is evolving from spyware and rooting exploits toward more malicious and invasive forms. Increasing behaviors include premium SMS, fraud, and downloaders and installers that give the attacker remote control over the device or use exploits to get installed on vulnerable systems.

MALWARE MANTRA:

GET DATA, HIJACK DEVICE



Android malware using the "MasterKey" exploit illustrates how clever malware writers have become. Malware authors use the "MasterKey" vulnerability as a tool to weaponize basic Trojans and complicate attacks. This software flaw permits unchecked code to execute on the device.

Here's how it works: during the installation of the app, the Android OS usually verifies the app. However, in this threat, the verification process is tricked into missing malicious, extra code that has not been signed. This malicious code can be executed once the application has been installed.[3]

McAfee Mobile Security alerted users to Exploit/MasterKey.A

Malware authors use the "MasterKey" vulnerability as a tool to weaponize basic Trojans and complicate attacks.

3 http://blogs.mcafee.com/mcafee-labs/android-master-key-malware-already-blocked-by-mcafee-mobile-security

Play It Safe

When deciding to accept and download an app, ask yourself if the purpose of the app truly meets the access requested. If something seems unnecessary, it probably is. Learn more about the permissions an app may ask for.

DEVICE INFORMATION
Many apps use your unique device identifier (IMEI, MEID, ESN, or IMSI) to track installation of the app and can be used to track you through your device. The READ_PHONE_STATE permission is the culprit.

PERSONAL INFORMATION
Apps can retrieve your Contacts and communicate to your Contacts list. They can also read and write to your calendar.

YOUR LOCATION
Apps can retrieve your precise location via GPS. They can get your coarse location via the cell tower or Wi-Fi network you are connected to. Don't accept any permission that includes the word LOCATION unless location is part of the app's job. Remember: when you don't want your precise physical location shared, you can turn the GPS capability off.

MONITORING OF TASKS
By monitoring what you do with your device, apps can collect information to let developers market to you or eavesdrop on your life, or help a malicious app evade defenses. Look for the GET_TASKS permission.

McAfee Mobile Security reviews permissions of downloaded apps and offers you a chance to remove unwanted apps. Install a free trial of McAfee Mobile Security today.

YOUR PHONE AND MESSAGES
Apps can retrieve your phone and MMS or SMS message logs and read the phone status. Some apps may intercept outgoing/incoming calls, make phone calls, or send SMS messages. This can be costly and intrude on your communication privacy.

YOUR ACCOUNTS
Some apps ask for access to the list of accounts in the Accounts Service, letting them manage accounts and log in or authenticate to certain accounts. Watch for use of the GET_ACCOUNTS permission.

DEVICE STORAGE
Your SD card is intended for data storage, controlled by you. Apps may want to add, modify, or delete data on your SD card without your knowledge.

DEVICE HARDWARE CONTROLS
What about other device features? Apps could have the ability to take pictures, videos, change settings, and record audio.

DEVICE SYSTEM TOOLS
Apps that ask for permissions to System Tools want to:

- Change or add synchronization settings
- Change user interface settings
- Prevent your device from sleeping
- Retrieve running applications
- Change or create wireless access point settings, or even create a wireless access point

Summary

Smartphones and tablets offer a unique synthesis of online and mobile lifestyles. Apps and messaging connect us, entertain us, and enrich our lives. But malware, ad libraries, and aggressive permissions complicate the digital experience. We give up our privacy and identifiable data in exchange for convenience, access, and personalization.

This report shows how much our apps are sharing about us. It shows how malware authors are adapting to mobile business models and technologies as fast as the devices and operating systems arrive. And it shows clearly that consumers can use all the help they can get in understanding and managing the information they reveal about themselves through their mobile devices.

Resources

Keep your digital life protected against changes in the mobile threat landscape:

- McAfee Security Advice Center
- 99 Things You Wish You Knew Before Your Device Was Hacked
- www.mcafeemobilesecurity.com

About the Authors

Irfan Asrar, Alex Hinchliffe, Barbara Kay, and Abhishek Verma wrote this report.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe.

www.mcafee.com