RISKIQ®

2020 Mobile App Threat Landscape Report

Tumultuous Year Bred New Threats, But the App Ecosystem Got Safer

Users downloaded

218Bn+

apps in 2020

Users spent

$240Bn+

in app stores worldwide

Each year, businesses invest more in mobile as the lifestyle of the average consumer becomes more mobile-centric. Mobile growth exploded in 2020, with the COVID-19 pandemic advancing mobile adoption "by at least two to three years." According to App Annie, Americans are now spending more time on mobile than watching live TV, and social distancing caused them to migrate more of their physical needs to mobile, such as food shopping and education. App Annie also shows that mobile spending grew to a staggering $143 billion in 2020, year over year growth of 20%.

This ravenous demand for mobile creates a massive proliferation of mobile apps. Users downloaded 218 billion apps in 2020 and spent more than $240 billion in app stores worldwide. Meanwhile, RiskIQ noted a 33% overall growth in mobile apps available. For organizations, these apps drive business outcomes. However, they can be a dual-edged sword—the app landscape is a significant portion of an enterprise's overall attack surface that exists beyond the firewall, where their 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 or otherwise purport to be something they're not, purpose-built to fool customers into downloading them. Once an unsuspecting user downloads these malicious apps, threat actors can have their way, phishing them for sensitive information or uploading malware to their devices.

These rogue apps appear in official stores on rare occasions, even breaching the Google Play and Apple App stores' robust defenses. However, hundreds of less reputable app stores represent a murky mobile underworld outside of the relative safety of reputed stores. Apps in these stores are far less regulated than official app stores, and some are so overrun with malicious apps that they outnumber their safe offerings.

Many malicious apps are available in stores that reside in countries known for cybercrime, such as China, or outside of stores altogether on the open web (often referred to as feral apps), making it extremely difficult for security teams to keep tabs on them. However, that doesn't mean businesses are off the hook. Even though an organization doesn't own or manage a copycat app, it's still part of its attack surface because it's leveraging its branding and targeting its prospects, customers, and employees. Security teams must detect and address them.

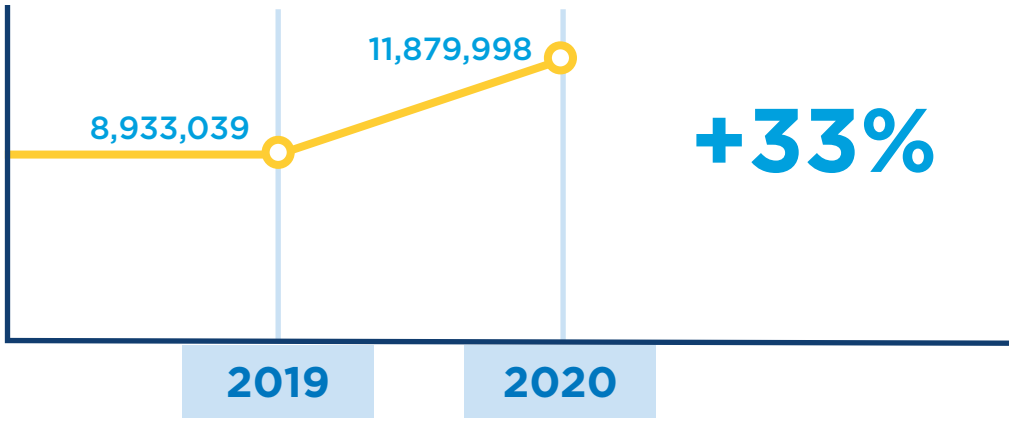
With a proactive, store-first scanning mentality, RiskIQ observes and categorizes the threat landscape as a user would see it, monitoring both the well-known stores like the Apple App Store and Google Play and more than 120 secondary stores around the world. RiskIQ also leverages daily scans of nearly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

This report will give a snapshot of 2020's mobile threat landscape and dive into emerging trends we anticipate carrying into 2021.

The App Ecosystem Got Bigger in 2020

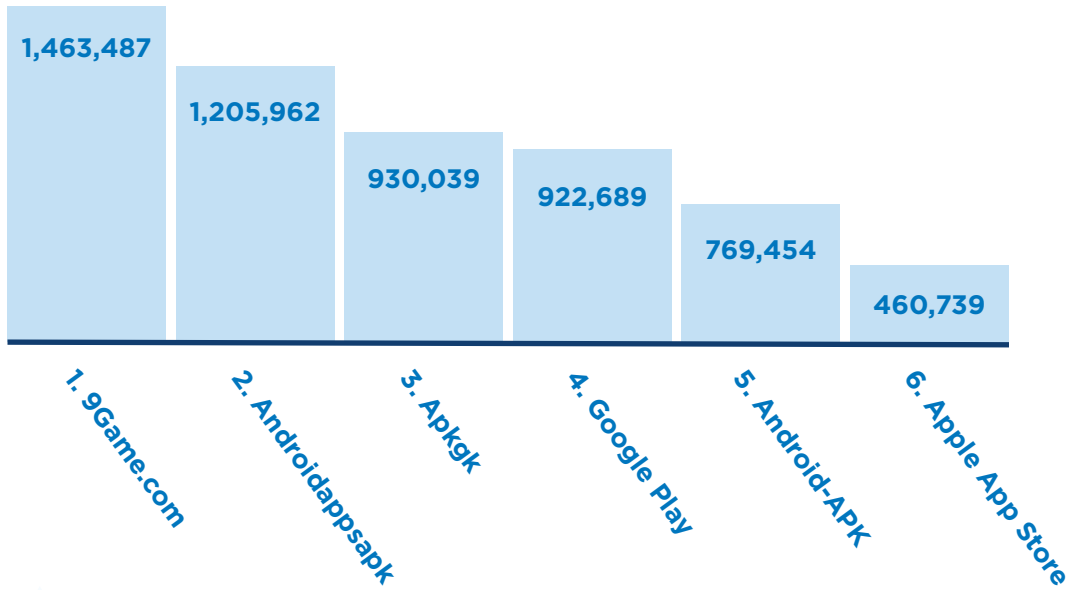
By any measure, the mobile landscape is getting bigger, busier, and more complex. RiskIQ cataloged 33% more apps worldwide in 2020 than in 2019.

Newly Observed Apps 2020:



China remains the largest app market, accounting for 40% of consumer app spending. The top-three most prolific app stores in 2020 were Chinese, ahead of both Google and Apple.

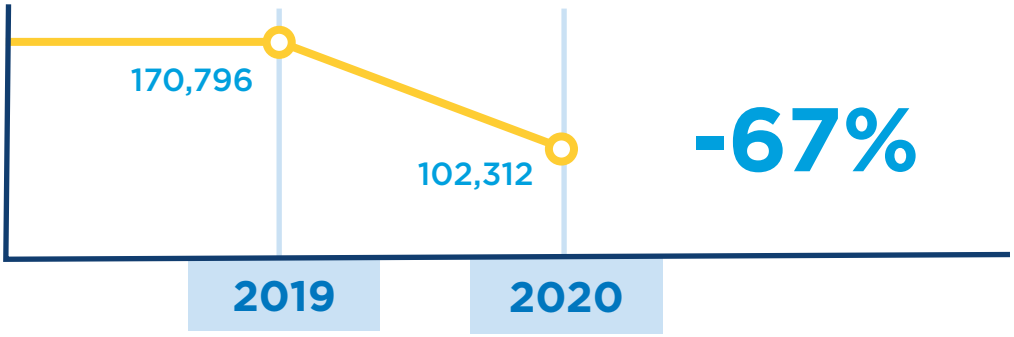
Most prolific stores of newly observed apps in 2020:



It Also Got Safer

Although new threats arose to take advantage of events such as COVID-19 and the election, it appears the mobile app ecosystem got safer overall in 2020. RiskIQ's Internet Intelligence Graph cataloged 30% more apps in 2020 but noted only 102,312 blacklisted apps*, more than 67% fewer than in 2019.

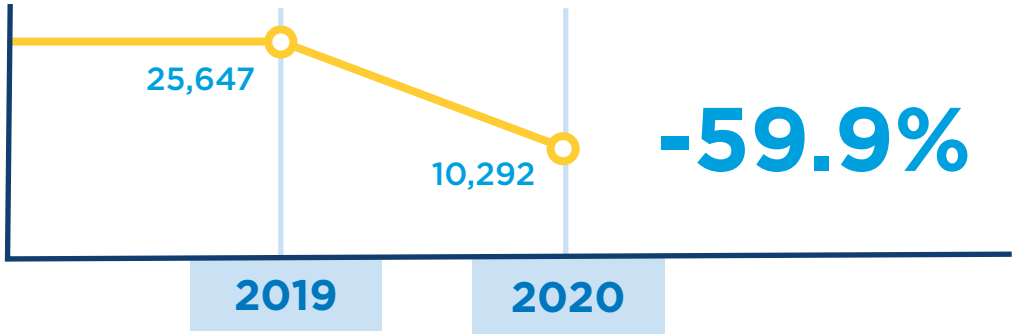
Total Blacklisted Apps in 2020:



Google is Cracking Down

Apple treats its App Store like Fort Knox and rarely hosts dangerous apps. Google Play's reputation in this regard is not quite as good. However, its 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 60% in 2020. We've found that blacklisted apps have now fallen in Google Play for two consecutive years.

Blacklisted Apps in the Google Play Store in 2020:

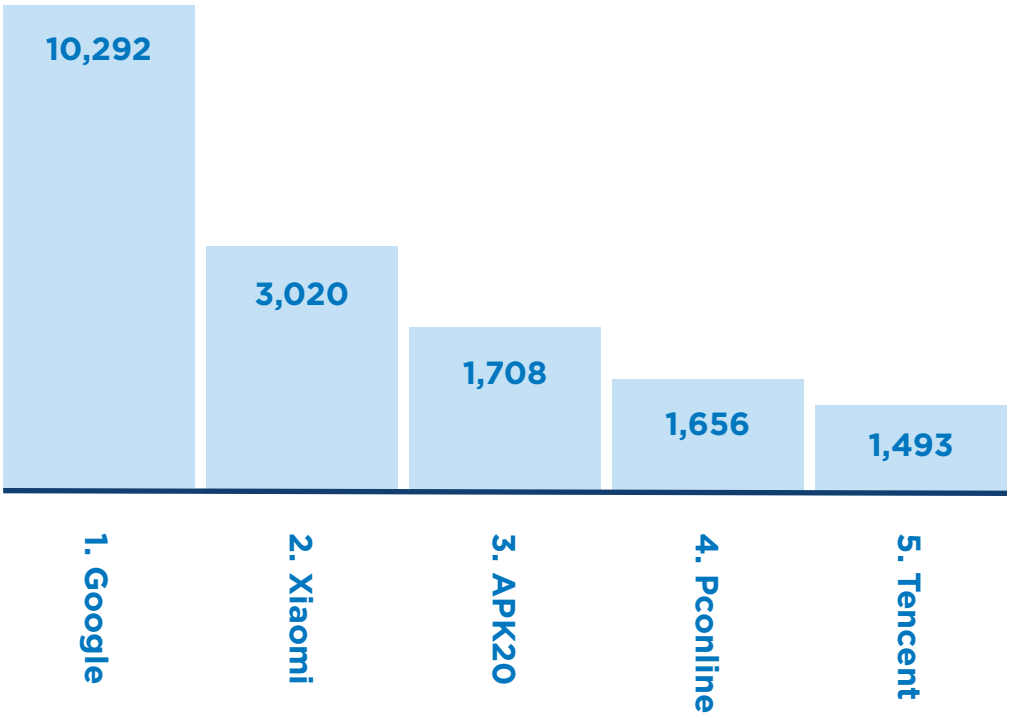


* Blacklisted apps appear on at least one global blacklist, such as VirusTotal, which, per its website, inspects files or web pages with over 70 antivirus products and other tools. A blacklist hit from VirusTotal shows that at least one vendor has flagged the file as suspicious or malicious.

Leading Blacklisted App Offenders

Because leading app stores like the Apple App Store and Google Play are inhospitable for malicious apps, threat actors must turn a profit elsewhere. However, there are hundreds of stores worldwide where 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.

The most prolific stores of blacklisted apps in 2020 were:



Some app stores are more dangerous than others and have a higher concentration of malicious apps. In 2020, these were the stores from which you were most likely to download a malicious app:

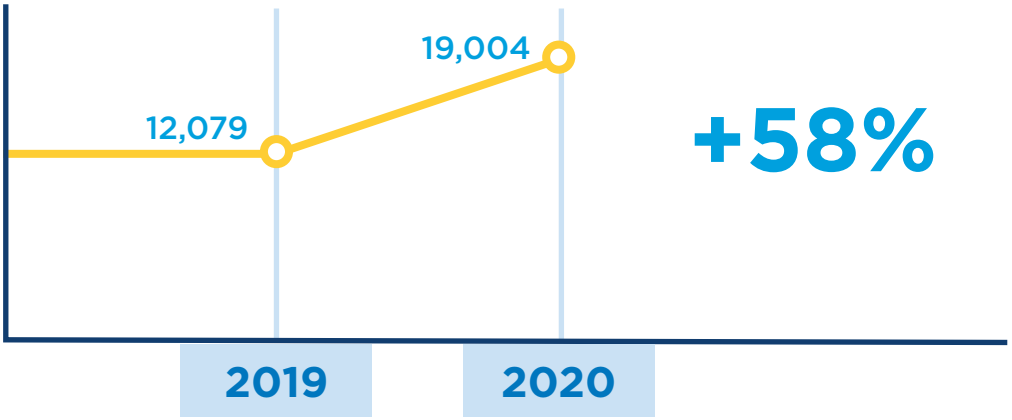
1. Xiaomi
2. Baidu
3. Pconline
4. AppLenovo
5. APK20

Top blacklisted app offenders lost their bite: In 2020, individual app stores seemed to host fewer blacklisted apps than in years past. The stores with the top-three most blacklisted apps accounted for 112,407 blacklisted apps. In 2020, that number shrunk to 15,020.

Blacklisted apps went feral: Many threat actors seemed to eschew app stores altogether. In 2020, RiskIQ data showed that Feral apps were responsible for the most blacklisted apps. Despite blacklisted apps falling 67%, blacklisted feral apps rose nearly 58%.

9Game.com, a usual suspect: While its blacklisted offering dropped in 2020, 9Game.com, 2019's most dangerous app store, topped the list of 2020's most prolific app sellers. This will be a situation to monitor closely over the next year.

Blacklisted feral apps in 2020:



2020 Mobile Threat Highlights By Quarter

Q1: Mobile Pay Dismay: A report by Upstream found that 93 percent of the 1.71 billion mobile transactions it analyzed were fraudulent. According to the report, these fraudulent payments would have cost victims $2.1bn in unwanted charges. Secure-D reported that five popular Android apps alone, totaling nearly 700 million downloads, accounted for 353 million suspicious mobile transactions. They were detected and blocked but would have resulted in $430 million in fraudulent charges. These apps had all been at some point available on the Google Play Store.

Q2: COVID Copycats: With the COVID-19 pandemic now in full swing, threat actors took advantage of the world's increased reliance on mobile apps for news and information on the crisis. Bitdefender released a report showing a massive spike in apps leveraging COVID-19-related keywords and imagery. However, many were unrelated to the virus, and some apps "contained aggressive adware or were bundled with malware."

To date, RiskIQ has detected 506 COVID-related apps in official stores and 2,042 in secondary stores. Of these, 28 are blacklisted, including two that reside in official stores.

Q3: Mobile Mistrust: Tiktok and other Chinese-owned mobile apps came under intense scrutiny due to concerns over privacy and security controls. The FBI also issued a warning that increased use of banking apps could play into threat actors' hands. With the election just a few months away, voting apps were also examined closely. RiskIQ systems surfaced 152 unauthorized applications comprising 16 state elections, some of which may have been copied or developed to misinform American voters.

Q4: Black Friday Blacklist: To analyze the methods these cybercriminals would employ over Holiday Shopping events and where they're targeting their efforts, RiskIQ ran a keyword query of our Global Blacklist and mobile app database focusing on top e-commerce brands. These brands had a combined total of 1,654 blacklisted apps that contain their branded terms in the title or description.

Conclusions

2020 continued mobile's wild growth, with RiskIQ noting 33% more apps and App Annie reporting massive increases in mobile usage and spend, which were accelerated by the COVID-19 pandemic. While new threats arose to take advantage of the pandemic and these new consumer habits, the overall mobile app ecosystems got safer, with blacklisted apps dropping significantly for the second consecutive year.

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 protect 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 the number of downloads, where present, also help to reassure 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 essential. Still, having visibility into apps in lesser-known app stores across the world—and across the web—is paramount.

Extending security and IT protection outside the firewall requires mapping these billions of relationships between the internet components belonging to every organization, business, and threat actor on Earth. These include mobile apps. RiskIQ built our Internet Intelligence Graph to prepare enterprises for this reality by enabling them to discover unknowns across their attack surface and investigate threats to their organization.

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

sales@riskiq.net

1 888.415.4447

Learn more at riskiq.com