

INNOVATION EDITORS' PICK

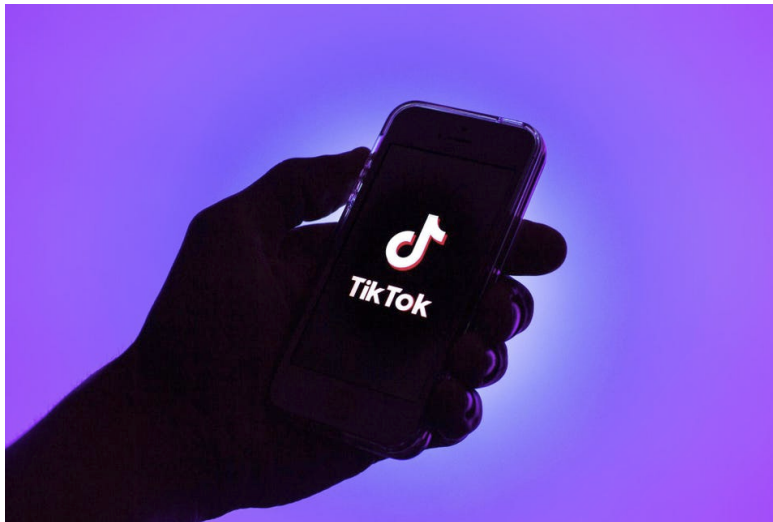
TikTok's In-App Browser Includes Code That Can Monitor Your Keystrokes, Researcher Says

Richard Nieva Forbes Staff

Follow

 13

Aug 18, 2022, 04:54pm EDT



In-app browsers on TikTok and other apps include code that could potentially track user activity on websites. (Photo Illustration by Thiago Prudêncio/SOPA Images/LightRocket via Getty Images) SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

When TikTok users enter a website through a link on the app, TikTok inserts code that can monitor much of their activity on those outside websites, including their keystrokes and whatever they tap on the page, according to new research shared with *Forbes*. The tracking would make it possible for TikTok to capture a user's credit card information or password.

TikTok has the ability to monitor that activity because of modifications it makes to websites using the company's in-app browser, which is part of the app itself. When people tap on TikTok ads or visit links on a creator's profile, the app doesn't open the page with normal browsers like Safari or Chrome. Instead it defaults to a TikTok-made in-app browser that can rewrite parts of web pages.

TikTok can track this activity by injecting lines of the programming language JavaScript into the websites

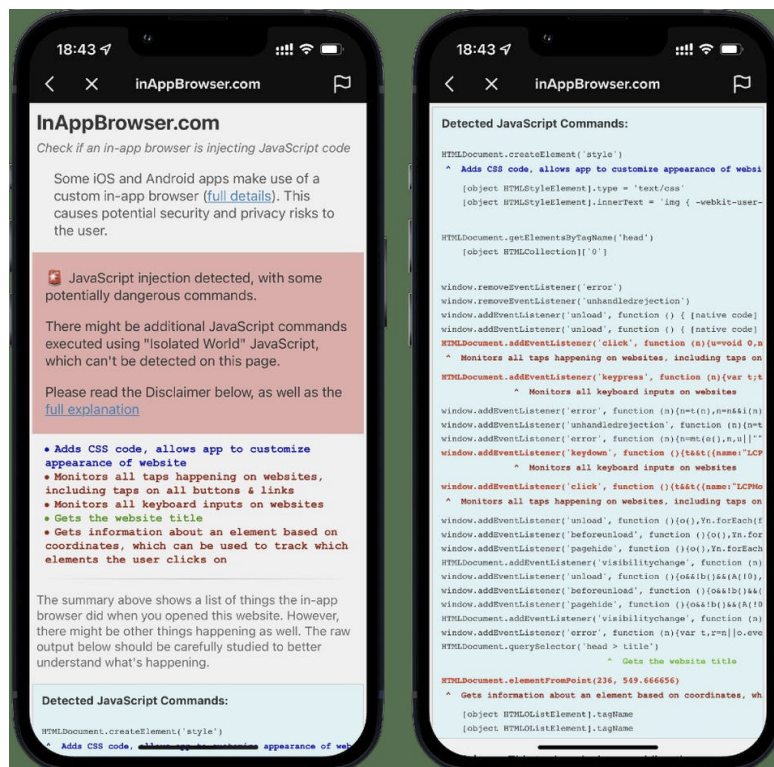
visited within the app, creating new commands that alert TikTok to what people are doing in those websites.

BETA

“This was an active choice the company made,” said Felix Krause, a software researcher based in Vienna, who [published a report](#) on his findings Thursday.

“This is a non-trivial engineering task. This does not happen by mistake or randomly.” Krause is the founder of Fastlane, a service for testing and deploying apps, which Google acquired five years ago.

TikTok strongly pushed back at the idea that it is tracking users in its in-app browser. The company confirmed those features exist in the code, but said TikTok is not using them.



The code injected into websites through TikTok's in-app browser, according to Krause. FELIX KRAUSE

"Like other platforms, we use an in-app browser to provide an optimal user experience, but the JavaScript code in question is used only for debugging, troubleshooting and performance monitoring of that experience — like checking how quickly a page loads or whether it crashes," spokesperson Maureen Shanahan said in a statement.

The company said the JavaScript code is part of a third-party software development kit, or SDK, a set of tools used to build or maintain apps. The SDK includes features the app does not use, the company said. TikTok did not answer questions about the SDK, or what third party makes it.

While Krause's research reveals the code companies including TikTok and Facebook parent Meta are injecting into websites from their in-app browsers, the research does not show that these companies are actually using that code to collect data, send it to their servers or share it with third parties. Nor does the tool reveal if any of the activity is tied to a user's identity or profile. Even though Krause was able to identify a few specific examples of what the apps can track (like TikTok's ability to monitor keystrokes), he said his list isn't exhaustive and the companies could be monitoring more.

The new research follows a [report last week](#) by Krause about in-app browsers, which focused specifically on Meta-owned apps Facebook, Instagram and Facebook Messenger. WhatsApp,

which the company also owns, appears to be in the clear because it doesn't use an in-app browser.

BETA

Krause on Thursday also released a tool that lets people check if the browser they are using injects any new code into websites, and what activity the company might be monitoring. To use the tool to check Instagram's browser, for example, send the link InAppBrowser.com to a friend in a direct message (or have a friend DM you the link). If you click on the link in the DM, the tool will give you a rundown of what the app is potentially tracking — though the tool uses several developer terms and may be difficult to decipher for non-coders.

For his new research, Krause tested seven iPhone apps that use in-app browsers: TikTok, Facebook, Facebook Messenger, Instagram, Snapchat, Amazon and Robinhood. (He did not test the versions for Android, Google's mobile operating system.)

Of the seven apps Krause tested, TikTok is the only one that appears to monitor keystrokes, he said, and seemed to be monitoring more activity than the rest. Like TikTok, Instagram and Facebook both track every tap on a website. Those two apps also monitor when people highlight text on websites.

**This is a non-trivial
engineering task. This**

does not happen by mistake or randomly.

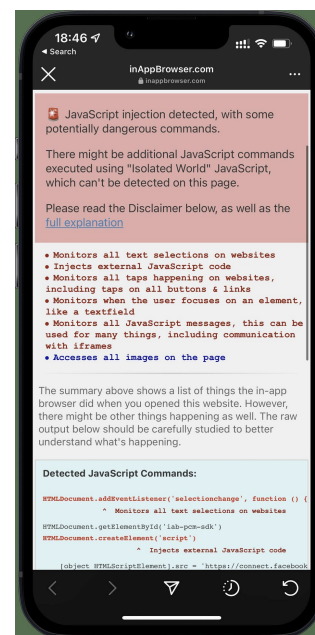
BETA

Meta did not answer specific questions related to the tracking, but said in-app browsers are “common across the industry.” Spokesperson Alisha Swintek said the company’s browsers enable certain features, like allowing autofill to populate properly and keeping people from being redirected to malicious sites. (However, browsers including Safari and Chrome have those features as well.)

“Adding any of these kinds of features requires additional code,” Swintek said in a statement. “We have carefully designed these experiences to respect users' privacy choices, including how data may be used for ads.”

Meta also said the script names featured in the tool can be misleading because they are technical JavaScript terms that people may misunderstand. For example, “message” in this context refers to code components communicating with each other, not personal text messages.

Snapchat seemed to be the



The code that Instagram inject into websites, according to

least data-hungry. Its in-app

Krause. FELIX KRAUSE

browser didn't appear to inject any new code into web pages. However, apps have the ability to hide their JavaScript activity from websites (like Krause's tool) because of an operating system update Apple made in 2020. So it's possible that some apps are running commands without detection. Snapchat didn't respond to a request for comment on what activity, if any, is monitored on its in-app browser.

BETA

The in-app browser isn't nearly as prevalent on TikTok as it is on Instagram. TikTok doesn't allow users to click on links in DMs, so the in-app browser comes up usually when people click on ads or links on a creator or brand's profile.

The browser-tracking research comes as TikTok, owned by Chinese parent company ByteDance, faces intense scrutiny over the bounds of its potential surveillance, and questions about its ties to the Chinese government. In June, BuzzFeed News [reported](#) that U.S. user data had been repeatedly accessed from China. The company has also been working to move some U.S. user information stateside, to be stored at a data center managed by Oracle, in an effort internally known as Project Texas.

But the potential tracking could also compromise privacy related to elections. TikTok on Wednesday [announced](#) its efforts in election integrity, ahead of the U.S. midterms. The initiative includes a new

Elections Center, which connects people to authoritative information from reliable sources including the National Association of Secretaries of State and Ballotpedia.

TikTok explicitly promises privacy as part of the initiative. “For any action that requires a user to share information, such as registering to vote, users will be directed away from TikTok onto the website for the state or relevant non-profit in order to carry out that process,” the company said in a blog post. “TikTok will not have access to any of that off-platform data or activity.”

TikTok will likely use its in-app browser to open those websites. Krause’s tool suggests TikTok could have access to that information, potentially letting the company track someone’s address, age and political party. TikTok also pushed back against that scenario, again emphasizing that while those tracking features exist in the code, the company doesn’t use them.

In recent years, the business model behind big tech — in which companies like Facebook and Google Hoover up user data to prop up their targeted advertising machines — has become widely known, so some people may not be surprised by the tracking in in-app browsers. However, neither Meta nor TikTok have specific sections in their privacy policies on in-app browsers that disclose those monitoring practices to users.

Some privacy experts also balk at the type of

keystroke monitoring that TikTok appears to be capable of doing. “It’s very sneaky,” said Jennifer King, privacy and data policy fellow at the Stanford University Institute for Human-Centered Artificial Intelligence. “The assumption that your data is being pre-read before you even submit it, I think that crosses a line.”

Krause said he would like to see the industry move away from in-app browsers, instead using browsers like Safari or Chrome, which people usually have set as default browsers on their phone. Apple did not respond to a request for comment asking if the company would crack down on in-app browsers, requiring apps to instead use a device’s default browser.

Both TikTok and Meta offer the option for you to open links in Safari or your phone’s default browser, but only after the apps take you to their respective in-app browsers first. The default option is also behind a menu screen in both TikTok and Instagram — already too out of the way for many users who don’t even know the option exists.

Send me a secure [tip](#).



Richard Nieva

Follow

Join Our Conversation 13 comments

I’ve been the target of spyware and doxxing based in San Francisco. Send me tips at OneCommunity.ManyVoices@gmail.com. Create a free account to share your thoughts. Read our community guidelines [here](#)



What do you think?

BETA

Sort by **Best** ▾

P

Pyxy



22 August, 2022

If it is in their code, but they're not using it, why is it even in their code in the first place??

Reply · 7 · Share

1 reply

SM

Shane Millsom



22 August, 2022

Screenshots are all shown on an Apple iPhone, but JavaScript code injection like this is strictly against Apple's App Store rule and would see these apps rejected and banned.

Can you confirm whether iOS apps do contain this code? Or is this another Android-only security hole being misrepresented by ...**See more**

Reply · 1 · Share

A

anonymous



24 August, 2022

"For his new research, Krause tested seven iPhone apps that use in-app browsers: TikTok, Facebook, Facebook Messenger, Instagram, Snapchat, Amazon and Robinhood. (He did not test the versions for Android, Google's mobile operating system.)"

↩ Show more replies

KH

Katerina Haria

...

BETA

21 August, 2022

I think that important research like this must be distributed in several languages . So all the people that can't read English can understand!

Reply · 👍 1 · Share

↩ 2 replies

