

TikTok Browser Can Track Users' Keystrokes, According to New Research

In the web browser used within the TikTok app, supplementary code lets the company track every character typed by users. The company said the capability was for troubleshooting.

By Paul Mozur, Ryan Mac and Chang Che

Published Aug. 19, 2022 Updated Aug. 21, 2022

The web browser used within the TikTok app can track every keystroke made by its users, according to new research that is surfacing as the Chinese-owned video app grapples with U.S. lawmakers' concerns over its data practices.

The research from Felix Krause, a privacy researcher and former Google engineer, did not show how TikTok used the capability, which is embedded within the in-app browser that pops up when someone clicks an outside link. But Mr. Krause said the development was concerning because it showed TikTok had built in functionality to track users' online habits if it chose to do so.

Collecting information on what people type on their phones while visiting outside websites, which can reveal credit card numbers and passwords, is often a feature of malware and other hacking tools. While major technology companies might use such trackers as they test new software, it is not common for them to release a major commercial app with the feature, whether or not it is enabled, researchers said.

“Based on Krause’s findings, the way TikTok’s custom in-app browser monitors keystrokes is problematic, as the user might enter their sensitive data such as login credentials on external websites,” said Jane Manchun Wong, an independent software engineer and security researcher who studies apps for new features.

She said TikTok’s in-app browser could “extract information from the user’s external browsing sessions, which some users find overreaching.”

In a statement, TikTok, which is owned by the Chinese internet firm ByteDance, said Mr. Krause’s report was “incorrect and misleading” and that the feature was used for “debugging, troubleshooting and performance monitoring.”

“Contrary to the report’s claims, we do not collect keystroke or text inputs through this code,” TikTok said.

Mr. Krause, 28, said he was unable to ascertain whether keystrokes were actively being tracked, and whether that data was being sent to TikTok.

The research could raise questions for TikTok in the United States, where government officials have scrutinized whether the popular app could endanger U.S. national security by sharing information about Americans with China. Although debate in Washington about the app had receded under the Biden administration, new concerns have boiled over in recent months after revelations from BuzzFeed News and other news outlets about TikTok’s data practices and ties to its Chinese parent.

Apps sometimes use in-app browsers to prevent people from visiting malicious sites or to make online browsing easier with the auto-filling of text. But while Facebook and Instagram can use in-app browsers to track data like what sites a person visited, what they highlighted and which buttons they pressed on a website, TikTok goes further by using code that can track each character entered by users, Mr. Krause said.

A spokesman for Meta, the parent company for Facebook and Instagram, declined to comment.

Mr. Krause said he carried out the research on TikTok only on Apple’s iOS operating system and noted that the keystroke tracking would only occur within the in-app browser.

As with many apps, TikTok offers few chances for people to click away from its service. Instead of redirecting to mobile web browsers like Safari or Chrome, an in-app browser appears when users click on ads or links embedded within the profiles of other users. These are often the moments people enter key information like credit card details or passwords.

In a CNN interview in July, Michael Beckerman, a TikTok policy executive, denied that the company logs users’ keystrokes but acknowledged monitoring their patterns, such as typing frequency, to safeguard against fraud.

Mr. Krause said he feared those tools had “very similar architectures” and could be repurposed to track keystroke content.

“The problem is they have infrastructure set up to do this stuff,” he said.