Quokka

WHITEPAPER

The Real Threats Posed by TikTok

Key Findings From Our Research

Executive Summary

TikTok has recently been at the center of significant attention from legislators, the press, and users worldwide. The U.S. federal and local governments have taken steps to ban the app on work-related mobile devices, highlighting how one app can be a microcosm of a much larger security problem. While TikTok is just one of many apps, it raises critical questions about the broader landscape of mobile app security, including pre-installed apps and those that collude with others on a device.

These malicious behaviors present substantial security and privacy risks to both users and enterprises. In this white paper, we objectively examine the risks associated with TikTok and demonstrate how a single app can escalate into significant challenges for business operations. Additionally, we provide strategic guidance on safeguarding against these risks, emphasizing proactive measures such as risk assessments, app policy development, and enhancing the overall mobile security posture.

Our goal is to help CISOs and mobile security leaders better understand these dynamics so they can protect their organizations from evolving threats posed by mobile apps, ultimately fostering a more secure mobile ecosystem.

Introduction

In recent years, TikTok has grown into one of the most widely used social media platforms, with over a billion active users worldwide and 150 million in the U.S. alone. While it offers an engaging and dynamic platform for content creation and sharing, TikTok's ownership by ByteDance, a China-based company, has raised significant privacy and security concerns. These concerns are particularly pressing for government agencies and enterprises to ban its use on work devices due to fears of data privacy violations and potential surveillance.

Bill seeking to address TikTok threats passed

In April 2024, President Biden signed a bill that would force TikTok's parent company, ByteDance–a Beijing-based firm with a valuation of $268 billion–to sell the app or face a ban in the U.S. This decision reflects growing security concerns, tensions and declining trust between the U.S. and China.

Security researchers have identified multiple vulnerabilities in TikTok's code, raising fears that ByteDance could be compelled by the Chinese government to provide sensitive access to sensitive user data or spread propaganda. The law aims to mitigate these risks and protect user privacy.

Several national governments, including the U.S., have already taken steps to ban the TikTok mobile app from government devices due to these growing concerns. Notably, India has implemented a complete nationwide ban on TikTok and 58 other Chinese apps.

How a ban may introduce more risk

While a ban on TikTok would require Google and Apple to remove the app from their respective marketplaces, they could also uninstall it remotely from user devices. However, this approach might lead users to seek various workarounds to circumvent the ban. These tactics expose organizations to new vulnerabilities, as users may turn to unofficial sources or employ risky methods to access the app.

- **VPN Usage**: Users may attempt to access TikTok through VPN connectivity by using built-in device settings or a VPN app. Even though VPNs can bypass geographic restrictions, they can also create security risks by intercepting data on the device or acting as a carrier for mobile malware. Malicious VPNs or poorly configured ones may capture sensitive information such as login credentials and corporate data, leading to data breaches or unauthorized access.
- **App Sideloading:** Third-party app stores may host various versions of TikTok or clones, which can be breeding grounds for malicious software development kits (SDKs). These app stores often lack rigorous security processes, increasing the risk of downloading compromised apps.
- **Rooting and Jailbreaking:** To sideload an app, users often need to enable features known as jailbreaking (iOS) or rooting (Android), which involves removing built in security protections to accept unknown apps. This practice makes devices more vulnerable to other security threats, such as device takeovers.
- **Malware Risks:** Users could be tricked into downloading malware masquerading as a replacement for the banned app. It is particularly concerning for Android users who may sideload apps without going through an official marketplace, bypassing security vetting processes and weakening the device's overall security posture.

These risks are compounded when undertaken by users who may need help understanding the security implications, further increasing the mobile attack surface.

What, really, are the risks?

Security teams and users must recognize that TikTok isn't going away anytime soon. It's essential to assess the risks and determine if ignoring them compromises organizational security.

Employees spend 56 minutes daily on non-work related phone activities. 51% of employees rely on company-mandated apps for mobile work task.

The evolving mobile threat landscape

First, we must examine the mobile threat landscape and how quickly it evolves. Organizations worldwide have embraced the full potential of mobile devices, resulting in increased productivity, enhanced mobility, and faster access to vital information. However, this positive transition has made mobile devices and apps gateways to sensitive corporate data and internal systems. As a result, we have seen mobile app threats increase by more than 30% in 2023.

Risks introduced by mobile device users

Second, there are the mobile device users themselves. With 87% of companies adopting policies that integrate personal devices into the workplace, this risk is higher than ever. The average mobile device has 80 apps installed, each with its own individual threat profile. Most devices feature unique combinations of apps, and when apps are combined, they can collude, exposing data to other installed apps. The sheer number of apps, combined with the countless possible combinations of apps–*such as games, social media, productivity, and health*– across employees' devices, makes it difficult for security teams to keep up with new threats.

Where does the line blur between personal and work

Lastly, apps are integral to our work lives, whether taking phone calls on the go, responding to emails, or using work apps. This proliferation of apps blurs the line between personal and professional use by enabling access to corporate resources on personal devices.

Moreover, the security problem with apps is exacerbated by how they are developed. Many apps rely on open-source code and third-party libraries, which can introduce vulnerabilities into the software. Attackers can exploit these vulnerabilities, whether they are intentional or not, to gain unauthorized access to sensitive data or to infiltrate internal systems. As apps become the new endpoint in the digital workspace, addressing these security issues is critical to protecting business operations.

[1] Atto: 10 Cell Phones at Work Statistics for 2023: Facts & Key Takeaways, June 12, 2023

TikTok: Large User Base, Widespread Risk

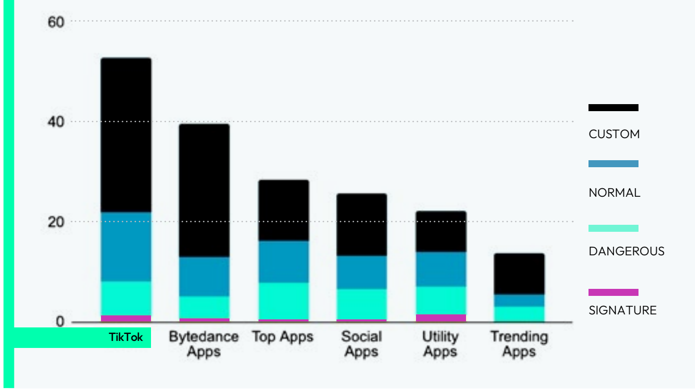
Now that we understand mobile device and app risks, it's time to review the risks associated with one of the most widely used apps in the world: TikTok. It's the fifth most popular social networking app and shows little signs of slowing down.

We examined the risks of TikTok in two key respects: **privacy** and **security**.

Permission analysis reveals significant risks

According to Quokka research, TikTok demands an alarming number of permissions from its users, requesting access to twice as much data as typical social media platforms. ByteDance apps, including TikTok, consistently rank among the most data-hungry in the industry, raising significant privacy concerns.

Permissions Requested by TikTok vs App Categories



Our research began in 2019 when we delved into these risks associated with TikTok and uncovered alarming details. We found that TikTok was collecting an excessive amount of data and had permissions allowing it to access information it shouldn't need, including all data in your notifications. These practices raised serious concerns about user privacy and security, prompting the critical question: Is TikTok the only app engaging in such invasive data collection?

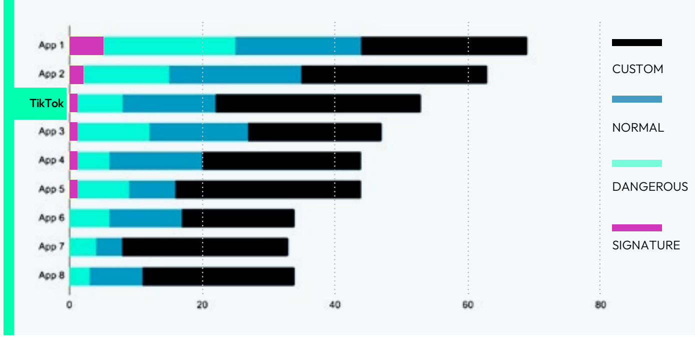
When apps ask for permissions, they request access to specific features or data on your device. Here's an overview of the privacy risks associated with app permissions:

Privacy risks of app permissions:

- **Data Collection and Sharing:** Collecting personal data and sharing it with third parties or using it for targeted advertising without obtaining explicit consent from users.
- **Location Tracking:** Accessing location services can allow apps to track users' movements, potentially leading to invasive profiling and unwanted surveillance.
- **Access to Contacts and Messages:** Accessing contacts or messages can result in unauthorized data sharing, risking user privacy and security, such as phishing.
- **Camera and Microphone Access:** Accessing the camera or microphone can record audio or videos without the users' knowledge, leading to severe privacy violations.
- **Device and App Usage Monitoring:** Gathering information about device usage patterns, app activity, and browsing habits, leading to detailed user profiles that can be exploited for various purposes.

Of the apps analyzed in this research, TikTok is ranked third in the list of the most invasive apps. Even in the short list of the most popular apps in the market, a number of them either exceed or come very close to the level of access that TikTok has. Further, our analysis was only based on a sample set, suggesting that many other apps may match TikTok regarding invasiveness.

Most Invasive Apps Ranked by Total Permissions



Focusing on the TikTok Android app, the version tested, 28.9.4, requests 59 different permissions:

- **25 are standard Android Framework permissions,** which are common across many apps.
- **6 are its own custom permissions unique to TikTok,** allowing the app to access specific features or data.
- **28 are used to integrate with vendor devices and external libraries**, expanding TikTok's functionality and data access.

These extensive permissions are problematic because they give TikTok access to a wide range of data device features. Some of these permissions require explicit user approval, while others are automatically granted upon installation, leading to privacy concerns.

Security analysis

Threats in the mobile security landscape are multifaceted and require comprehensive evaluation. Our research now shifts from analyzing permissions to examining the security weaknesses within TikTok. Evaluating these security risks is complex and involves considering several factors, including weaknesses in the app's code, the likelihood of exploitation, and the methods and locations of sharing data.

Our results highlight the risks identified in TikTok's code, with severity levels categorized as high and medium. This assessment is based on industry standards established by NIST, OWASP, NIAP, and academic research.

Pinpointing overlooked app vulnerabilities

In addition to identifying high and medium risks, we leverage one of our advanced engines to focus on **manifest analysis** to uncover crucial yet often overlooked vulnerabilities in the app ecosystem.

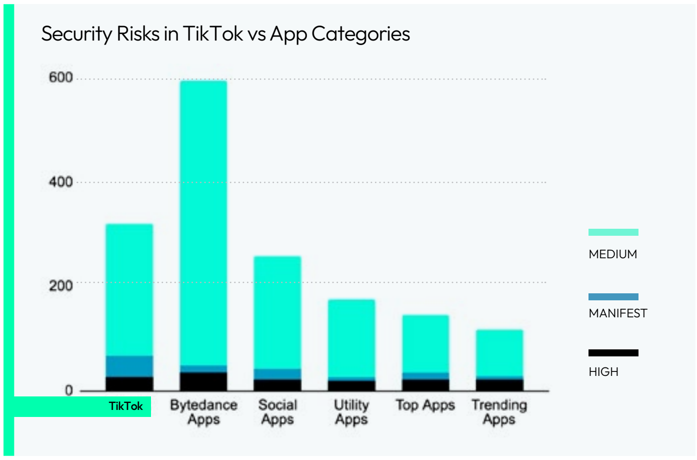
Previous research conducted by Quokka's R&D team revealed that many widely used apps contain misconfigurations in their manifest files, potentially resulting in severe security issues. Our tool has detected a significant number of these misconfigurations, highlighting the prevalence of security vulnerabilities across both Google Play and pre-installed apps.

Our engine allows us to analyze each app's high, medium, and manifest risks. It not only identifies unique vulnerabilities, such as the use of a weak cipher for encrypting data but also measures the total occurrences of each risk. For instance, encrypting data with a weak cipher 100 times presents more risk than doing it only once or twice.

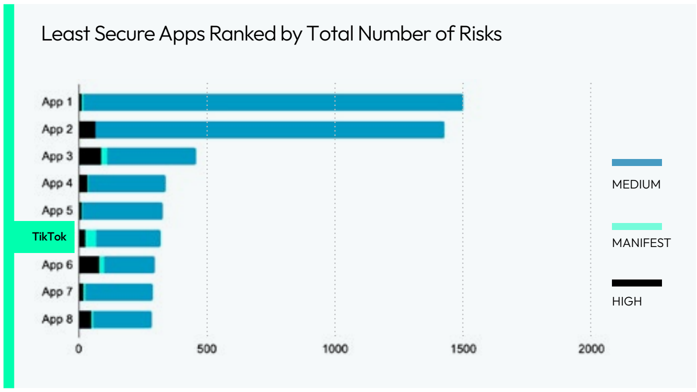
Comparing security risks across apps

In analyzing popular mobile apps, our research reveals that TikTok poses more security risks than the average social media app. However, it is not the worst offender among the apps reviewed. ByteDance has developed a range of apps that, along with offerings from other developers, collectively present significant security challenges.

Compared to apps in similar categories, TikTok exhibits a higher number of manifest risks compared to medium and high, setting it apart from other apps in the industry. While TikTok's security profile is concerning, its manifest vulnerabilities are particularly notable and make it stand out among other apps. This underscores the need to prioritize manifest analysis as a crucial part of app security assessments.



As we shift the focus to examining app security from a different perspective, we reviewed the least secure apps available in the market. TikTok was ranked sixth based on the number of identified risks. This ranking highlights the challenge of balancing security and privacy when it comes to TikTok. While it may be lower on the list of least secure apps, its privacy issues can pose significant threats to business operations, with the potential risk of leaking sensitive employee data and intellectual property.



ByteDance Apps and Code Are Prevalent, and Problematic

TikTok has been downloaded over **one billion times** from the Google Play store alone. The broader concern lies with other ByteDance apps, which are available through the same app stores and present even greater risks. When analyzing our database of apps in the market, we found ByteDance's code in just about every app category.

About 40% of those ByteDance apps had over 100 million downloads each.

ByteDance's expanding influence through SDKs

Beyond its own apps like CapCut and Lemon8, ByteDance extends its reach through Software Development Kits (SDKs), integrating its code into a wide range of apps available in the app stores.

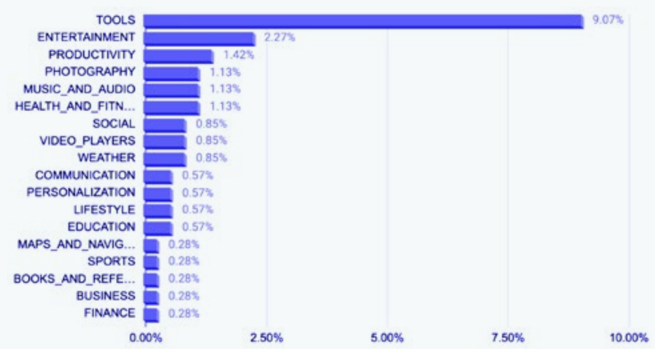
In our analysis of a sample set of 10,000 Android apps, we looked for direct references with the com.bytedance Group ID. Over 3% of these apps included at least one ByteDance SDK, collectively accounting for over 3.6 billion downloads. These numbers are staggering, demonstrating the extensive reach of ByteDance within just a small sample set.

3.15% of apps using ByteDance SDKs

+3.6B 3,626,748,110 downloads for ByteDance SDK apps

TikTok itself has over 1 billion downloads, but ByteDance's code through their SDKs could have 10 to 100 times the number of total downloads. Our findings also show that ByteDance SDKs are primarily concentrated in one app category, with games accounting for about 77% of the total. The remaining 23% are distributed across various other categories, which are outlined below.

Category Breakdown for ByteDance SDKs - Minus Games



Software development kits: friend or foe?

To understand the security risks of SDKs, it's important to know their role in app development. Publicly available SDKs are essential for creating Android and iOS apps, allowing developers to quickly and efficiently extend functionality. These pre-built components, tools, and APIs simplify integration, saving developers time and effort compared to coding the entire app from scratch. For instance, SKDs like Google Maps, Firebase, and Facebook offer ready-to-use modules for maps, analytics, social media features, and more — enhancing user experience and accelerating development.

Security risks associated with SDKs

- **Weaknesses in Code:** SDKs may contain vulnerabilities that can be exploited by attackers to compromise the security of the host app and its users.
- **Lack of Transparency:** Developers may not have full visibility into what an SDK does behind the scenes, leading to hidden security and privacy risks.
- **Data Leakage:** SDKs can inadvertently or deliberately leak sensitive data, exposing users to risks such as identity theft and financial fraud.
- **Complex Supply Chains:** The inclusion of third-party SDKs complicates the app's supply chain, making it harder to track and manage security updates.
- **Cross-App Data Sharing:** SDKs can facilitate the sharing of data between apps, potentially leading to cross-app tracking and profiling of users.
- **Potential for Malware:** Malicious SDKs can introduce malware into apps, posing significant security threats to users and their devices.

Proactive Strategies for Managing TikTok Security Concerns

Big tech firms, app developers, and device manufacturers share a collective responsibility to protect users and their data from unauthorized access and data harvesting. Despite strong efforts by major tech service providers to enhance privacy and security, risks persist. Banning every risky app is impractical and not a feasible solution.

Given the security and privacy challenges revealed by our analysis of TikTok and other ByteDance apps, organizations must adopt strategic measures to protect their data and users:

1. **Educate and Train Employees:** Conduct regular training to educate employees about mobile security risks and best practices. It's important for users to understand what permissions and settings their apps require and why, as well as what data they've granted access to. This knowledge helps them make informed decisions about app usage and enhances overall organizational security.
2. **Conduct Comprehensive Risk Assessments:** Our findings highlight the need for regular evaluations of the security and privacy risks posed by TikTok and similar apps. Organizations should first identify what their acceptable risk thresholds are and assess the potential vulnerabilities, consider the impact of data breaches, and prioritize risk based on the severity and likelihood of exploitation.
3. **App Vetting and Management: I**mplement a thorough app vetting process to evaluate the security and privacy implications of apps before they are used within the organization. This includes assessing permissions, reviewing data handling practices, and ensuring that apps meet your security standards. Regularly update this process to adapt to emerging threats and vulnerabilities.
4. **Enhance Security with Mobile Security Solutions:** Utilizing Mobile Device Management (MDM), Mobile Threat Defense (MTD), and Mobile App Intelligence solutions can help enforce security policies, remediate mobile threats, and analyze malicious behaviors to enforce proactive security measures based on risk.
5. **Monitor Emerging Threats and Update Security Measures:** Stay informed about the latest security threats and vulnerabilities related to TikTok and other mobile apps. Use mobile threat intelligence to monitor for risks and stay up to date on the latest mobile threats.

Implementing proactive strategies is a great starting point for organizations to address these challenges head-on, enhancing their security posture and minimizing threats.

Quokka

Protecting organizations from emerging mobile threats

Quokka is committed to reducing the mobile attack surface to decrease the overall security risk for enterprise organizations. As mobile security remains under invested, the mobile attack surface continues to increase in size and complexity across all sectors. Unvetted, high-risk apps are proliferating on mobile devices that access enterprise data and assets.

Quokka solutions are powered by the industry's only Contextual Mobile Security Intelligence engine. Our platform provides actionable insights, enabling security teams to take proactive remediation measures across app development, third-party app vetting, and device zero-days, ensuring comprehensive protection for your mobile ecosystem.

Built on over a decade of research and development, **Quokka was one of the first to alert the U.S. government to TikTok's data vulnerabilities and app collusion risk** in 2018. Today, we remain the U.S. government's longest-running mobile app security vendor, working closely with both federal and state organizations.

Through our research alone, we have disclosed over 230 CVEs (Common Vulnerabilities and Exposures) and many additional discoveries that have been privately disclosed.

To learn more about how Quokka solutions can help your business guard against the threats posed by risky mobile apps like TikTok, **request a demo today**.

Learn more at www.quokka.io or email info@quokka.io.