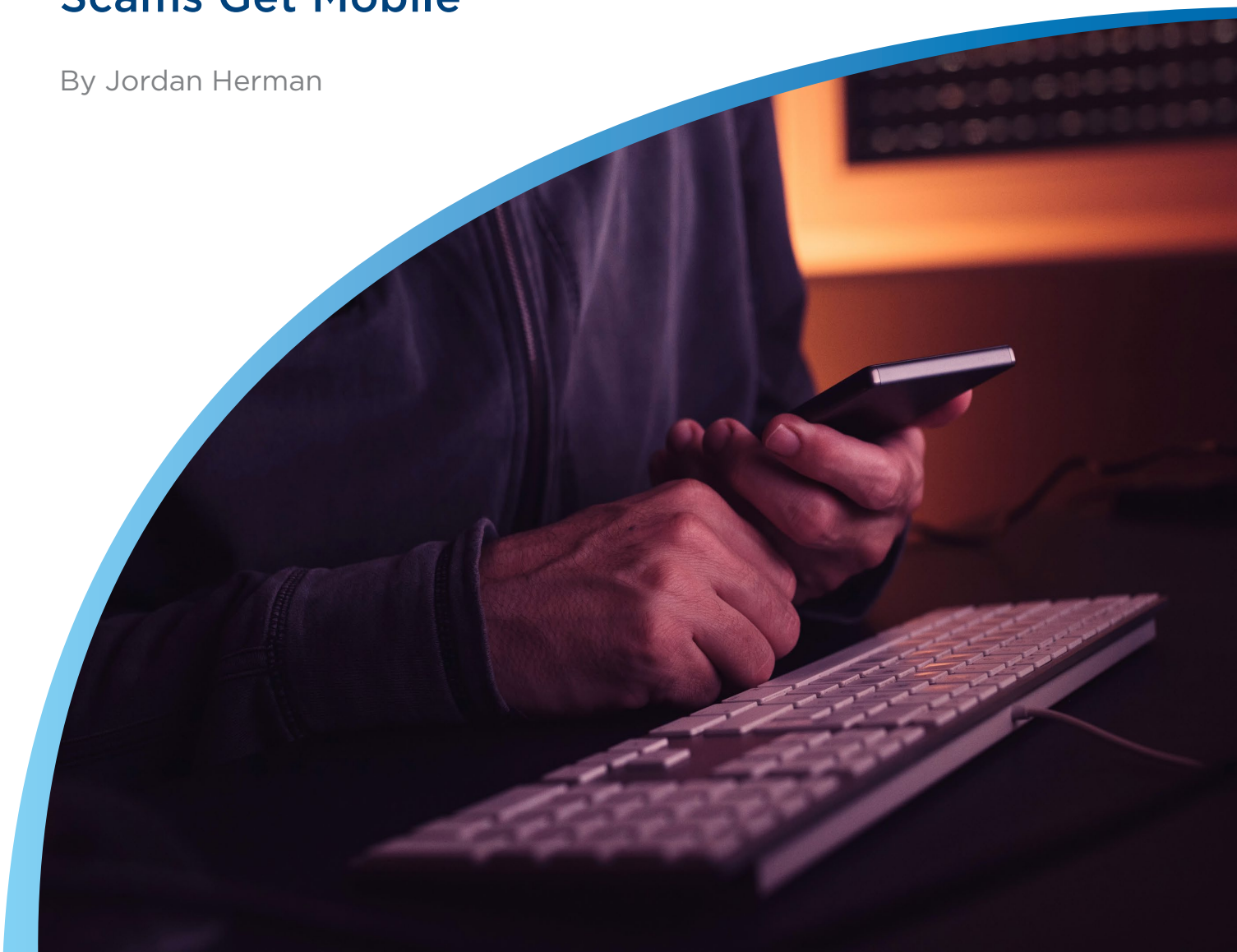
RISKIQ®

The Q2 2018

Mobile Threat Landscape Report

Blacklisted Apps on the Rise as Scams Get Mobile

By Jordan Herman



RiskIQ monitors

120+

mobile app stores

Leveraging

2 billion

daily scanned resources

Introduction

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. To highlight the mobile threat landscape in the second quarter of 2018, RiskIQ applied its crawling platform, which monitors 120+ mobile app stores around the world and leveraged our daily scans of nearly 2 billion resources to look for mobile apps in the wild.

Q2 showed a nearly 57 percent increase in blacklisted apps over Q1 but featured a host of familiar threats such as brand imitation, phishing, and malware—as well as new ones including malvertising scams crossing int the mobile realm, the use of apps to target users of MyEtherWallet, and the misuse of location data by major mobile providers.

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 give an overview of these mobile threats, as well as emerging trends we anticipate will be prevalent in the future, to help you protect yourself and your customers.

Running the Numbers

Google is Once Again the Busiest App Store

RiskIQ saw 1,427,286 apps in Q2 of 2018, 81,539 less than in Q1. Google Play added by far the most new apps with 376,774, followed by AndroidAppsGame at 199,541, and Apple at 116,951.

Aptoide, after adding 483,175 apps in Q1 only added 61,784 in Q2, a decrease of 87%. Aptoide was added to our data shortly before Q1, so our numbers for Q2 are more indicative of the rate at which new apps are added to the store. Aptoide remains in the top-three app stores for total apps seen over the last four quarters at 544,955, behind AndroidAppsGames (678,058) and Google Play (750,947). AndroidAppsGames consistently adds around 200,000 apps each quarter since we began tracking it around Q4 of 2017.

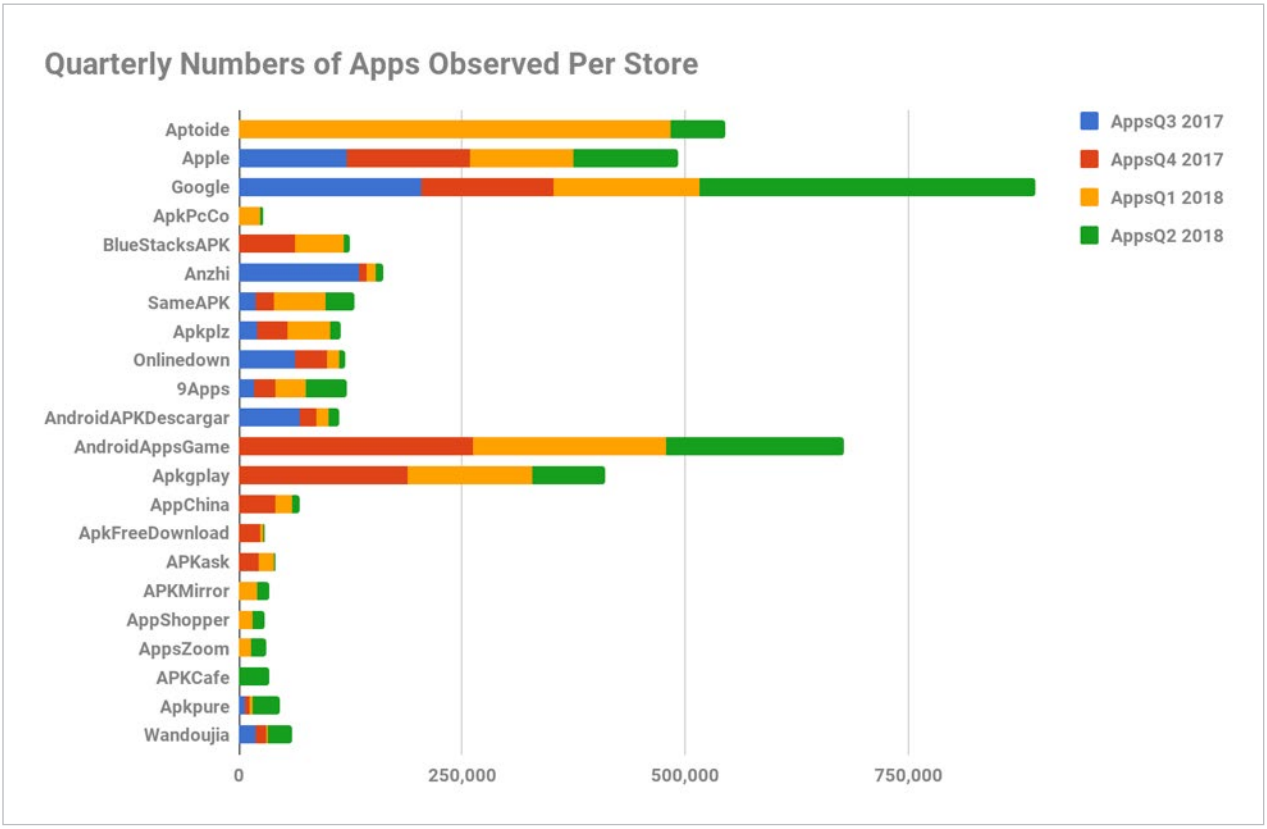


Fig. 1: Once again, Google leads the pack with most apps and most apps added

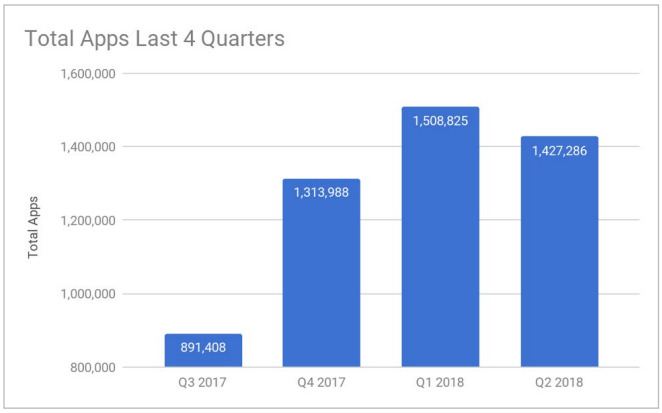


Fig. 2: Total apps observed by RiskIQ slightly dipped in Q2

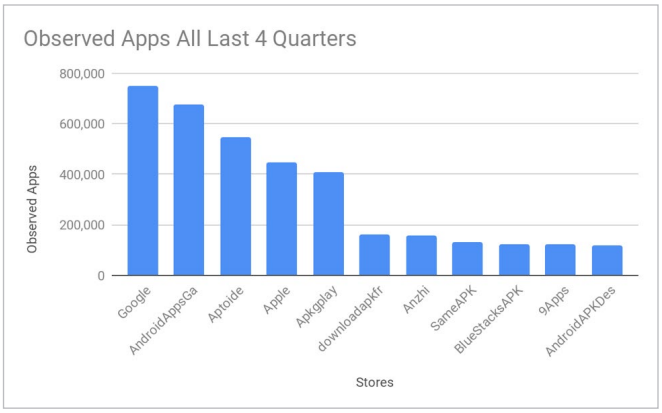


Fig. 3: Google Play consistently hosts the most apps of any store

Blacklisted apps made up 4% of all apps in Q2 at 52,885. This number is an increase of two percentage points and 23,000 apps over the low Q1 numbers, but it is also 35,851 and six percentage points fewer blacklistings than in Q3 of 2017.

Note: our stats for Q3 have been corrected from our previous report as post-processing led to a significant increase in the number of blacklisted apps observed during that quarter.

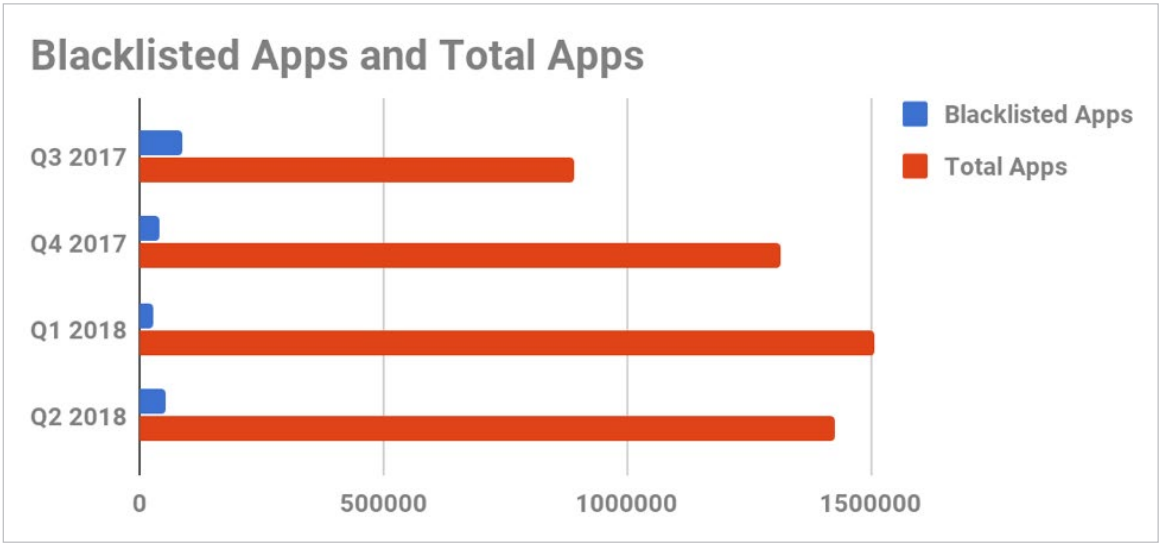


Fig. 4: Total apps observed by RiskIQ decreased in Q2, but the percentage of Blacklisted apps increased

When we compare blacklisted apps over time, we see a spike from May to June in 2017 and 2018, although this increase is much less dramatic in 2018 (there is an increase of around 30,000 apps in 2017, versus 12,000 in 2018). The June spike continues an upwards trend in blacklistings since the lows of January and February of this year. But 2018 numbers are still far lower than 2017 overall. It will be interesting to see if this upward trend continues and somewhat mirrors the previous year where an even decline followed highs in June and July through the latter half of the year. As of yet, there is little indication of a pattern.

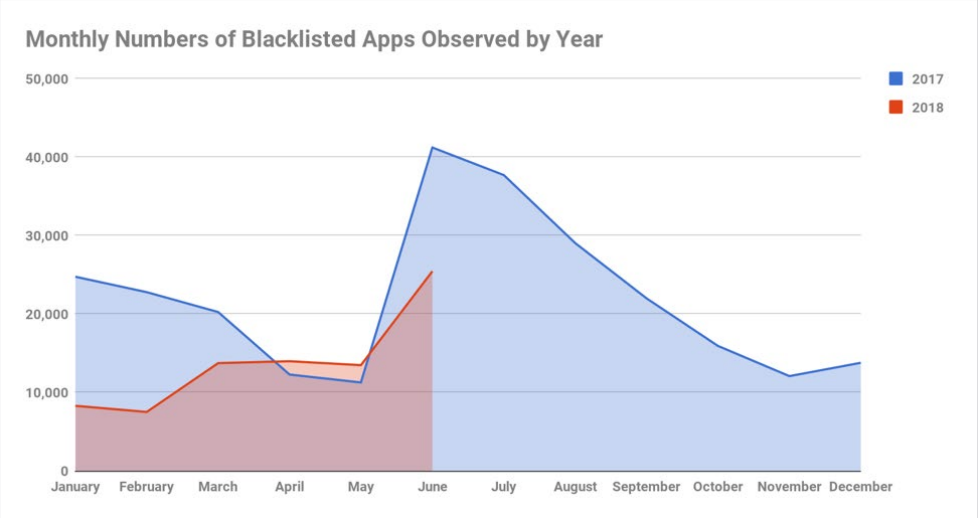


Fig. 5: For the second-straight year blacklisted apps increased in Q2

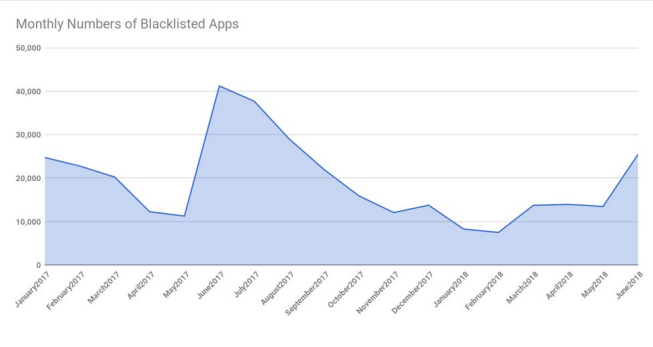


Fig. 6: Will Q3 2018 follow the trend of Q3 2017 and decline after a spike in Q2?

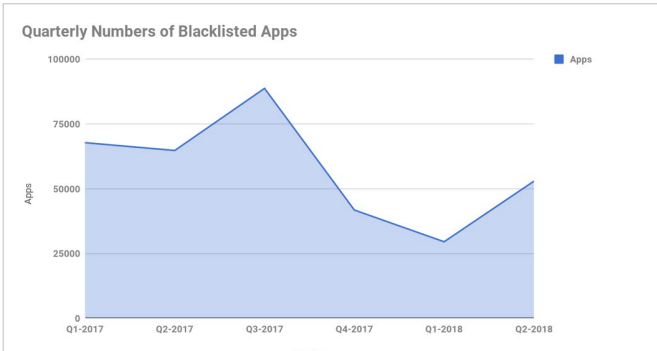


Fig. 7: Total blacklisted apps are down in 2018, but they're following a trend laid out in 2017

The number of blacklisted apps observed on Google Play increased by over 20,000 from Q1, 8,287, to Q2, 28,533. Previously, around 8,000 or 9,000 blacklisted apps were consistently observed in the Play store each quarter going back to Q1 of 2017. We also observed 11,288 blacklisted Feral apps (apps observed outside of any app store), 4,750 blacklistings in the 9Apps third-party store, and 2,985 blacklistings for AndroidAPKDescargar. The Play store curated over 2.5 times more blacklisted apps last quarter than the Feral App category and over six times that of the next most blacklisted store, 9apps.

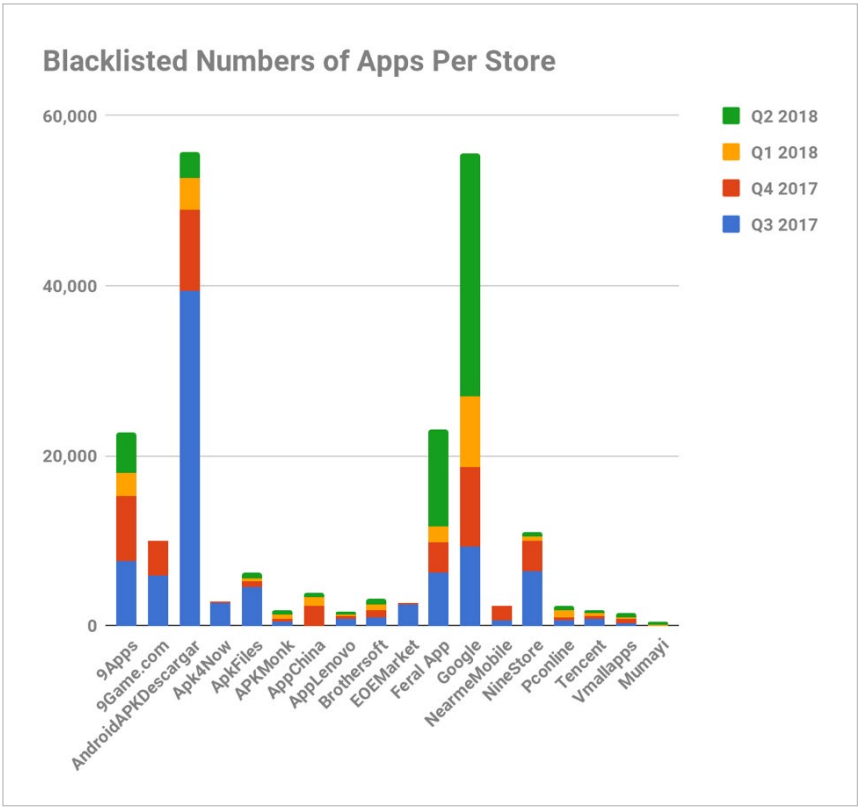


Fig. 8: The total apps in some leading stores ebb and flow, but Google Play always top the list

However, we also saw a much higher number of apps added to the Play store overall than in previous quarters meaning that the percentage of blacklisted apps in that store remained low, though it did increase from 5% in Q1 to 8% in Q2. 81% of Feral apps were blacklisted, an increase of 35 percentage points from Q1, while 9Apps and AndroidAPKDescargar were 10% and 24% blacklisted respectively. Other significantly blacklisted stores include ApkFiles (54%), Brothersoft (21%), Pconline (19%), and Mumayi (19%).

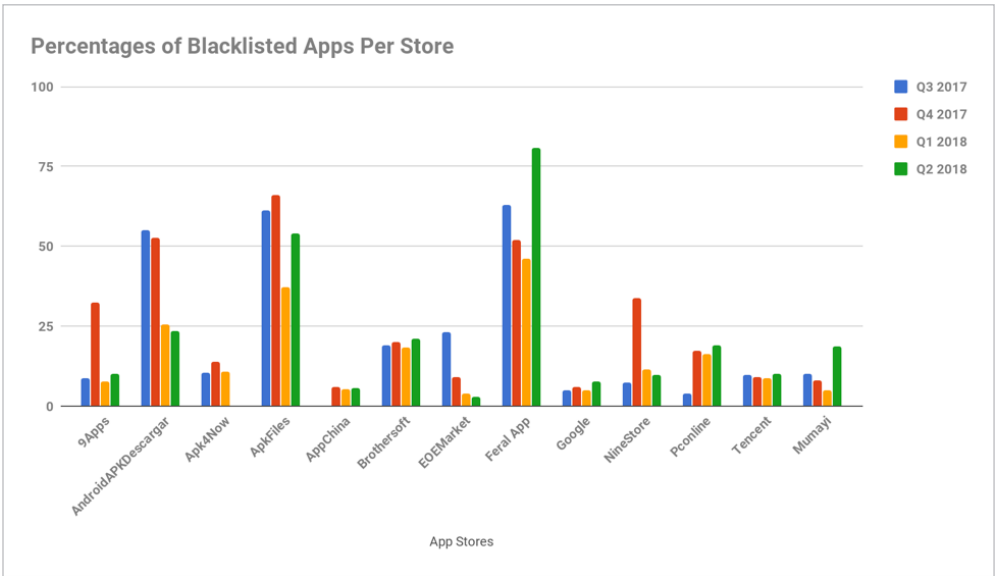


Fig. 9: Feral apps continue to be disproportionately dangerous

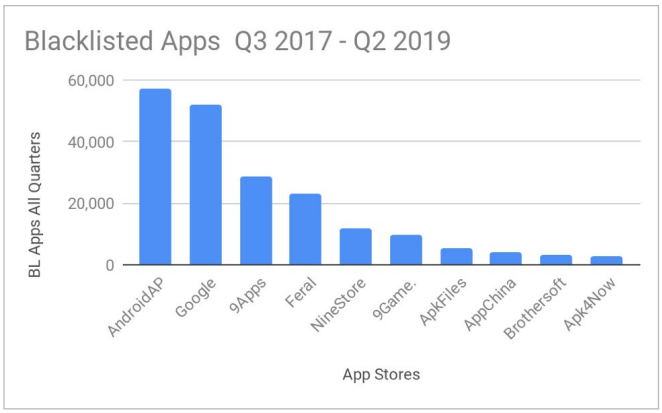


Fig. 10: AndroidAP leads the pack in blacklisted apps over the past years

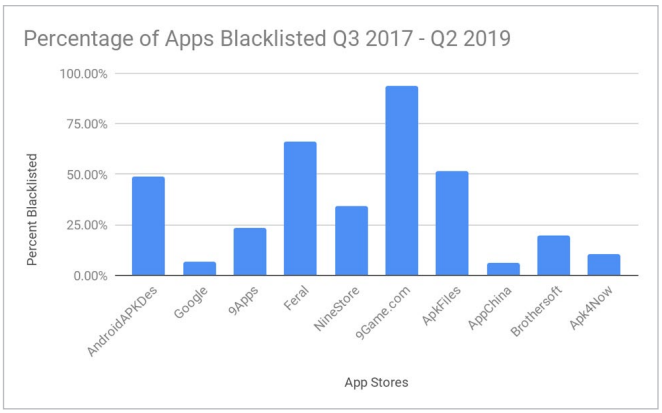


Fig. 11: 9Game.com had the highest percentage of blacklisted apps over the last year

Examining the blacklisted apps by the categorization assigned them by various antivirus vendors shows that Trojans and Adware dominate the types of malicious apps that are encountered. The next most numerous portion of blacklisted apps are miscellaneous blacklisted apps, followed by Spyware apps, then Botnet apps.

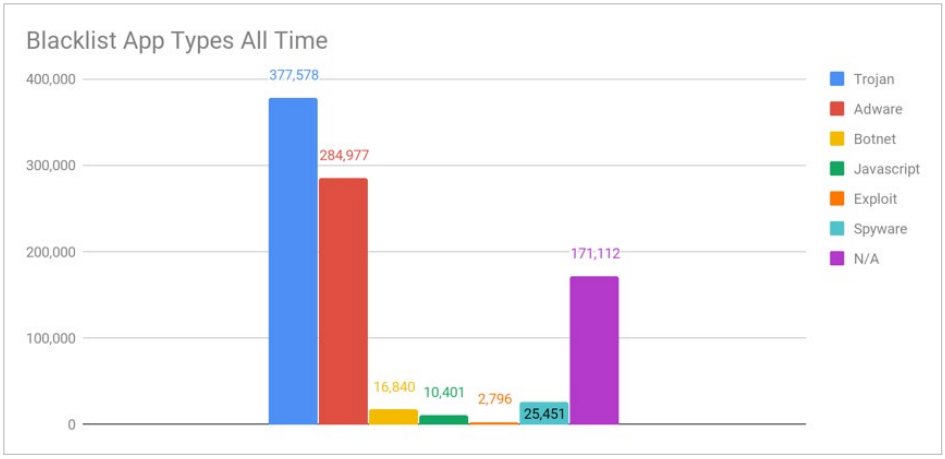


Fig. 12: Trojans are the most common type of blacklisted app of all time

This ratio was borne out over the period from Q1 2017 through Q2 2018 as well, with non-categorized apps outpacing trojans and adware in a few quarters. Additionally, apps the turn mobile devices into bots significantly increased in Q2 2018, with 6,266 observations. These botnet apps were mainly Feral, though 13 did appear in the Play store.

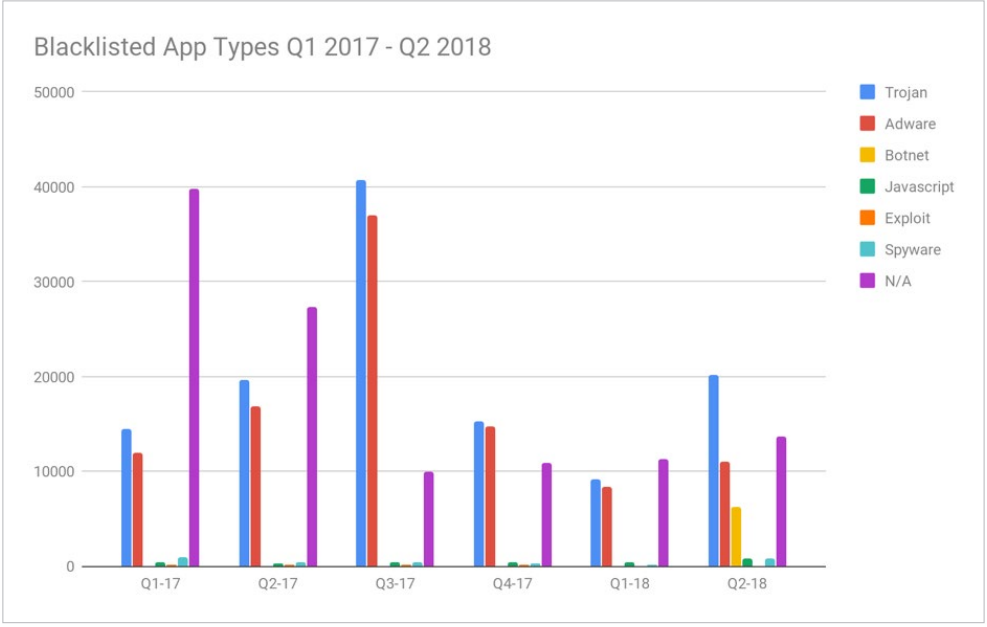


Fig. 13: Trojans remain the most popular, but uncategorized apps are skyrocketing in number

Totaling up blacklisted app types over the last four quarters and comparing each against the total number of blacklisted apps illustrates the ratio of each type to the total.

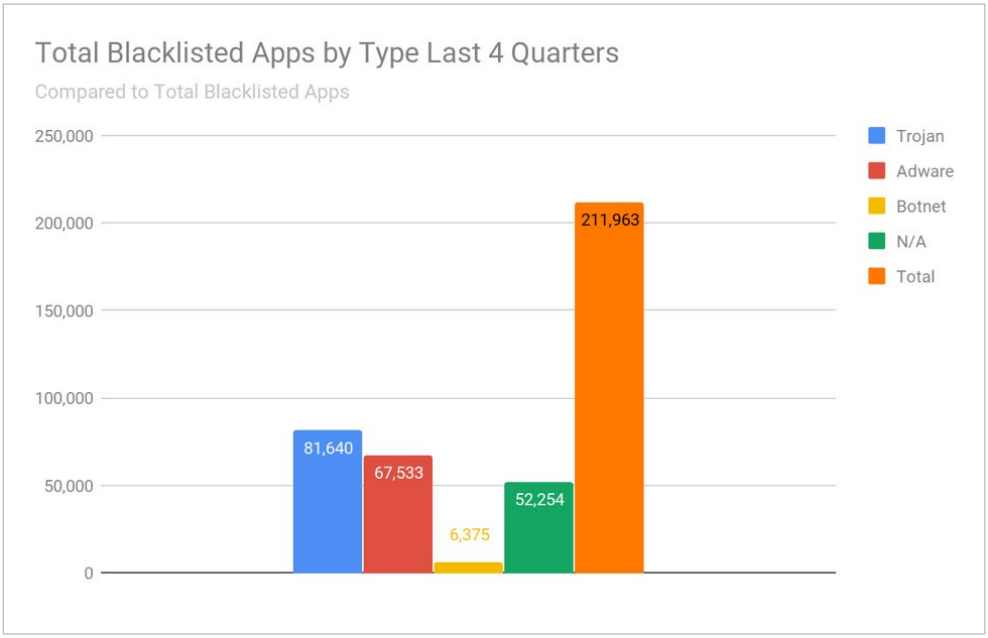


Fig. 14: Trojans and adware continue to lead the pack of categorized blacklisted apps

These tables illustrate the overlaps among types both in terms of numbers and percentages. Most app types significantly overlap with the Trojan type, which makes sense as “Trojan” is a rather wide-open designation for anything malicious program that tricks you into installing it. Most other blacklisted app types do not significantly overlap.

Blacklisted App Types Overlap Last 4 Quarters

	Trojan	Adware	Botnet	Spyware	Javascript	Exploit	
Trojan	81,640	52,296	6,363	1,583	1,329	85	Trojan
Adware	64.06%	67,469	20	849	577	23	Adware
Botnet	7.79%	0.03%	6,375	462	282	1	Botnet
Spyware	1.94%	1.26%	7.25%	1,759	37	1	Spyware
Javascript	1.63%	0.86%	4.42%	2.10%	1,912	26	Javascript
Exploit	0.10%	0.03%	0.02%	0.06%	1.36%	311	Exploit
%Trojan		77.51%	99.81%	89.99%	69.51%	27.33%	%Trojan

Blacklisted App Types Overlaps Q2

	trojan	adware	botnet	spyware	javascript	exploit	
trojan	20,158	5467	6263	795	688	28	trojan
adware	27.12%	11,065	4	223	195	8	adware
botnet	31.07%	0.04%	6266	446	274	1	botnet
spyware	3.94%	2.02%	7.12%	841	28	0	spyware
javascript	3.41%	1.76%	4.37%	3.33%	855	16	javascript
exploit	0.14%	0.07%	0.02%	0.00%	1.87%	69	exploit
%trojan		49.41%	99.95%	94.53%	80.47%	82.35%	%trojan
Only	7706	5584	3	45	154	34	Only
%Only	38.23%	50.47%	0.05%	5.35%	18.01%	49.28%	%Only

The top categories into which blacklisted apps report for themselves can be seen below. In Q2 the category 其他 (Chinese for "other") leads the rest with 442 entries, making up nearly all blacklistings for the AppChina store. The next most numerous category is Entertainment at 383, then Tools at 355, both mostly in 9Apps and, to a lesser degree, Brothersoft. These numbers do not represent a significant portion of blacklisted apps overall.

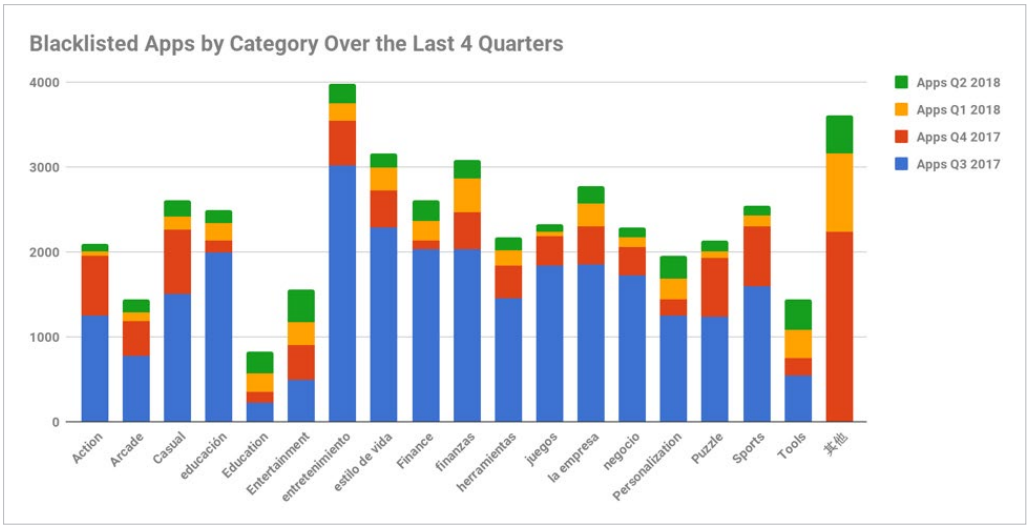


Fig. 15: Blacklisted apps continued to decrease in Q2 2018

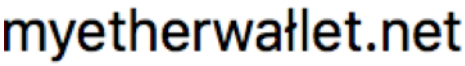
Developments

A look at new threat tactics in Q2 2018

Phishing for MEW

In May, RiskIQ research analyst Yonathan Klijnsma exposed a mobile threat aspect of the MEWKit phishing ATS (Automated Transfer System), which targets users of MyEtherWallet[1]. The threat actor created a Telegram group purporting to be MyEtherWallet and its support team. The group was named MyEtherWallet, @officialMyEther and had 9,064 followers at the time of the blog post's publication. The actor forwarded tweets from the official MEW Twitter account and regularly sent their own message pointing subscribers to download an Android app masquerading as an official MEW app from the link provided in the message.

The malicious app was actually an empty shell using the service GoNative.io that only serves websites. This allows web apps to be used as native apps. In the case of the fake MEW app, the website was an IDNA encoded URL: xn--myetherwalet-lcc[.] net. This IDNA encoding means that the address is almost indistinguishable from the official MEW site, myetherwallet.net (see screenshot below).



The phishing page served is a copy of the official MEW website from September 2017, except it contains a couple of scripts, one new and one modified, that together send authentication data to C2 servers when the victim enters their password to access/decrypt their wallet. The phishing page then works exactly as the official MEW page, allowing the victim to see their balance and carry out transactions so that they are not alerted to the fact that they have just been phished.

This attack illustrates the growing focus on both mobile and digital currencies by threat actors. Rather than relying only on email phishing (which had been MEWKit's focus in the past), this actor cleverly created a Telegram group and used the GoNative.io service to create a custom app designed to phish those who installed it. This allowed them to go after Android users' with Ethereum wallets. From what we can tell, this particular campaign was not widely effective, but probably netted the criminal(s) behind it some profit. And it may provide a template for more effective phishing attacks in the future.

Location, Location, Location

In May it was revealed that major mobile providers AT&T, Sprint, Verizon, and T-Mobile were sharing all of their customers' real-time location data with third parties that were both cavalier about privacy and ignorant/incompetent when it came to security concerns.[2] Location data was sold to and used by these third parties without customer consent or knowledge and without a warrant or court order.

The companies named include Securus and LocationSmart, from which Securus bought the location data through another reseller.[3] Securus peddled their real-time location tracking service to various law enforcement entities throughout the United States. Motherboard was presented with evidence that the company had been breached, exposing the data of thousands of law enforcement professionals along with the passwords and usernames they used to access the service.[4] Additionally, Krebs reported that dozens of Securus's internal documents containing sensitive information, including a login page lacking basic security controls for a county jail, had been uploaded to Virustotal and were able to be viewed and downloaded by anyone who purchases access to VT's file repository.[5]

LocationSmart was providing a free trial of its service for some time. Robert Xiao, a Ph.D. student at Carnegie Mellon, provided his findings to Krebs On Security that anyone could use this trial to look up the real-time location of anyone using a cell-phone tied to one of the major providers in the US. All that would be required was that phone number of the device one wished to track. There were no controls for authorization, consent, or authentication in place.[6]

LocationSmart and Securus both exhibited incompetence regarding security and privacy protection. The failings of Securus opened the door for malicious actors to use their service via compromised credentials. Additionally, law enforcement should not be allowed to track anyone's location without a warrant or court order. Fortunately, the Supreme Court blocked this practice in June. LocationSmart just left the door wide open in the first place.[7]

However, the main issue is with the mobile providers who compromised their customers' data by selling it to such entities in the first place. *Location data is intensely sensitive information, and it should not be given to anyone without informed user consent or a court order.*

AT&T, Sprint, Verizon, and T-Mobile have stated that they will no longer provide location data to third parties. However, there is nothing to prevent them from selling location data in the future. For that legislation from Congress will be required.

All Your Firebase Are Belong To Us

Firebase is a cloud-based database service Google provides to mobile developers as a back-end development platform for mobile and web apps. Appthority, a mobile app security company, discovered that a large number of these databases were unsecured by either firewalls or authentication controls.[8] This exposed hundreds of gigs of data, including personally identifiable information, to anyone. The only thing required to view the data is the project name and /.json appended to the project's Firebase URL, i.e.:

https://<Firebase project name>.firebaseio.com/.json

Among the exposed data was:

- over 3,000 apps leaking 2,300 databases w/ over 100 million records - 113 gigs
- 2.6 million plaintext passwords and user IDs
- 4 million+ PHI (Protected Health Information) records (chat messages and prescription details)
- 25 million GPS location records (cool, more location data exposure)
- 50,000 financial records including banking, payment and Bitcoin transactions
- 4.5 million+ Facebook, LinkedIn, Firebase, and corporate data store user tokens.

Firebase does not require authentication or any other security by default, leaving many devs to leave their databases wide open.

Moral of the story, if you're using a cloud-based database service, whether it is S3 Buckets or Firebase, make sure you secure your stuff.

aLTEr(ed) States

4G LTE communications are vulnerable to remote hijacking as demonstrated by three attacks developed by a team of security researchers from Ruhr-Universität Bochum and New York University Abu Dhabi.[9] These attacks allow an attacker to eavesdrop on LTE network communications via a sniffing device, fingerprint websites visited, and to carry out an active MitM attack called aLTEr which enables the attacker to intercept communications and redirect the victim to malicious sites.

The researchers targeted Layer 2, the data link layer which controls resource access for all users on the network, correction of transmission errors, and data protection via encryption. The aLTEr attack is possible because the LTE data link layer uses AES-CTR encryption without integrity protection which allows modification of bits within the encrypted data packet and thereby, decryption to plaintext. By using a device that appears to be cell tower (such as a Stingray) an attacker can intercept LTE communications and modify Layer 2 packets via aLTEr to redirect the victim to malicious sites.

5G communications may be vulnerable to this type of attack as well. The 4G vulnerabilities are due to a design flaw and are un-patchable.

Run for Your (Battery) Life

At RiskIQ we've seen a number of mobile scam pages that claim to detect battery life issues and provide a solution to make your battery run like new if only you click the link provided. In Q2 we spotted one with a new twist. The scam page directed the victim to a malicious "battery life" app that was hosted in the Google Play store under the name Advanced Battery Saver.[10]

The app itself did contain functionality to extend battery life, but it also claimed very excessive permissions including the ability to read sensitive log data, receive text messages (SMS), receive data from Internet, and modify system settings. It also stole IMEI data, phone numbers, location data, and included an ad-clicker as a revenue generator for the app author. Analysis of data from the C2 server showed that revenue generating ads to click were sent from the server to infected phones and that premium text messaging services also generated revenue. There were also indications that the Advanced Battery Life app infected at least 60,000 devices.

1 https://www.riskiq.com/blog/external-threat-management/mewkit/

2 https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html

3 https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/

4 https://motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked

5 https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/

6 https://krebsonsecurity.com/2018/05/mobile-giants-please-dont-share-the-where/

7 https://krebsonsecurity.com/2018/06/supreme-court-police-need-warrant-for-mobile-location-data/

8 https://thehackernews.com/2018/06/mobile-security-firebase-hosting.html

9 https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

10 https://www.riskiq.com/blog/interesting-crawls/battery-saving-mobile-scam-app/

Appendix: Data Tables

Total Numbers of Apps Observed Over the Previous 4 Quarters Per Store

App Store	Q3 2017	Q4 2017	Q1 2018	Q2 2018
Aptoide	0	0	483,175	61,784
Apple	120,195	138,662	116,294	116,951
Google	205,007	146,997	163,449	376,774
ApkPcCo	0	0	24,192	2,263
BlueStacksAPK	0	63,011	55,208	6,484
Anzhi	134,017	9,487	9,325	9,175
SameAPK	19,427	20,414	57,780	31,764
Apkplz	20,575	34,146	47,395	11,142
Onlinedown	62,771	36,304	14,034	5,645
9Apps	16,939	23,606	34,523	46,686
AndroidAPKDescargar	67,991	18,111	14,444	12,687
AndroidAppsGame	0	262,932	215,854	199,541
Apkgplay	0	189,606	139,915	81,307
AppChina	0	41,568	18,544	8,201
ApkFreeDownload	0	24,015	2,469	2,516
APKask	0	21,716	17,460	2,055
APKMirror	0	0	20,764	12,500
AppShopper	0	0	15,213	13,576
AppsZoom	0	0	14,256	15,587
APKCafe	0	0	0	33,302
Apkpure	7,331	3,930	4,582	30,042
Wandoujia	17,890	13,230	1,467	26,866

Observed Apps by Store Last 4 Quarters

Stores	Observed Apps
Google	750,947
AndroidAppsGame	678,058
Aptoide	544,955
Apple	448,300
Apkgplay	410,226
downloadapkfree	163,164
Anzhi	157,618
SameAPK	129,288
BlueStacksAPK	123,827
9Apps	122,779
AndroidAPKDescargar	117,081

Blacklisted Apps Last 4 Quarters

App Store	Q3 2017	Q4 2017	Q1 2018	Q2 2018
Blacklisted Apps	88716	41768	29527	52885
Total Apps	891,408	1,313,988	1,508,825	1,427,286
Percentage	10%	3%	2%	4%

Blacklisted Apps by Time

Month	Apps
January 2017	24,743
February 2017	22,774
March 2017	20,243
April 2017	12,274
May 2017	11,266
June 2017	41,209
July 2017	37,699
August 2017	29,033
September 2017	21,984
October 2017	15,922
November 2017	12,075
December 2017	13,771
January 2018	8,292
February 2018	7,505
March 2018	13,730
April 2018	13,972
May 2018	13,473
June 2018	25,440

Blacklisted Apps by Quarter

Quarter	Apps
Q1 2017	67,760
Q2 2017	64,749
Q3 2017	88,716
Q4 2017	41,768
Q1 2018	29,527
Q2 2018	52,885

Blacklisted Numbers of Apps Over Last 4 Quarters

App Store	Q3 2017	Q4 2017	Q1 2018	Q2 2018
9Apps	7,614	7,659	2,655	4,750
9Game.com	5,859	4,083	0	
AndroidAPKDescargar	39,477	9,511	3,692	2,985
Apk4Now	2,737	85	34	
ApkFiles	4,584	590	425	594
APKMonk	420	335	621	422
AppChina	0	2,347	971	455
AppLenovo	720	326	312	325
Brothersoft	1,010	794	687	730
EOEMarket	2,557	69	32	20
Feral App	6,267	3,507	1,981	11,288
Google	9,281	9375	8,287	28,533
NearmeMobile	617	1,679	56	
NineStore	6,423	3,503	536	497
Pconline	673	271	811	605
Tencent	751	387	346	371
Vmallapps	278	473	282	500
Mumayi	10	11	10	463

Blacklisted Percentages of Apps Over Last 4 Quarters

App Store	Q3 2017	Q4 2017	Q1 2018	Q2 2018
9Apps	9	32.45	8	10
AndroidAPKDescargar	55	52.52	26	24
Apk4Now	10	14	11	0
ApkFiles	61	66	37	54
AppChina		6	5	6
Brothersoft	19	20	18	21
EOEMarket	23	9	4	3
Feral App	63	52	46	81
Google	5	6	5	8
NineStore	7	33.80	12	10
Pconline	4	17.38	16	19
Tencent	10	9	9	10
Mumayi	10	8	5	19

Blacklisted Apps All 4 Quarters

Stores	BL Apps All Quarters	Total Apps	%
AndroidAPKDescargar	56,987	117,081	48.67%
Google	52,049	751,363	6.93%
9Apps	28,499	122,777	23.21%
Feral	23,154	34,949	66.25%
NineStore	11,629	33,743	34.46%
9Game.com	26	appastrophe	54
9,747	10,399	93.73%	51
ApkFiles	5,445	10,617	51.29%
AppChina	4,087	68,576	5.96%
Brothersoft	3,273	16,722	19.57%
Apk4Now	2,912	27,897	10.44%

Blacklisted App Types

	Trojan	Adware	Botnet	Javascript	Exploit	Spyware	N/A	Total
All-Time	377,578	284,977	16,840	10,401	2,796	25,451	171,112	889,155
Q1 17	14,444	11,917	57	396	171	982	39,793	67,760
Q2 17	19,624	16,900	74	315	110	424	27,302	64,749
Q3 17	40,696	36,948	51	421	132	483	9,985	88,716
Q4 17	15,227	14,669	30	471	138	277	10,956	41,768
Q1 18	9,175	8,329	28	393	59	199	11,344	29,527
Q2 18	20,158	11,065	6,266	855	69	841	13,631	52,885

Blacklisted Apps by Category Over the Last 4 Quarters

Categories	Apps Q3 2017	Apps Q4 2017	Apps Q1 2018	Apps Q2 2018
Action	1,250	701	55	89
Arcade	769	421	100	156
Casual	1,503	755	158	186
educación	1,996	139	207	155
Education	216	139	210	265
Entertainment	494	406	275	383
entretenimiento	3,018	528	206	226
estilo de vida	2,293	434	267	169
Finance	2,029	105	235	236
finanzas	2,029	437	400	217
herramientas	1,452	384	180	150
juegos	1,837	344	55	88
la empresa	1,857	441	273	199
negocio	1,727	331	111	123
Personalization	1,242	200	241	266
Puzzle	1,238	690	80	123
Sports	1,591	710	124	119
Tools	538	208	339	355
其他		2,233	931	442

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn more at riskiq.com

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com
1 888.415.4447 @RiskIQ