RISKIQ®

2019 Mobile App Threat Landscape Report

The Mobile Ecosystem Swells, but Google Leads a Decline in Malicious Apps

By Jordan Herman

Users downloaded

200Bn +

apps in 2019

Users spent

$120Bn +

in app stores worldwide

The digital revolution is causing businesses to invest significantly in mobile not only to make more frequent and meaningful interactions with consumers but also to feed a ravenous demand. Users downloaded over 200 billion apps in 2019 and spent more than $120 billion in app stores worldwide. In 2020, consumers will surpass those marks, as mobile usage takes up more and more of our daily lives—3.7 hours on average and rising, according to App Annie.

Although mobile apps help drive business, the app landscape is a significant portion of an enterprise's overall attack surface that exists beyond the firewall, where security teams often suffer from a critical lack of visibility. Threat actors have made a living taking advantage of this myopia to produce "rogue apps" that mimic well-known brands and are purpose-built to fool customers into downloading them. These imposter apps are an effective tactic because our brains recognize and make instantaneous judgments about visual stimuli. Once downloaded, they can phish users for sensitive information or upload malware to their devices.

On rare occasions, these rogue apps appear in official stores, even breaching the robust defenses of the Google Play and the Apple App stores. However, there are hundreds of less reputable app stores that represent a murky mobile underworld that exists outside of the relative safety of reputable stores. With many of these apps found in stores hosted in countries known for cybercrime, such as China, or outside of stores altogether on the open web (often referred to as feral apps), it's no wonder CISOs can't keep tabs on them. However, for businesses, even though they don't own or manage these apps, they're still a part of their attack surface and thus are responsible for detecting and addressing them.

With a proactive, store-first scanning mentality, RiskIQ observes and categorizes the threat landscape as a user would see it, monitoring both the well-known stores like the Apple App Store and Google Play, but also more than 120 others around the world. RiskIQ also leverages daily scans of nearly two billion resources to look for mobile apps in the wild. Every app we encounter is downloaded, analyzed, and stored so that we can record changes and new versions.

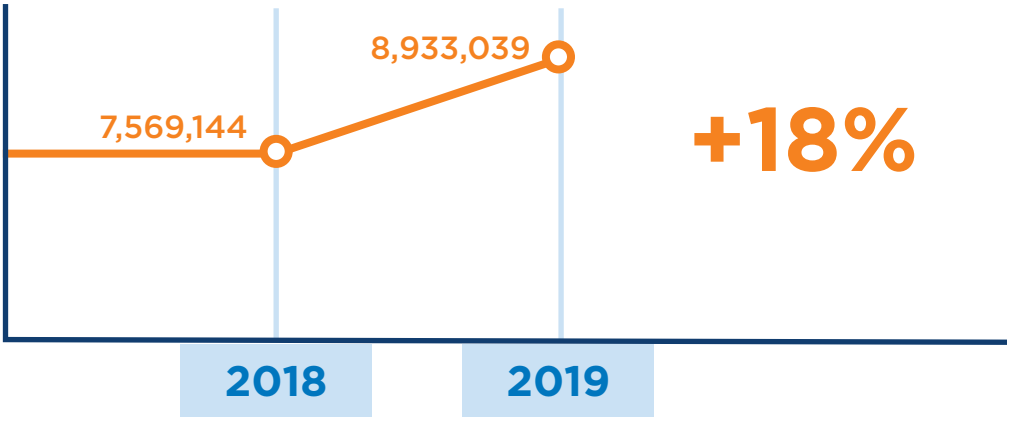
In this report, we'll give a snapshot of 2019's mobile threat landscape and dive into emerging trends we anticipate carrying into the 2020s.

China app market accounts for **40%** of app apending

The App Ecosystem is Growing Every Year, Fueled by China

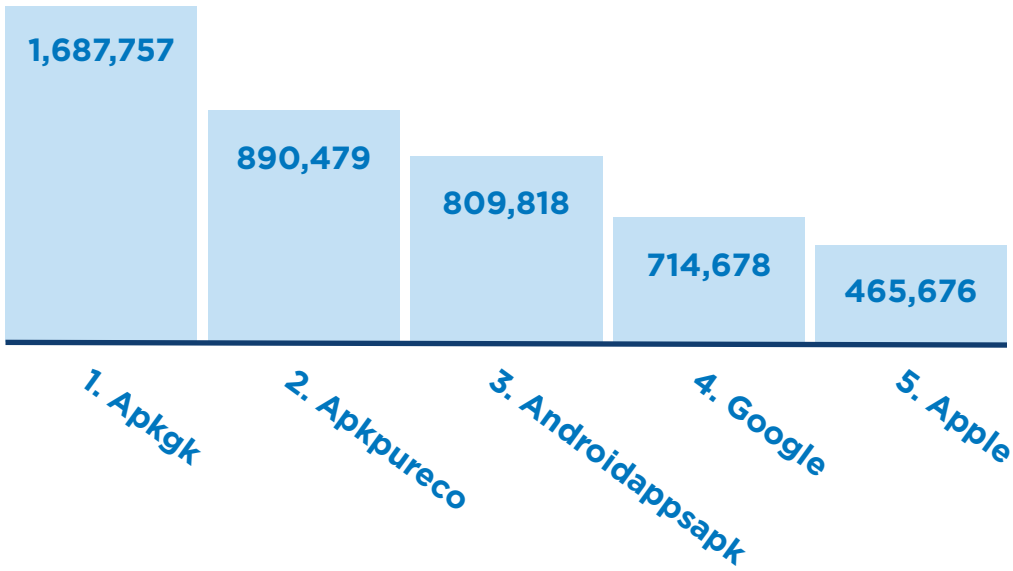
By any measure, the mobile landscape is getting bigger, busier, and more complex. RiskIQ cataloged 18% more apps worldwide in 2019 than in 2018.

Newly Observed Apps in 2019:



China remains the largest app market, accounting for 40% of consumer app spending. The top-three most prolific app stores in 2019 were Chinese, ahead of both Google and Apple.

Most prolific stores of newly observed apps in 2019:

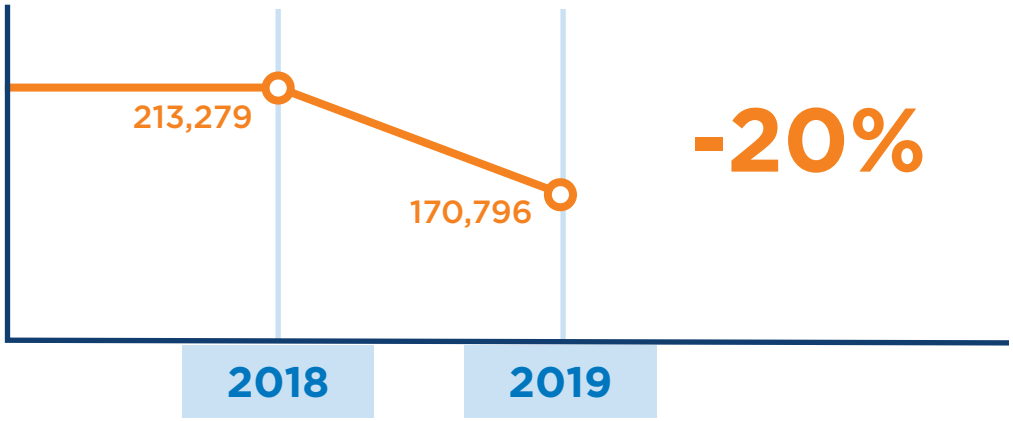


RiskIQ blacklisted **76% less** apps than in 2018

Mobile Got Safer in 2019

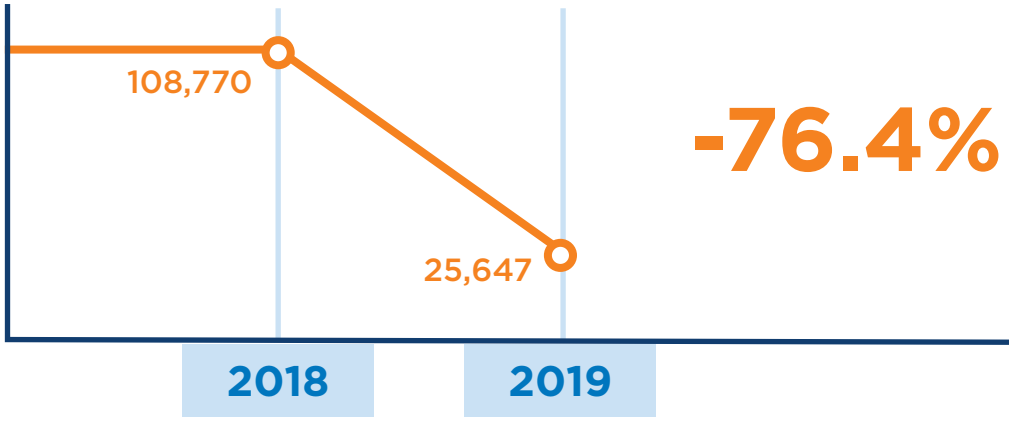
Despite seeing and cataloging far more apps in 2019, RiskIQ blacklisted 25,796 apps, more than 76% fewer than in 2018. Blacklisted apps are apps that appear on at least one blacklist such as VirusTotal, which, per its website, inspects files or web pages with over 70 antivirus products and other tools. A blacklist hit from VirusTotal shows that at least one vendor has flagged the file as suspicious or malicious.

Total Blacklisted Apps in 2019:



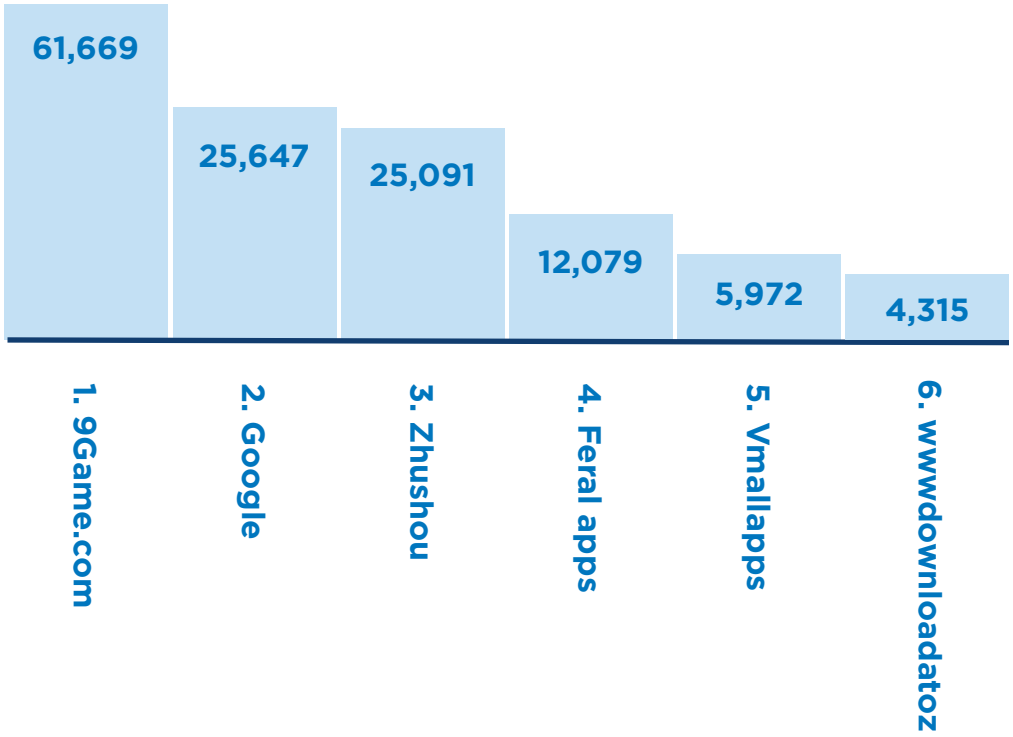
Apple treats its App Store like Fort Knox and rarely hosts dangerous apps. Meanwhile, Google's security controls are improving despite allowing troublesome apps to enter the Play Store at a rate it finds acceptable—the number of blacklisted apps in the Play store dropped an impressive 76.4% in 2019.

Blacklisted Apps in the Google Play Store in 2019:



Because the two leading app stores are inhospitable for malicious apps, threat actors must turn elsewhere to turn a profit. However, there are hundreds of stores across the world in which threat actors can comfortably sell their wares. They can also make their apps available as feral apps across the open web, outside of stores altogether.

Most prolific stores of newly observed apps in 2019:



Some app stores are more dangerous than others and have a higher concentration of malicious apps. In 2019, these were the stores from which you were most likely to download a malicious app:

1. 9Game.com
2. Feral apps
3. VmallApps
4. Xiaomi
5. Zhushou

2019 Mobile Threat Highlights

Q1: Adware Agony - TechCrunch reported that millions of Android users were tricked into downloading 85 adware apps from the Google Play store. Researchers said these apps included popular utilities and games. They served deceptively displayed ads, including full-screen ads, hidden ads, and ads running in the background, enabling them to monetize off of unsuspecting Android users.

Q2: Targeting Taxes - In the 2019 tax season, attackers are capitalized by using the brand names of leading accounting firms and tax filing software to exploit users filing their taxes by creating fake mobile apps and landing pages. RiskIQ returned 4,162,450 total mobile apps matching these branded terms in app stores around the world, and 30% of these apps, 1,221,070, were blacklisted.

Q3: Enter Fleeceware - As RiskIQ's Evil Internet Minute found that mobile app is blacklisted every three minutes, researchers discovered a new group of Android apps in the Google Play Store known as fleeceware, which severely overcharge users. These apps are available for free or at low-cost, and after a short trial period, begin charging the user hundreds of dollars unless they both uninstall the application and inform the developer they do not want to continue to use the app.

Q4: Black Friday Blacklist - To analyze the methods these cybercriminals would employ over Black Friday and Cyber Monday 2019 and where they're targeting their malicious efforts, RiskIQ ran a keyword query of our unmatched Global Blacklist and mobile app database focusing on the top-10 most trafficked sites on Thanksgiving weekend. These brands had a combined total of 6,353 blacklisted apps that contain their branded terms in the title or description.

Conclusions

As Attacks Become More Sophisticated, Discretion is your Best Defense

Users should be discerning and skeptical when downloading anything and have passive protection such as legitimate antivirus software along with regular backups. Although they cannot make up for preventative measures such as checking permissions, anti-malware products provide some protection from malicious code.

Luckily, some of these malicious lookalike apps are easy to spot. One potential giveaway is excessive permissions, where an app requests permissions that go beyond those required for its stated functionality. Another is a suspicious developer name, especially if it does not match the developer name associated with other apps from the same organization. User reviews and number of downloads, where present, also help to give some level of reassurance that the app is legitimate.

If you find you have installed an app that spams you with links or tries to force downloads—or it turns out to be a lookalike or disappears after installation or one use—having regular, recent backups lets you wipe the phone and restore it to a safe state.

Know Your Mobile Attack Surface

This hidden mobile threat landscape is a branding and consumer trust nightmare for businesses. Whether they have an official mobile presence or not, brands must be aware of this mobile app landscape to understand the entirety of their mobile attack surface. Monitoring primary stores like the Apple App Store and Google Play is important. Still, also having visibility into apps in lesser-known app stores across the world—and across the web—is paramount.

About RiskIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75%of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com