Report

Mobile Security: McAfee Consumer Trends Report

Trends in risky apps, mobile misbehavior, and spyware

Table of Contents

About This Report 3

Key Findings 3

Risky Apps Defined: Malware and Suspicious URLs 3

Risky Mobile App Sources 4

Black Hat SEO and Mobile App Stores 5

1 In 6 App Downloads Could Be Risky 5

Malware + Suspicious URLS = Sophisticated Scams 6

Mobile Malware Defined 6

Multiple Misbehaviors 7

Reusable Code, Reusable Bots, Reusable Botnets 8

Spotlight on Spyware 9

What's Next? 10

Resources 10

About This Report

As a leader in security research and mobile security products, McAfee is harvesting its extensive global threat intelligence database to educate consumers about mobile threat realities. This report documents the ways cybercriminals use malicious code and websites separately and in combination to target consumer devices and personal information.

In this report, we focus on "real world risk." What is the chance of an average mobile device user encountering malware or a suspicious website? What sorts of things will the malware do? This "real world" analysis contrasts our overall zoos of apps and mobile malware with data collected from the installed base of McAfee Mobile Security users.

Key Findings

- Unlike the email- and website-based infections typical of PCs, mobile malware is distributed primarily through infected apps today
- 3 percent of malware-infected apps in our overall mobile app zoo came from the Google Play store
- Within the fairly conservative McAfee user community, 75 percent of malware-infected apps were downloaded from Google Play
- Crooked app stores use black hat search engine optimization (SEO)
- Based on the experience of McAfee users, typical consumers have at least a 1 in 6 chance of downloading apps that include malware or suspicious URLs
- Almost 1/4 of the risky apps that contain malware also contain suspicious URLs
- 40 percent of malware families misbehave in more than one way, showing the sophistication and determination of the criminals
- 23 percent of mobile spyware joins a botnet or opens a backdoor, increasing the risk of data loss or device abuse

Once you own a smartphone or tablet, you are not likely to give it up. Our hope is that you can understand where the risks are and steer around them as you enjoy your mobile digital life.

Risky Apps Defined: Malware and Suspicious URLs

Risky apps are delivery vans for cybercrime tools. They can carry all sorts of malicious code and hacker tools, as well as links to websites that criminals control. Risky apps containing mobile malware can steal personal information (to invade your privacy or steal your identity), perpetrate fraud (such as an SMS content scam), or abuse a device by making it part of a criminal bot network.

Risky apps may include both malware and suspicious URLs in combination to permit more complex schemes (discussed later in this report), or a risky app may contain no malware, merely a suspicious URL.

Suspicious links typically help involve consumer mobile devices in profitable (to the fraudster) scams. These URLs perform click fraud, phish for personal information, advertise shady content, or instigate nuisance interactions like spam. Most device owners prefer to avoid all of these activities, using their devices, time, and data plans for actions they consciously select.

So far, few apps that contain suspicious URLs lead to sites with drive-by downloads. Most malware on a web page still needs to be "accepted" by the user, giving consumers the chance to back out. However, we saw our first mobile drive-by downloads in 2012 and expect more in 2013.[1]

Glossary

Risky Apps—Downloadable mobile apps that contain any form of malware or links to suspicious websites.

Suspicious URLs—Web pages that contain malware, browser exploits, phishing behaviors, spam sign up forms, or affiliations with other shady web sites.

Malware—Unique samples of malicious or potentially undesirable code that may take many forms, including viruses, Trojans, worms, or exploit code.

Malware Families—Related groups of unique samples of malware that evolve from the same components like a family tree. They show the same behavior.

Malware Packages—Separate implementations or variants of a malware family; often the same software is recompiled or manipulated to go unrecognized by security software.

Zoo—A collection of all samples of something, such as "app zoo" or "malware zoo."

The Numbers Game

Wondering how to compare our numbers to other vendors' reports? Each report's numbers vary, since every vendor makes different decisions on how to classify, count, and report threat data. They may choose to report unique families of malware, unique packages of these families, or all possible unique malware instances found to be carrying out these threats. Vendors reporting unique malware instances generally have larger numbers than those who report only malware families or packages.

For example, criminals have packaged the Skulls family of malware in more than 100 different ways. These packages are then rearranged, recompiled, and deployed in many different app instances. At the core, the same Skulls malware family carries out the same threats.

With so many different numbers floating around and creating confusion, we chose to focus primarily on proportions and trends. This report reflects our analysis of both unique malware samples found in apps and distinct malware packages. While we base our app source conclusions on all unique malware instances, we do not provide overall instance counts in order to avoid inflating perceptions of perceived risk.

In the full *McAfee Quarterly Threats Reports*, we present the unique count of malware packages reported to date to give readers a sense of the rapid expansion in malware diversity.

Risky Mobile App Sources

The McAfee research database includes a gigantic collection of mobile apps—both innocent and risky. Because we stalk the bad stuff—proactively searching for and researching intriguing samples—a high percentage of our overall apps database is risky.

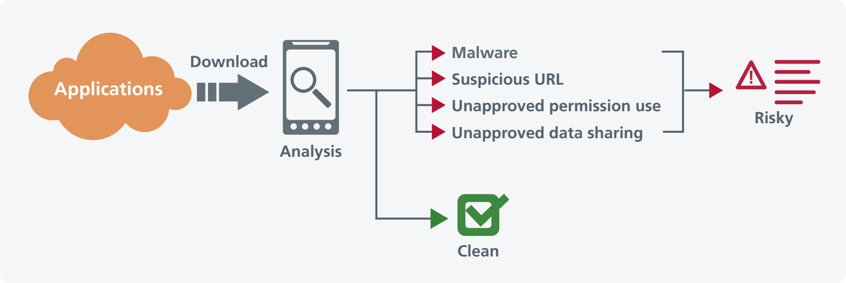

Figure 1. McAfee software scans each downloaded app to see if bad stuff is contained inside, or if the app might abuse your trust and privacy.

This toxic pool does *not* reflect the typical mobile device user's environment, but it does provide interesting insights into criminal networks. For example, we first looked at the stores where our automated collection software found malware-infected apps.[2] Our crawlers found that 57 percent of all of the malware-infected apps in our collection came from just three app stores, all in Russia. This concentration likely means that organized criminals run the app stores. For comparison, only about three percent of our overall zoo of malware-infected apps came from the Google Play store. It ranked as the ninth largest source of malware-infected apps in our sample.

We then looked at the sources of malware-infected apps downloaded by the installed base of McAfee Mobile Security users. These numbers were very different. Since Google Play is the primary source of all apps for Android users, we were not surprised to see that 75 percent of malware-infected apps downloaded by our user base came from Google Play. No other commercial or carrier-owned store appeared on either list of malware-infected app sources.

Our conclusion is that while Google Play is safer than many app stores, users should still be wary with any app. Pay attention to the permissions that any app requests. Scan all apps for malware. And keep an eye on monthly bills to catch premium content fraud quickly.

Source	Entire Malware-Infected App Zoo (Sourced)	Source Ranking	McAfee Mobile Security Installed Base Malware-Infected App Zoo (Sourced)	Source Ranking
Source 1 (Russia)	26%	1	3%	4
Source 2 (Russia)	22%	2	1%	10
Source 3 (Russia)	9%	3	0%	21
Google Play	3%	9	75%	1

Black Hat SEO and Mobile App Stores

Many users want content such as native language games or utilities that are unavailable in commercial app stores. When users turn to alternative stores, risk escalates. For example, in 2012, Google and Adobe discontinued distribution of the Flash player for Android.[3] Anyone wanting to visit websites with Flash content still needs a player app, and they might use a search engine to find one. Shady app storekeepers seized the opportunity. We found five app stores with names based on variations of the words "Android Flash Player."

Researchers call this technique "black hat search engine optimization (SEO)." Criminals think about ways a potential victim would search for content, then use those keywords in their URLs, web pages, and page tags. They hope to appear high in the search engine results page, above legitimate content, and win the click. For additional traffic, fraudsters may use phishing or spam (links distributed in traditional email, social media, or SMS messages) to lure victims to their site.

The criminal profits when the user downloads the malicious app. The criminal can mine the victim's device for data or misuse it in the many ways we discuss in this report.

Similarly, four other app stores used the words "cut the rope," presumably to lure people (especially children) interested in downloading the candy-eating monster game one reviewer said, "has all the addictive qualities of Angry Birds."[4] Success breeds scams.

Black hat SEO works particularly well in the mobile space because it is harder for users to know the actual URL they are visiting. A mobile browser may not present the URL within the visible window by default. When the URL is not completely visible, an attacker can use typosquatting (presenting a site name that is almost the same as the legitimate one) or special URLs to trick users into thinking that they're at the intended site, such as amazon.com.

Also, developers creating content with HTML5 can make their site appear to be a native mobile app, without a visible URL or address bar. A user needs to move or "sweep" a page down to see the address bar. Even then, on a mobile screen, a user may not be able to see the entire URL.[5]

1 In 6 App Downloads Could Be Risky

We next looked more closely at the nature of the risky apps downloaded by our user community. What level and type of risks do real users really face? More than you might think. Of the apps our users downloaded between April and December of 2012, our tests found 16 percent—1 in 6 apps—to be infected with malware or to contain links to risky URLs.

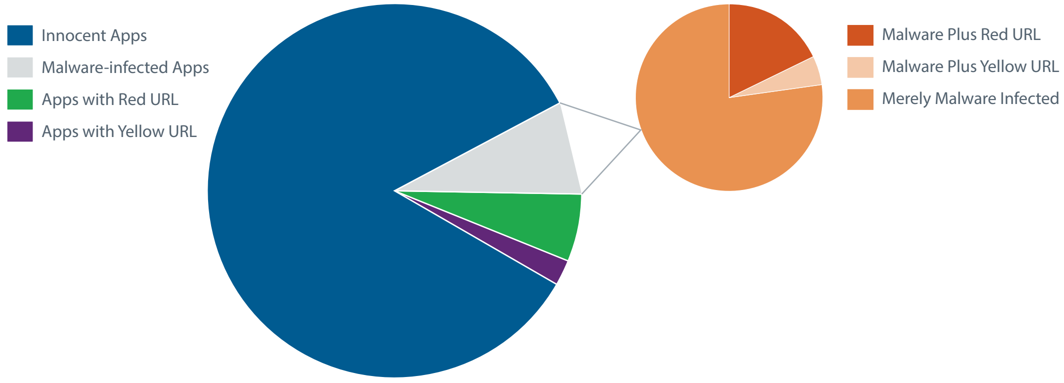

Figure 2. McAfee users have a 1 in 6 track record of downloading risky apps. Of the 8% of our users' downloaded apps that contained malware, 23% also contained suspicious URLs.

Four malicious app stores preyed on gamers using the words "cut the rope"

(Image Courtesy Amazon.com)

Our "Real World" Data Sources

McAfee Mobile Security users have downloaded more than 430,000 apps. This count reflects every release and version of an app. For example, there are 50 different flavors of the Facebook app.

When a user downloads an app, the McAfee software looks at a variety of things, including

- The permissions that the app requests
- Whether or not it shares data
- The presence of malware
- The reputation of any URLs within the app

McAfee Mobile Security presents a risk assessment, and the user can easily delete the app.

McAfee Mobile Security users are clearly risk averse: they have purchased a mobile security product. They also see a warning if they try to visit websites with a reputation for being risky, which gives them a chance to stop before they encounter a risky app. For these reasons, we believe that 1 in 6 represents the very conservative end of the app riskiness spectrum. Like a child without a vaccination, anyone without mobile security has a greater risk of infection.

Malware + Suspicious URLS = Sophisticated Scams

Next, we examined the 8 percent of apps that contained malware. Of these, some malware was complex. About 23 percent contained both malware and suspicious (Red or Yellow) URLs. An app with both malware and a suspicious URL may be helping with a black hat SEO program that pushes up ad impressions and clicks. To do this, the malicious code might add bookmarks to the browser or install an app that launches the target website or ad URL. More advanced malware will attempt to initiate ad clicks or drive users to a forum or site that pays the criminal based on traffic.

Mobile Malware Defined

We classify an app as containing malware if it does one or more of the following:

- Sends your handset or personal information to someone else without your permission
- Spys on and records your activity (browsing history, messages, videos played)
- Sends premium rate SMS messages to sell ringtones, downloads, or subscription data services
- Commits click fraud
- Exploits a vulnerability or software bug on your device to cause it to do something you aren't expecting (often through downloading other malware)
- Roots your device to give an attacker control of it
- Installs a backdoor or turn your device into a bot client, often collecting personal information as a side benefit
- Installs a hacking tool that allows the attacker to control your device
- Downloads a secondary piece of malicious code from a website
- Is destructive to your device or its data
- Sends spam messages via SMS from your device

Multiple Misbehaviors

McAfee analyzed Android[6] malware families identified from 2007 through 2012. We found that sending handset information and spying represented about half of all malicious behaviors in the families.

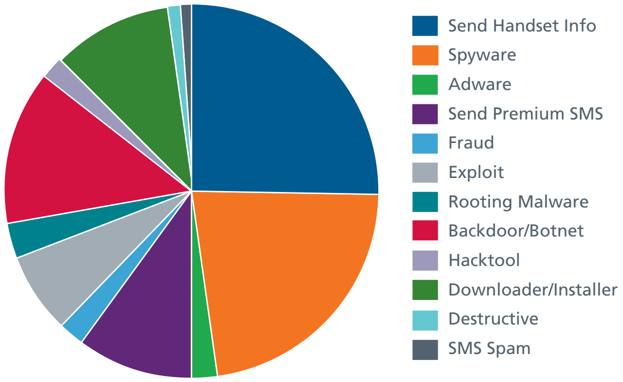

Figure 3. Mobile malware shows a broad range of malicious or potentially undesirable behaviors.

We also discovered that 40 percent of our malware families exhibited more than one form of misbehavior. This complexity helps the criminal achieve success in two ways. First, the attacker can customize each assault to the technologies and vulnerabilities of the device. Second, some combinations make it difficult for users (or security software) to recognize the behavior as unusual or malicious, allowing the attack to proceed undetected.

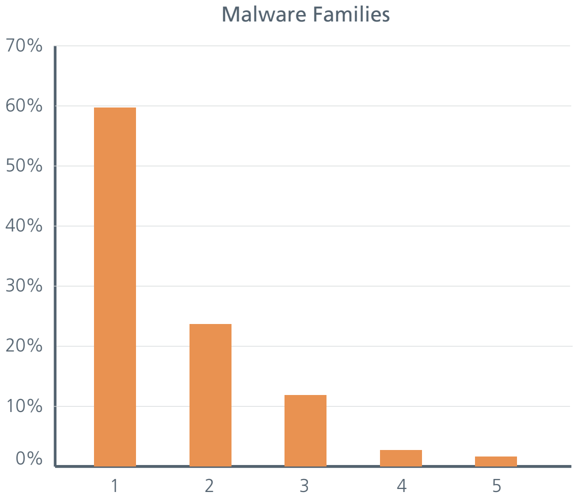

Figure 4. 40 percent of malware families include more than one form of suspicious behavior.

In the families that include four or more misbehaviors, we uncovered some common factors:

- 100 percent send personal or handset information
- 100 percent set up a backdoor or botnet on the device
- 75 percent include a downloader or installer
- 62 percent act as spyware
- 50 percent have rooting malware

These carefully designed attacks include names you may recognize from the press: DroidDream, RootSmart, Stiniter,[7] DroidKungFu,[8] Geinimi, and DroidDreamLite. Several of these families share characteristics:

> *"DroidKungFu.A takes hints from other complex Android malware families, such as Geinimi and Android/ DrdDream—its code is included in a number of apps, including a handful of games. Like DrdDream, DroidKungFu.A also uses a pair of root exploits to reduce system security and maintain itself on the device."*
>
> *—McAfee Security Journal, Summer 2011*

The 100 percent overlap between sending handset information and setting up a backdoor or botnet client makes perfect sense. Imagine a hacker wants to make your device part of a bot network or collect details on what you do. In order to communicate with your device, the bad guy needs to know its identification number, so the first task after the malware installs is to send handset information from the device.

We found that 75 percent of the most complex families then went a step further. They pulled down additional malware or control software to give the attacker more tools, such as spyware and rooting malware. Like rooting or jailbreaking an iPhone, rooting malware lets the attacker overcome internal controls and take over the device.

Reusable Code, Reusable Bots, Reusable Botnets

Botnet clients, downloaders, and rootkits are generically useful software sold on black markets as part of software toolkits. With these pre-packaged toolkits, it does not take much work or deep technical expertise for a criminal to assemble the right package for each purpose. Just select a few options and rules, and "voila": premium SMS and click fraud, spam distribution, data theft, or bank fraud.

Commercial criminals reuse and recombine these components as they devise different schemes. If a botnet manager, or bot herder, finds another criminal willing to pay to rent the bot network, the bot herder can load the renter's new commands into the code. In this clever criminal use of the cloud, the same basic botnet plumbing supports different crimes. For example, in *Mobile Security: McAfee Consumer Trends Report*, we described the versatility of two attacks, Android/Funsbot.A and Android/Backscript.A:

> *"Android/Funsbot.A is a botnet client that was part of a larger advanced persistent threat malware campaign. It takes commands that upload and download files from the attacker's server. The client can also browse the directories of an infected Android device. This allows an attacker to both gather information on a particular target and also maintain and increase control of that target.*
>
> *Android/Backscript.A is another advance in Android malware. This botnet client gets updates of new commands and functionality from the attacker's control server. Instead of downloading native executables, it uses a form of JavaScript that runs in mobile Java to shorten development time. Currently the malware performs pay-per-install installations of a particular third-party app, and can be easily updated to install other apps for a fee."*

Building or renting malware is easy with the anonymity of the Internet. Easier still is to steal someone else's working system. In China, criminals frequently take over one another's botnets of mobile devices.

Spotlight on Spyware

23 percent of spyware also adds the device to a botnet or opens a backdoor

In this edition, we chose to investigate spyware and found it represents about 1/3 of all malware families in our zoo. Most of the spyware is "just" spyware that will watch and record your browsing history, messages, or locations. However, some spyware is actively evil. Of the 70 malware families classified as spyware, 23 percent activated a botnet client or backdoor, enabling the sort of takeover discussed above, while 7 percent sent premium SMS messages.

Geinimi is a great example of spyware that joins a botnet. It also forwards all SMS messages to the attacker. This lets the attacker intercept messages from your bank, from premium SMS services, or from a money transfer service. It can also install new spyware or adware and steal your contacts to distribute a worm or for spam targeting. Finally, it can load URLs in the browser for ad clicks or traffic generation.

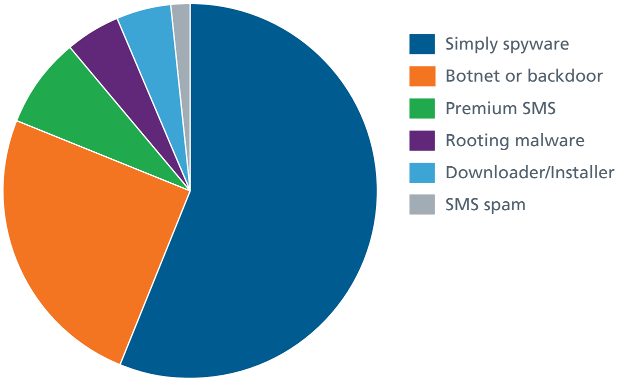

Figure 5. We found that spyware often includes other misbehavior.

Be Smart on Your Smart Device

To avoid malicious apps:

- Download apps only from Google Play and other well-known mobile device manufacturer- or carrier-operated stores
- Opt not to download apps that appear unusual
- Remove apps that your security software indicates are risky

If you *really* want an app that is not available from a commercial store, then you should really use a mobile security solution that checks the permissions, reputation, and content of the app.

What's Next?

We expect attacks to become increasingly sophisticated in the near future. Suspicious URLs will result more often in malware infections, likely through more use of silent drive-by downloads. Joining drive-by downloads and black hat SEO, other proven PC-oriented threats will migrate into mobile device environments.

Criminals will also look at ways to generate revenue from features only mobile devices have. Through 2012, about 16 percent of our malware families attempted to get devices to subscribe to premium SMS messages. In 2013, we foresee an increase in threats such as MarketPay, which is a premium content corollary that targets users of third-party app stores. Users will find out they bought premium apps only when they check their bills.

We anticipate more fraud-oriented malware in 2013. One likely innovative content swindle will abuse the tap-and-pay near field communications (NFC) technology used in mobile payment programs, or "digital wallets." This scam could involve worms that propagate through proximity, what we call "bump and infect." This distribution path could quickly spread malware through a trainload of passengers or a theme park. When the newly infected device is used to "tap and pay" for the next purchase, the scammer collects the details of the wallet account and secretly reuses these credentials to steal from the wallet.

Want to learn more? Refer to the McAfee Labs 2013 Threats Predictions Report for descriptions of other potential new concerns. It describes malware that blocks security updates to mobile phones and ransomware "kits" that allow criminals without programming skills to extort payments to unlock a device. How about malware that renews a connection after a botnet has been taken down, allowing zombie machines to come back to life? Stay tuned. McAfee researchers are tracking all these exciting—and dangerous—developments in mobile threats.

Resources

Keep up with changes in the mobile threat landscape:

- McAfee Security Advice Center
- 99 Things You Wish You Knew Before Your Device was Hacked
- mcafee.com/us/mms

About the Authors

Barbara Kay, Jimmy Shah, and Abhishek Verma wrote this report.

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence.™ The McAfee Labs team of 500 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public. www.mcafee.com/labs

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on finding new ways to keep our customers safe. www.mcafee.com

[1] In Spring 2012, researchers discovered NotCompatible, the first mobile drive-by download malware that installed silently when a user visited a site, without the user "accepting" the code.

[2] Our overall zoo contains app samples that our crawlers have found, as well as samples identified by other researchers. We only have source information for the apps identified by our crawlers.

[3] http://howto.cnet.com/8301-11310_39-57554629-285/install-adobe-flash-player-on-jelly-bean-devices/

[4] http://www.ign.com/articles/2010/10/08/cut-the-rope-iphone-review-the-next-angry-birds

[5] http://blogs.mcafee.com/mobile/mobile-browsers-trouble-comes-in-threes

[6] As of the end of 2012, developers had written 97 percent of mobile malware for the Android platform.

[7] DroidDream was active in 2011. The McAfee Labs First Quarter 2012 Threats Report said of RootSmart and Stiniter: "Android/RootSmart.A uses a root exploit to download Android/DrdLive.A, a backdoor Trojan that sends premium-rate SMS messages and takes commands from a control server. Android/Stiniter.A uses a root exploit to download additional malware and sends information from the phone to sites under the control of the attacker. It also sends text messages to premium-rate numbers. The attacker's control server updates the message body and the number the hijacked phone sends to."

[8] "At the end of May, new malware was discovered in the official Android Market by researchers at North Carolina State University. Named DroidKungFu, this malicious software is capable of burrowing into the root level on vulnerable Android devices using the classical RageAgainstTheCage and CVE-2009-1185 exploits initially implemented by DroidDream. But, unlike its predecessor, DroidKungFu will use AES to encrypt the two exploits to evade detection from current mobile antivirus software. Aside from this difference, the behavior of the malware is the same as DroidDream: it collects information about the device, and it installs a second application that can download more malicious software onto the device. "*Android Malware: Past, Present, and Future*"

McAfee®
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

mobile-threat-report_0213_ETMG