



The Q1 2019

# Mobile Threat Landscape Report

**Blacklisted Apps Rise, Harmful Antivirus  
Apps Remain Prevalent**

By Jordan Herman





RiskIQ monitors

**120+**

mobile app stores

---

Leveraging

**2 billion**

daily scanned resources

The digital revolution is causing businesses to venture outside the safety of corporate perimeters into the expanses of the open internet where they can make more frequent and more meaningful touchpoints with employees, prospects, and customers. Unfortunately, this also makes them a target for a new breed of attackers that level internet-scale threats at their digital attack surface, a varied collection of client-facing assets outside the firewall that hackers can and will discover as they research their next threat campaigns.

A significant portion of this attack surface is the mobile channel.

The size, scope, and complexity of the global app ecosystem make it difficult for organizations to map and monitor their mobile presence and protect their customers and employees from bad actors. For the past 10 years, RiskIQ has applied its crawling platform, which monitors 120+ mobile app stores around the world and leverages our daily scans of nearly two billion resources, to look for mobile apps in the wild.

With a proactive, store-first scanning mentality, RiskIQ observes and categorizes the threat landscape as a user would see it. Every app we encounter is downloaded, analyzed, and stored. RiskIQ also records changes and new versions of apps as they evolve.

In this report, we'll provide a brief overview of 2018's mobile threat landscape and dive into emerging trends in our Q1 2019 Mobile Threat research to help you better protect your company, employees, and customers.

# 2018 in Review

## A Year Driven by Google Play

Over the last four quarters, RiskIQ has cataloged over 8 million mobile apps, of which 217,982 were blacklisted. Google Play had the most total apps of any app store with nearly 1,400,000, more than three times that of the Apple App Store. AndroidAppsGame had the second-most with 961,171.

In fact, Google accounted for nearly 58% of all blacklisted apps in 2018 with 114,469—far more than any other store. The next most blacklisted store, ‘9Apps’, accounted for about 19% of the blacklisted app total. Feral apps (those observed on the open web outside of any store) made up almost 9% of all blacklisted apps.

Highlights:

- **Q1: Bitcoin Bonanza** - RiskIQ put out a press release on blacklisted apps masquerading as or associating themselves with Bitcoin exchanges, Bitcoin wallets, or just “cryptocurrency” in general, which was indicative of the rise of digital currencies and their attractiveness as an income stream for both crooks and legitimate businesses.
- **Q2: Attacks on myetherwallet.net** - By copying the MyEtherWallet website and adding malicious scripts, threat actors spun up a phishing page that looked and acted like the official MyEtherWallet site, but sent authentication data to C2 servers when the victim enters their password to access/decrypt their wallet. This attack highlighted the trend of threat actors targeting the cryptocurrency landscape.
- **Q3: Magecart Goes Mobile** - In 2018 RiskIQ broke several stories involving Magecart online card skimming. One of these was a breach of British Airways, which involved the compromise of the company’s mobile app. Since the British Airways app loaded content from the official British Airways website the Magecart actors responsible for the breach were able to skim data from mobile app users just as they skimmed it from web users, through a compromised JavaScript library. 380,000 customers in total were affected by this breach.
- **Q4: Black Friday Blacklist** - To analyze the methods these cybercriminals would employ over Black Friday and Cyber Monday 2018 and where they’re targeting their malicious efforts, RiskIQ ran a keyword query of our unmatched Global Blacklist and mobile app database focusing on ten leading e-tailers. The results showed that Black Friday is a feast for threat actors. In total, RiskIQ [observed 52,885 blacklisted apps in Q2](#), which was 4% of all apps we saw and a 2% increase over Q1.

# Q1 2019: Running the Numbers

## Fewer blacklisted apps, Google is usurped

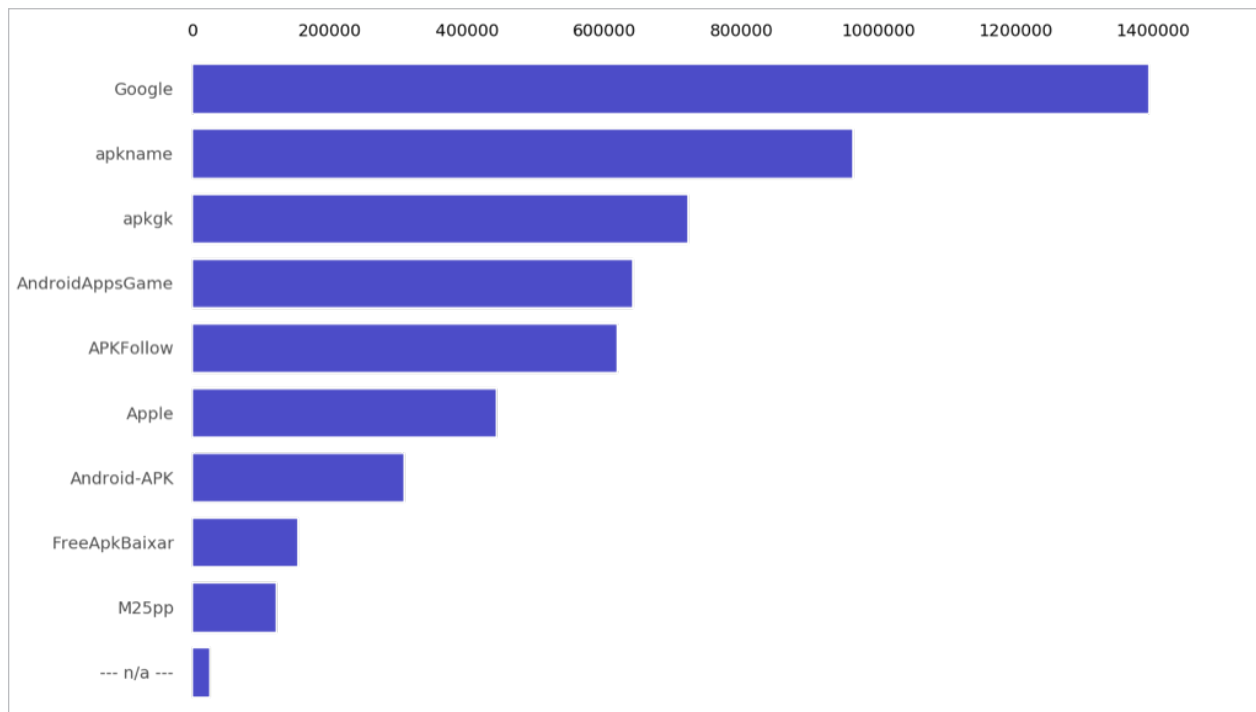
After three consecutive quarters of decline, Q1 showed a nearly 15% increase in blacklisted apps over Q4.

Blacklisted apps found 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. The percentage of Blacklisted apps relative to the total number of apps known by RiskIQ increased to nearly 2%, a .9% increase over Q4 2018.

These blacklisted apps featured a host of familiar threats such as brand imitation, phishing, and malware. The mobile threat landscape also saw attackers leveraging the [holiday shopping season](#) with malicious and fraudulent apps meant to fool consumers into downloading them.

Additionally, Q1 saw more research published on the [continued prevalence](#) of useless and malicious Android apps purporting to be antivirus, which RiskIQ has [reported on extensively](#).

In Q1, RiskIQ detected 2,263,268 apps, a nearly 6% increase from Q4 2018.



**Fig. 1: Total apps observed over the last 4 quarters**

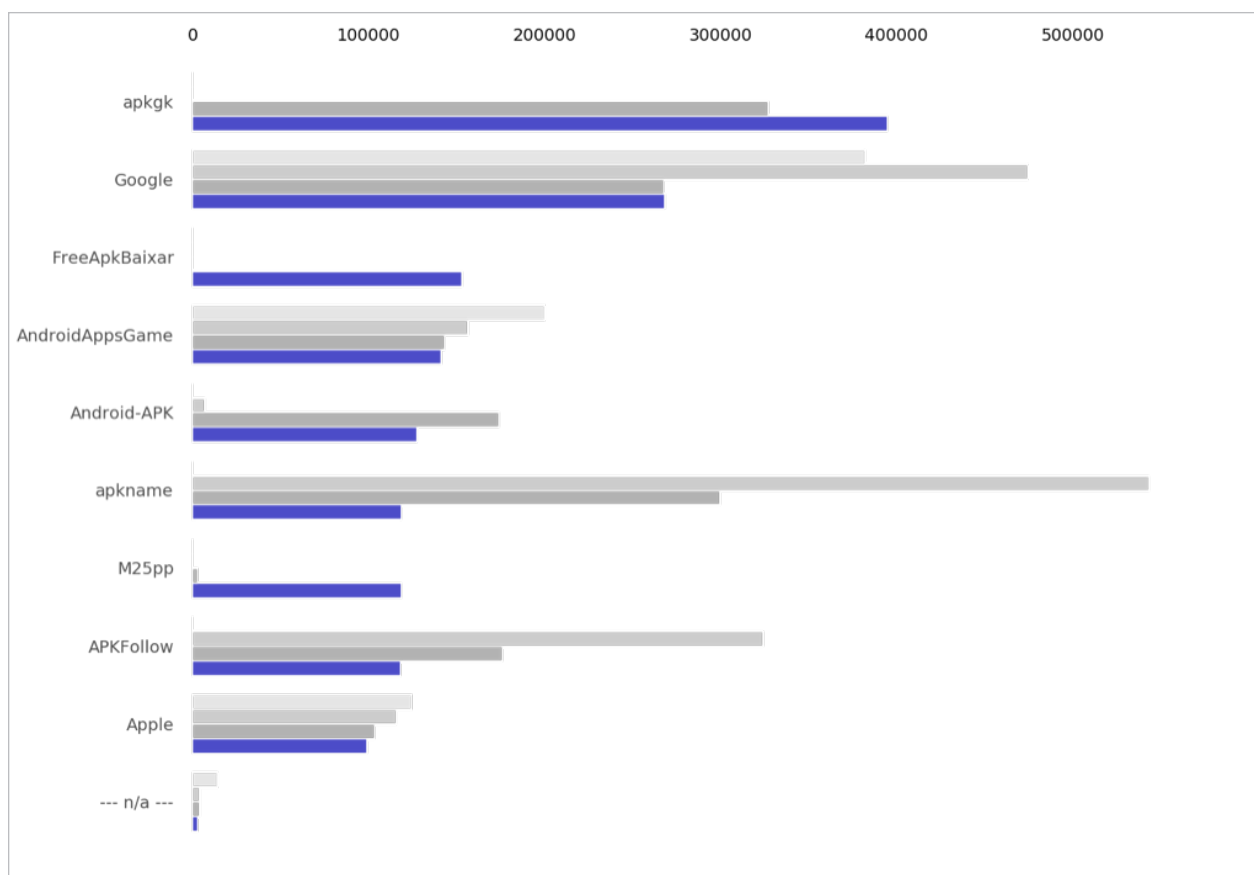
In Q1, blacklisted apps rose 14.5% from 37,592 to 43,049, accounting for nearly 2% of all apps. The number of blacklisted apps in the Google Play Store dropped for the second consecutive quarter and fell nearly 64% in the second half of 2018. In Q1, the store '9Game.com' hosted the most blacklisted apps of any store with 17,059, dethroning Google Play as the most prolific blacklist supplier for the first time in three quarters.



**Fig. 2: Blacklisted apps per quarter**

For the second-straight quarter, RiskIQ added over two million new apps to our database, partially due to RiskIQ's ever-expanding list of monitored mobile app stores, but also because of the continued explosive growth of the mobile app market. In Q1, RiskIQ observed 2,263,268 new apps, 123,415 more than were observed in Q4 2018.





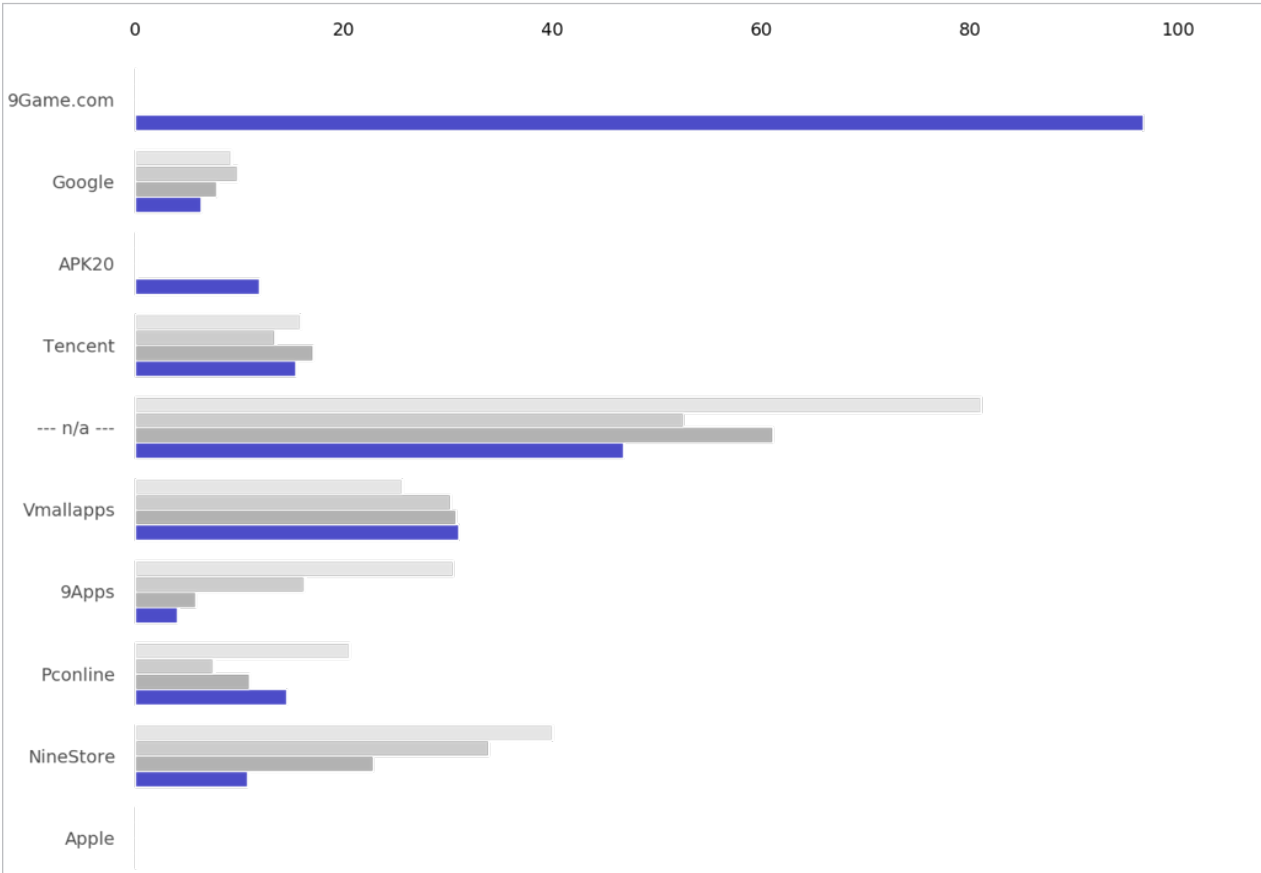
**Fig. 3: Newly observed apps per quarter**

In Q1, Google added 268,230 new apps, a total that has decreased for three-straight quarters. Apple is also added fewer apps each of the past 4 quarters, but adding them at only half the rate of Google. Despite minor fluctuations, the app market continues to be dominated by Google and trends within the Play Store drive those in the marketplace as a whole. Over the past four quarters, Google has added 31% more apps than the next most prolific supplier.

For the second-straight quarter, 'apkgk' beat the field as Q1's top app-adder. Two stores RiskIQ added to our detection in Q3 that added six-digit app numbers for the rest of the year, apkname and APKFollow, were again extremely prolific in Q1. However, a store RiskIQ added to our detection in Q1, FreeApkBaixar finished behind only Google and apkgk, showing the volatility of the global app market.

Turning once again to blacklisted apps, it is evident that the number of malicious apps in Google's store has grown apace with its legitimate offerings. Over Q4 2018 and Q1 2019, nearly 38,000 apps offered by Google were blacklisted, over 20,000 more than the next most blacklisted store, 9Game.com.

However, the percentage of blacklisted apps in Google’s store remained relatively low in Q1 at 6.3%, slightly lower than Q4. Meanwhile, 96% of apps in the 9Game.com and 30% of apps in ‘Vmallapps’ were blacklisted, and nearly half of all Feral apps were found to be malicious. Chinese app store Tencent decreased from 17% to 15% blacklisted, while another Chinese app store, NineStore, fell from around 22% malicious apps to only 10%.



**Fig. 4: Percentage of apps blacklisted per quarter**

## Developments

**How the Grinch went mobile:** To examine the cyber threat landscape over the 2018 holiday shopping season, RiskIQ conducted research using the RiskIQ Global Blacklist and mobile app database\* looking for instances of malicious apps and URLs targeting 10 of the most trafficked brands on Black Friday. [The findings included](#) over 16,800 blacklisted apps and confirmed that cyber threat activity was consistent through the holiday shopping season, with cyber threat actors leveraging these ten mega-popular brands across both web and mobile.

**More harm than good:** For years, RiskIQ has been reporting on fake antivirus apps that claim to be helpful but are at best useless. In Q1, [Wired published](#) more research confirming the phenomenon. “In a survey of 250 antivirus apps found in the Google Play Store, only 80 demonstrated basic competence at their jobs by detecting 30 percent or more of the 2,000 malicious apps AV-Comparatives threw at them. The remainder either failed to meet that benchmark, frequently mistook benign apps for malware, or have been pulled from the Play Store altogether.”

## 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. Watch out for malicious apps mimicking reputable, highly downloaded apps. There is a persistent problem of lookalike apps. This tactic is effective because our brains recognize and make instantaneous judgments about visual stimuli. So, when you see an app with the same logo as that popular encrypted messenger, it is easy to choose it without noticing that the name has a trailing period that should not be there.

You should also check an app’s permissions to make sure it does not have access beyond its stated functionality. Although they cannot make up for preventative measures such as checking permissions, anti-malware products provide some protection from malicious code. 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.



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.

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

✉ [sales@riskiq.net](mailto:sales@riskiq.net) 🌐 [RiskIQ.com](http://RiskIQ.com)  
☎ 1 888.415.4447 🐦 [@RiskIQ](https://twitter.com/RiskIQ)

Copyright © 2019 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 06\_19

The only warranties for RiskIQ products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. RiskIQ shall not be liable for technical or editorial errors or omissions contained herein.