The Q2 2019

Mobile Threat Landscape Report

Blacklisted Apps Increase 20%, Attackers Target Tax Season

By Jordan Herman

RiskIQ monitors

120+

mobile app stores

Leveraging

2 billion

daily scanned resources

The digital revolution is causing businesses to invest significantly in mobile, where they can make more frequent and more meaningful interactions with employees, prospects, and customers. Global app spending hit $101 billion in 2018 and will surpass that this year. However, mobile is a significant portion of the overall corporate attack surface that exists beyond the firewall, where security teams often suffer from a critical lack of visibility.

Rogue mobile assets such as fake apps are purpose-built to fool customers into downloading them by impersonating legitimate businesses. Once downloaded, they can phish users for sensitive information or upload malware to their devices. For businesses, even though they don't own or manage these apps, they're still responsible for detecting and addressing them.

For the past ten years, RiskIQ's discovery platform has mapped the global mobile threat landscape. It now monitors more than 120 mobile app stores around the world and scans nearly two billion resources daily to look for mobile apps in the wild. With this internet-wide telemetry, RiskIQ observes and categorizes the threat landscape as a user would see it, downloading analyzing, and storing every app we encounter while recording changes and new versions.

In this report, we'll provide an overview of the Q2 2019 Mobile Threat Landscape and dive into emerging trends you need to know for the rest of the year.

Q2 2019: Running the Numbers

Blacklisted Apps Surge

Blacklisted apps increased with a **20%** spike

For the second-consecutive quarter, blacklisted apps increased with a 20% spike, increased from 44,850 to 53,955, and accounting for over 2% of all apps in RiskIQ's dataset. 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.

The percentage of blacklisted apps relative to the total number of apps known by RiskIQ also increased for the second-straight quarter, jumping from 1.95% to 2.1 %.

These blacklisted apps featured a host of familiar threats such as brand imitation, phishing, and malware. The mobile threat landscape also saw attackers leveraging tax season with malicious and fraudulent apps meant to fool consumers filing their taxes into downloading them.

Additionally, Q2 saw an influx of heavily downloaded Android apps that abuse permissions and contribute to ad fraud, as well as the emergence of a sophisticated spy app dubbed Exodus that can access sensitive data such as pictures and contacts. Initially designed for Android, the app made its way to the Apple App Store.

The Global App Deluge Continues

App downloads increased by **11%**

App downloads are on the rise, predicted to reach 260 billion worldwide by 2022, and according to RiskIQ data, the supply has risen to meet that demand. In Q2 2019, RiskIQ observed 2,554,616 apps, a nearly 11% increase from Q1.

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, which saw 194 billion downloads in 2018, up from 178 billion in 2017.

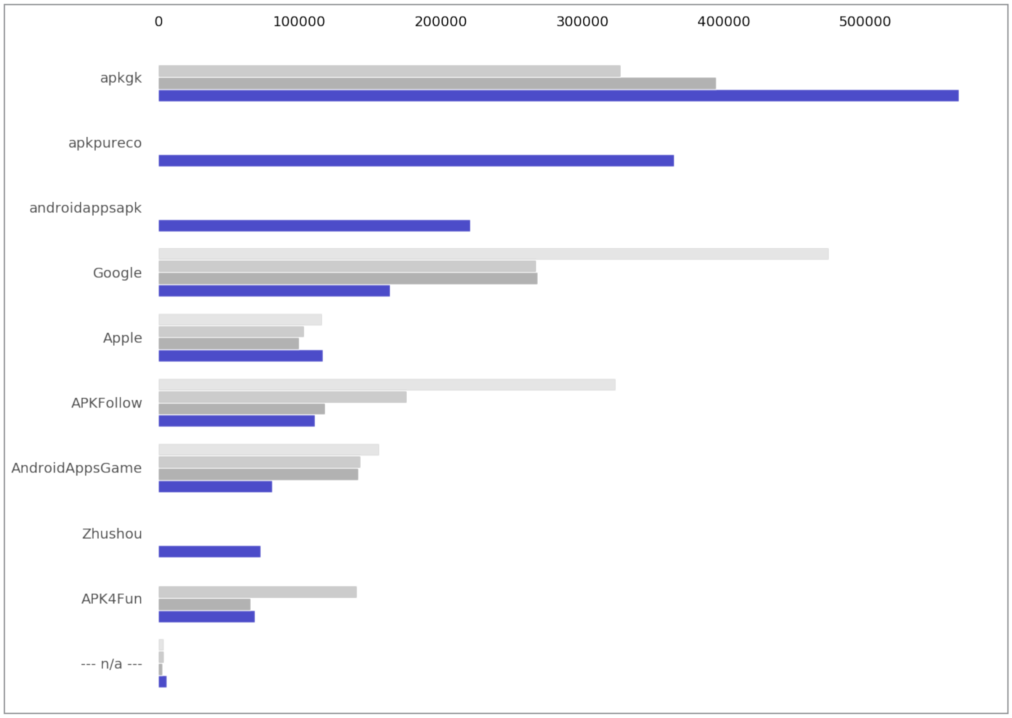

Fig. 1: Newly Observed Apps Per Quarter

App market continues to be dominated by **Google**

Google is typically the most prolific app supplier, but it only added 164,101 new apps in Q2, 38% fewer than Q1, and 189% fewer than the 474,663 it added in Q3 2018. Meanwhile, the Apple App Store continues to add apps at a much steadier pace, only increasing its inventory by 14.3%, or 116,210. This data reflects the activity within the Google Play and Apple App stores as a whole—of the 105 billion app downloads made through Google Play Store and iOS App Store, 76 billion come from 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. However, Q2 represented one of those fluctuations. From Q2 2018 to Q1 2019, Google added 31% more apps than the next most prolific supplier but was only the fourth-most prolific supplier in Q2 2019.

For the third-straight quarter, Apkgk beat the field as the top app-adder, followed by two stores RiskIQ recently added to our telemetry, 'apkpureco and 'androidappsapk,' which added 365,154 and 220,893 respectively.

However, don't expect this trend to continue. Over a long enough timeline, Google will almost certainly regain the top spot, and Apkgk's proliferation will decline.

Google Play is Getting Safer

Number of blacklisted apps in the Google Play Store decreased by **59%**

In Q2, blacklisted apps rose by 20%. However, despite the proliferation of blacklisted apps in Q2, the number of blacklisted apps in the Google Play Store decreased by a dramatic 59%. In fact, the percentage of blacklisted apps in the Play Store has declined steadily over the past four quarters. But is this reduction in malicious apps a result of a new commitment to safety by Google, or just fewer apps being added in general?

The answer could be both.

Google's security controls have always allowed some blacklisted apps to enter its store at a level they find acceptable. Therefore, the percentage of malicious apps in the Play Store typically grows or declines apace with its legitimate offerings. With Google adding 39% fewer apps in Q2, it stands to reason its blacklisted count would drop as well.

However, Google *has* been putting more emphasis on safety, pushing security updates more often, and enabling users to decide which permissions they want to accept in each app. Google has also enabled security programs that allow them to better monitor apps in the Play Store for Malware.

Abandon Security All Ye Who Enter Here

Vmallapps was a top blacklist supplier with **31%** of apps blacklisted

Google added 7,291 blacklisted apps in Q2, but its commitment to safety is keeping the percentage of blacklisted apps hosted in the Play Store low and dropping each quarter. However, there are some stores where you're almost guaranteed to download a malicious app if you choose to patronize it.

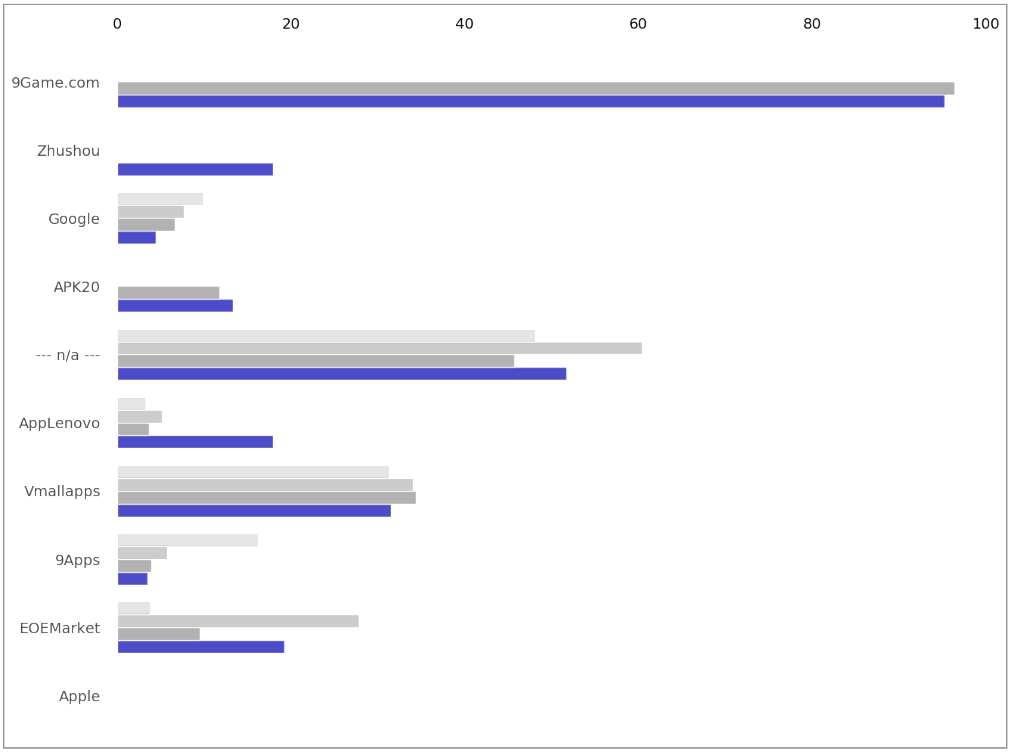

Fig. 2: Percentage of Apps Blacklisted Per Quarter

The app store '9Game.com' has flooded the market with blacklisted apps over Q1 and Q2, adding 34,880. Its total of 17,858 blacklisted apps in Q2 represented a staggering 95% of the total apps in its store. Another Chinese store, 'Zhushou,' added 12,972 blacklisted apps in Q2, 17% of its overall offering. "Vmallapps' was again a top blacklist supplier, with 31% of its offerings blacklisted.

As usual, feral apps, or apps not in any store and downloaded directly from the internet, proved to be exceptionally dangerous, with a 51% blacklist rate. Quarter after quarter, the data confirms that apps downloaded outside of the Google Play store and the Apple App Store are riskiest.

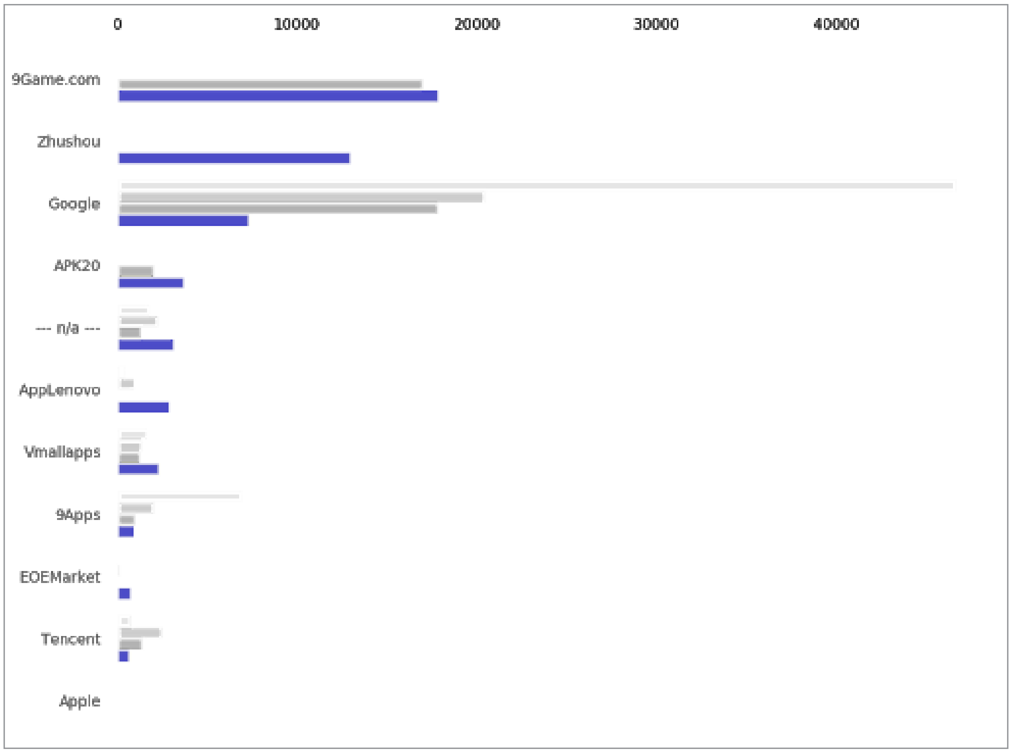

Fig. 3: Blacklisted Apps Per Quarter

Developments

30% of blacklisted apps discovered matched terms relating to the IRS or tax filing software

Victims Pay Twice: During tax season, criminals are happy to exploit the convenience of popular e-filing systems such as H&R Block and TurboTax via fake mobile apps. To analyze the methods these actors employed during tax season, and where they targeted their malicious efforts, RiskIQ ran a keyword query of the RiskIQ Global Blacklist and mobile app database looking for instances of terms related to the IRS and the brand names of ten of the leading tax filing software. The research found 4,162,450 total apps matching these branded terms in app stores around the world. 1,221,070 (or 30%) of those were found to be malicious.

More harm than good: TechCrunch's Zack Whittaker reported that security researchers had discovered a powerful surveillance app first designed for Android devices targeting victims with iPhones. The Android app, dubbed Exodus, affected hundreds of victims, who installed the app or had it installed. The Android version had a more extensive set of features and more spying capabilities via an additional exploit designed to gain root access to the device, giving the app near-complete access to the victim's data, including emails, cellular data, Wi-Fi passwords, and more.

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 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.

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