TikTok and 53 other iOS apps still snoop your sensitive clipboard data

reader comments

133 with 90 posters participating

Share this story

In March, researchers uncovered a troubling privacy grab by more than four dozen iOS apps including TikTok, the Chinese-owned social media and video-sharing phenomenon that has taken the Internet by storm. Despite TikTok vowing to curb the practice, it continues to access some of Apple users' most sensitive data, which can include passwords, cryptocurrency wallet addresses, account-reset links, and personal messages. Another 53 apps identified in March haven't stopped either.

The privacy invasion is the result of the apps repeatedly reading any text that happens to reside in clipboards, which computers and other devices use to store data that has been cut or copied from things like password managers and email programs. With no clear reason for doing so, researchers Talal Haj Bakry and Tommy Mysk found, the apps deliberately called an iOS programming interface that retrieves text from users' clipboards.

Universal snooping

In many cases, the covert reading isn't limited to data stored on the local device. In the event the iPhone or iPad uses the

same Apple ID as other Apple devices and are within roughly 10 feet of each other, all of them share a universal clipboard, meaning contents can be copied from the app of one device and pasted into an app running on a separate device.

That leaves open the possibility that an app on an iPhone will read sensitive data on the clipboards of other connected devices. This could include bitcoin addresses, passwords, or email messages that are temporarily stored on the clipboard of a nearby Mac or iPad. Despite running on a separate device, the iOS apps can easily read the sensitive data stored on the other machines.

“It’s very, very dangerous,” Mysk said in an interview on Friday, referring to the apps’ indiscriminate reading of clipboard data. “These apps are reading clipboards, and there’s no reason to do this. An app that doest have a text field to enter text has no reason to read clipboard text.”

The video below demonstrates universal clipboard reading:

[embedded content]
KlipboardSpy: How malicious apps on iPhone and iPad abuse the Universal Clipboard on your Mac.

Back in the news

While Haj Bakry and Mysk published their research in March, the invasive apps made headlines again this week with the developer beta release of iOS 14. A novel feature Apple added provides a banner warning every time an app reads clipboard contents. As large numbers of people began testing the beta release, they quickly came to appreciate just how many apps engage in the practice and just how often they do it.

This YouTube video, which has racked up more than 87,000 views since it was posted on Tuesday, shows a small sample of the apps triggering the new warning

[embedded content]
iOS14 Catches Apps Spying on Your Clipboard

TikTok in the spotlight

Recent headlines have focused particular attention on TikTok, in large part because of its massive base of active users (reported to be 800 million, with an estimated 104 million iOS installs in the first half of 2018 alone, making it the most downloaded app for that period).

TikTok's continued snooping has gotten extra scrutiny for other reasons. When called out in March, the video-sharing provider told UK publication The Telegraph it would end the practice in the coming weeks. Mysk said that the app never stopped the monitoring. What's more, a Wednesday Twitter thread revealed that the clipboard reading occurred each time a user entered a punctuation mark or tapped the space bar while composing a comment. That means the clipboard reading can happen every second or so, a much more aggressive pace than documented in the March research, which found monitoring happened when the app was opened or reopened.

> *To reproduce:*
> *1. Have something on your clipboard. Eg copy some text from Notes or a website*
> *2. Open TikTok and start typing in any text field*
> *3. You learn from iOS 14 beta each time an app "pastes" — but in this instance I didn't request it, and none of that text appears in UI*
>
> *— Jeremy Burge (@jeremyburge)* ***June 24, 2020***

In a statement, TikTok representatives wrote:

> *Following the beta release of iOS14 on June 22, users saw notifications while using a number of popular apps. For TikTok, this was triggered by a feature designed to identify*

> *repetitive, spammy behavior. We have already submitted an updated version of the app to the App Store removing the anti-spam feature to eliminate any potential confusion.*
>
> *TikTok is committed to protecting users' privacy and being transparent about how our app works. We look forward to welcoming outside experts to our Transparency Center later this year.*

On background, a spokesperson said that TikTok for Android never implemented the anti-spam feature.

I sent follow-up questions asking (1) if the TikTok version for Android monitored clipboards for any other reason, (2) if any clipboard text was uploaded from the device, and (3) why TikTok didn't remove the monitoring as promised in March. The spokesperson has yet to respond. This post will be updated if a reply comes later.

Not just TikTok

In all, the researchers found the following iOS apps were reading users' clipboard data every time the app was opened with no clear reason for doing so:

- **App Name —** BundleID

News

- **ABC News —** com.abcnews.ABCNews
- **Al Jazeera English —** ajenglishiphone
- **CBC News —** ca.cbc.CBCNews
- **CBS News —** com.H443NM7F8H.CBSNews
- **CNBC —** com.nbcuni.cnbc.cnbcrtipad
- **Fox News —** com.foxnews.foxnews
- **News Break —** com.particlenews.newsbreak
- **New York Times —** com.nytimes.NYTimes
- **NPR —** org.npr.nprnews

- **ntv Nachrichten –** de.n-tv.n-tvmobil
- **Reuters –** com.thomsonreuters.Reuters
- **Russia Today –** com.rt.RTNewsEnglish
- **Stern Nachrichten –** de.grunerundjahr.sternneu
- **The Economist –** com.economist.lamarr
- **The Huffington Post –** com.huffingtonpost.HuffingtonPost
- **The Wall Street Journal –** com.dowjones.WSJ.ipad
- **Vice News –** com.vice.news.VICE-News

Games

- ***8 Ball Pool*™ –** com.miniclip.8ballpoolmult
- ***AMAZE!!!* –** com.amaze.game
- ***Bejeweled* –** com.ea.ios.bejeweledskies
- ***Block Puzzle* –**Game.BlockPuzzle
- ***Classic Bejeweled* –** com.popcap.ios.Bej3
- ***Classic Bejeweled HD* –**com.popcap.ios.Bej3HD
- ***FlipTheGun* –** com.playgendary.flipgun
- ***Fruit Ninja* –** com.halfbrick.FruitNinjaLite
- ***Golfmasters* –** com.playgendary.sportmasterstwo
- ***Letter Soup* –** com.candywriter.apollo7
- ***Love Nikki* –** com.elex.nikki
- ***My Emma* –** com.crazylabs.myemma
- ***Plants vs. Zombies*™ *Heroes* –** com.ea.ios.pvzheroes
- ***Pooking – Billiards City* –** com.pool.club.billiards.city
- ***PUBG Mobile* –** com.tencent.ig
- ***Tomb of the Mask* –** com.happymagenta.fromcore
- ***Tomb of the Mask: Color* –** com.happymagenta.totm2
- ***Total Party Kill* –** com.adventureislands.totalpartykill
- ***Watermarbling* –** com.hydro.dipping

Social Networking

- **TikTok –** com.zhiliaoapp.musically
- **ToTalk –** totalk.gofeiyu.com
- **Tok –** com.SimpleDate.Tok
- **Truecaller –** com.truesoftware.TrueCallerOther
- **Viber –** com.viber

- **Weibo –** com.sina.weibo
- **Zoosk –** com.zoosk.Zoosk

Other

- **10% Happier: Meditation –**com.changecollective.tenpercenthappier
- **5-0 Radio Police Scanner –** com.smartestapple.50radiofree
- **Accuweather –** com.yourcompany.TestWithCustomTabs
- **AliExpress Shopping App –** com.alibaba.iAliexpress
- **Bed Bath & Beyond** – com.digby.bedbathbeyond
- **Dazn –** com.dazn.theApp
- **Hotels.com** – com.hotels.HotelsNearMe
- **Hotel Tonight** – com.hoteltonight.prod
- **Overstock –** com.overstock.app
- **Pigment – Adult Coloring Book –** com.pixite.pigment
- **Recolor Coloring Book to Color –** com.sumoing.ReColor
- **Sky Ticket –** de.sky.skyonline
- **The Weather Network –** com.theweathernetwork.weathereyeiphone

Shortly after the report was published, 10% Happier: Meditation and Hotel Tonight promised to stop the behavior and quickly followed through. TikTik also promised to stop but has never done so, Mysk said. None of the other apps has stopped either, he said.

Clipboard reading done right

In some cases, clipboard reading can make apps much more useful. The UPS iPhone app, for instance, pulls text from the clipboard and in the event the text matches the characteristics of a tracking number, the app prompts the user to track the corresponding package. Google Chrome also pulls text and, in the event it’s a URL, will prompt the user to browse to it. The Pixelmator photo editor reads data only if it’s an image. If it is, Pixelmator will prompt the user to open it for editing. In all three cases, the data reading has

a clear use case and is transparent.

TikTok and the other offending apps, by contrast, access the clipboard for no clear reason and with no indication they are doing so. For many apps, it’s hard to see any legitimate performance or usability reason for the access. Mysk said that Apple plans to credit his and Haj Bakry’s research as a catalyst for the new clipboard notification put into iOS 14.

The clipboard reading Haj Bakry and Mysk reported raises concerns that likely extend to those using Android and possibly other operating systems. Mysk said that clipboard reading in Android apps is “even worse” than iOS because the OS APIs are so much more lenient. Until version 10, for instance, Android allowed apps running in the background to read the clipboard. iOS apps, by contrast, can read or query clipboards only when active (that is, running in the foreground).

Mysk said that Apple’s notification feature is a good start but, ultimately, Apple and Google should do more. One possibility is to make clipboard access a standard permission, just as access to a mic or camera is now. Another possibility is to require app developers to disclose precisely what clipboard data is accessed and what the app does with it.

For now, users should remain aware that any data stored in the clipboard—despite it being inconspicuous to the naked eye—can be regularly accessed by apps that in many cases aren’t even installed locally on the device. When in doubt, flush the clipboard data by copying a character, word, or other piece of innocuous data.

https://arstechnica.com/?p=1687883