Opinion: Banning TikTok could weaken personal cybersecurity

April 12 2023, by Robert Olson

Credit: Unsplash/CC0 Public Domain

TikTok is not be the first app to be scrutinized over the potential

exposure of U.S. user data, but it is the first widely used app that the U.S. government has proposed banning over privacy and security concerns.

So far, the discussion has focused on whether TikTok should be banned. There has been little discussion of whether TikTok could be banned, and there has been almost no discussion of the effects on cybersecurity that a TikTok ban could cause, including encouraging users to sidestep built-in security mechanisms to bypass a ban and access the app.

As a cybersecurity researcher, I see potential risks if the U.S. attempts to ban TikTok. The type of risk depends on the type of ban.

Blocking TikTok in the network

Blocking access to TikTok by filtering traffic destined for addresses believed to be owned by TikTok is possible but would be difficult to accomplish. Server addresses can be changed and a TikTok ban could devolve into a game of cat and mouse.

Additionally, this sort of block could be bypassed using virtual private networks (VPNs), which encrypt data flowing between servers and devices. VPNs can be used to shield traffic between servers in other countries and devices in the U.S. VPNs were once widely recommended for people using public Wi-Fi, and people are already using VPNs to access blocked streaming services. While security experts no longer recommend VPNs for public Wi-Fi, many people have used them and so are familiar with a tool that would help them bypass a TikTok ban.

DNS sinkholes are another technique that could be used in TikTok bans. DNS, the Domain Name System, is a network protocol that behaves like the internet's phone book. Computers need to know the IP address of a server in order to communicate with it. DNS allows a computer to look

up that address using a name convenient for humans to remember, such as www.google.com.

DNS sinkholes stop that lookup. DNS sinkholes don't directly block access to a server. Rather, they stop other computers from being able to look up the server's address. It's fair to think of a DNS sinkhole as removing someone's name from a phone book.

DNS sinkholes are often used to stop malware and advertisements. They could be used in a TikTok ban. However, DNS sinkholes only work if lookups are confined to DNS servers that are configured to be sinkholes. A ban using DNS sinkholes would likely cover most DNS servers that people's computers use by default.

However, you can relatively easily change DNS settings on your computer to circumvent a ban based on DNS sinkholes. There are many public DNS servers that people could use instead of their current DNS servers, which are commonly maintained by internet service providers. Blocking TikTok with DNS sinkholes would require significant international cooperation to make it difficult for people to find DNS servers that could access TikTok.

People circumventing a ban by looking for an alternate DNS server would be at risk. Unless a DNS server uses an uncommon extension named DNSSEC, you can't verify the integrity of a DNS response. A malicious DNS server could reply to a lookup with an IP address of a server that's under criminal control. This opens the door for a number of different kinds of attacks that could put your data at risk.

Banning TikTok from your phone

Another way TikTok could be banned is by blocking the TikTok mobile app. This would not affect U.S. users' ability to access the TikTok

website, but it could change how and how often people access TikTok. Blocking the app could address the concern that TikTok could be used without the user's knowledge to access other systems on a network that a mobile device is connected to. This has been the motivation for some local TikTok bans.

Removing TikTok from app stores is unlikely to succeed by itself. Both Android and iOS devices have the ability to install apps from alternative sources, a technique known as sideloading. While this added step may discourage some people, sideloading tutorials are widely available online, and there is already popular software that must be sideloaded to be used on a phone.

Mobile devices assume that mobile apps are coming from a trusted source. Both Google and Apple audit mobile apps prior to the app being available for download. While these reviews aren't perfect, they help ensure apps don't contain vulnerabilities or malware. When app stores aren't involved, security responsibilities change. Sideloading makes users responsible for verifying an app's legitimacy, and criminals could trick users into installing malicious apps from third-party sources.

But what about the millions of people who already have TikTok installed on their phones? Enforcing a TikTok app ban would likely require that it be removed from mobile devices. Apple has long had the ability to remove software from iPhones, and Google could remove apps using Google Play Protect. These tools are important security controls that, at least on Android devices, can remove malware even if it was sideloaded. Enforcing a ban using security controls could motivate users to disable these controls, which would weaken the security of their devices.

Users might even be motivated to "jailbreak" their iOS devices or "root" their Android devices to prevent Apple or Google from removing the TikTok app, which would further weaken security. Jailbreaking an iOS

device allows users to bypass security restrictions in the operating system. Rooting an Android device means gaining the highest level security access, which allows users to make changes to the operating system. Jailbreaking and rooting are prohibited by Apple and Google. Both actions void the user's warranty and undermine the security controls that limit criminals' access to mobile devices.

Security tradeoffs

I find it unlikely that a TikTok ban would be technologically enforceable. Even China struggles with content filtering. These difficulties may be why proposed legislation includes significant punishments for bypassing the ban.

Even if the punishments are not aimed at the average TikTok user, this proposed legislation—aimed at improving cybersecurity—could motivate users to engage in riskier digital behavior.

Provided by The Conversation

Citation: Opinion: Banning TikTok could weaken personal cybersecurity (2023, April 12) retrieved 10 April 2024 from https://techxplore.com/news/2023-04-opinion-tiktok-weaken-personal-cybersecurity.html