

Android App Security Best Practices

Presented by Isuru Tharanga Malawige





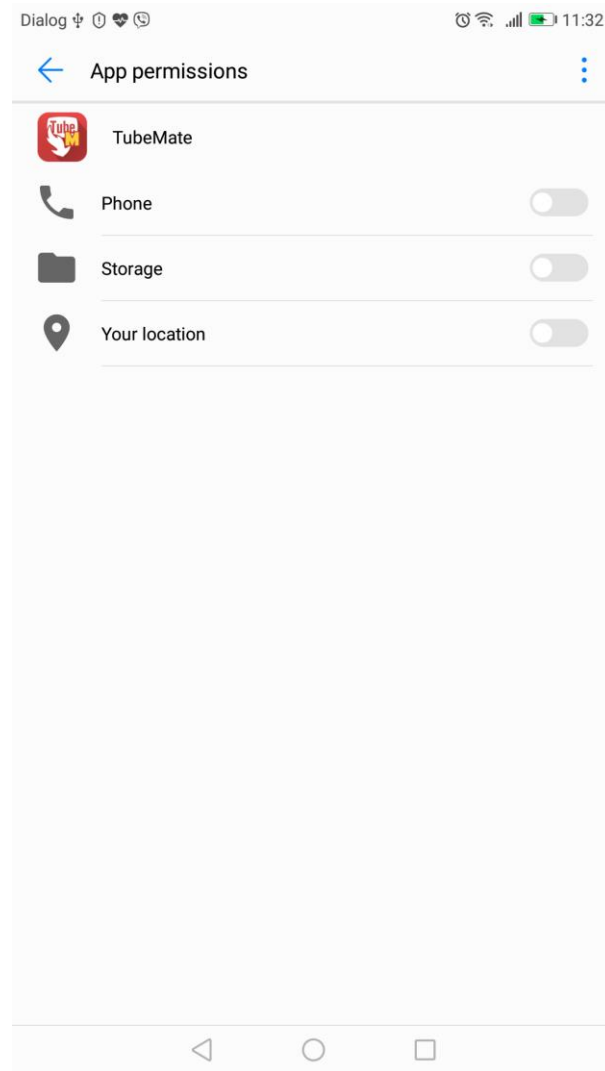
Demo

Remote access using a malicious APK (TubeMate)

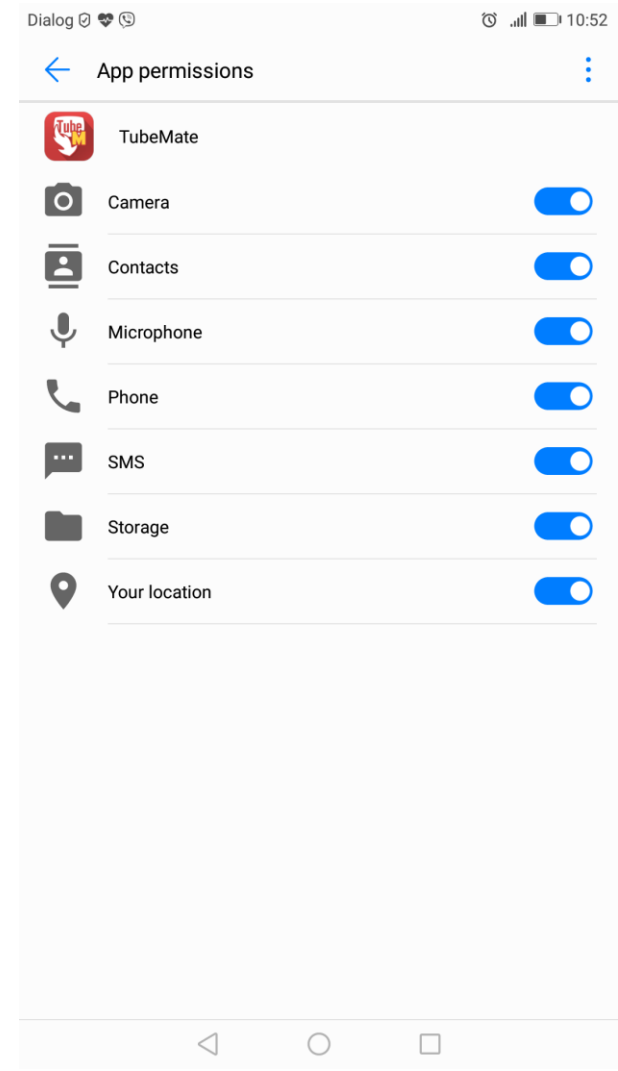


Permissions

Original App

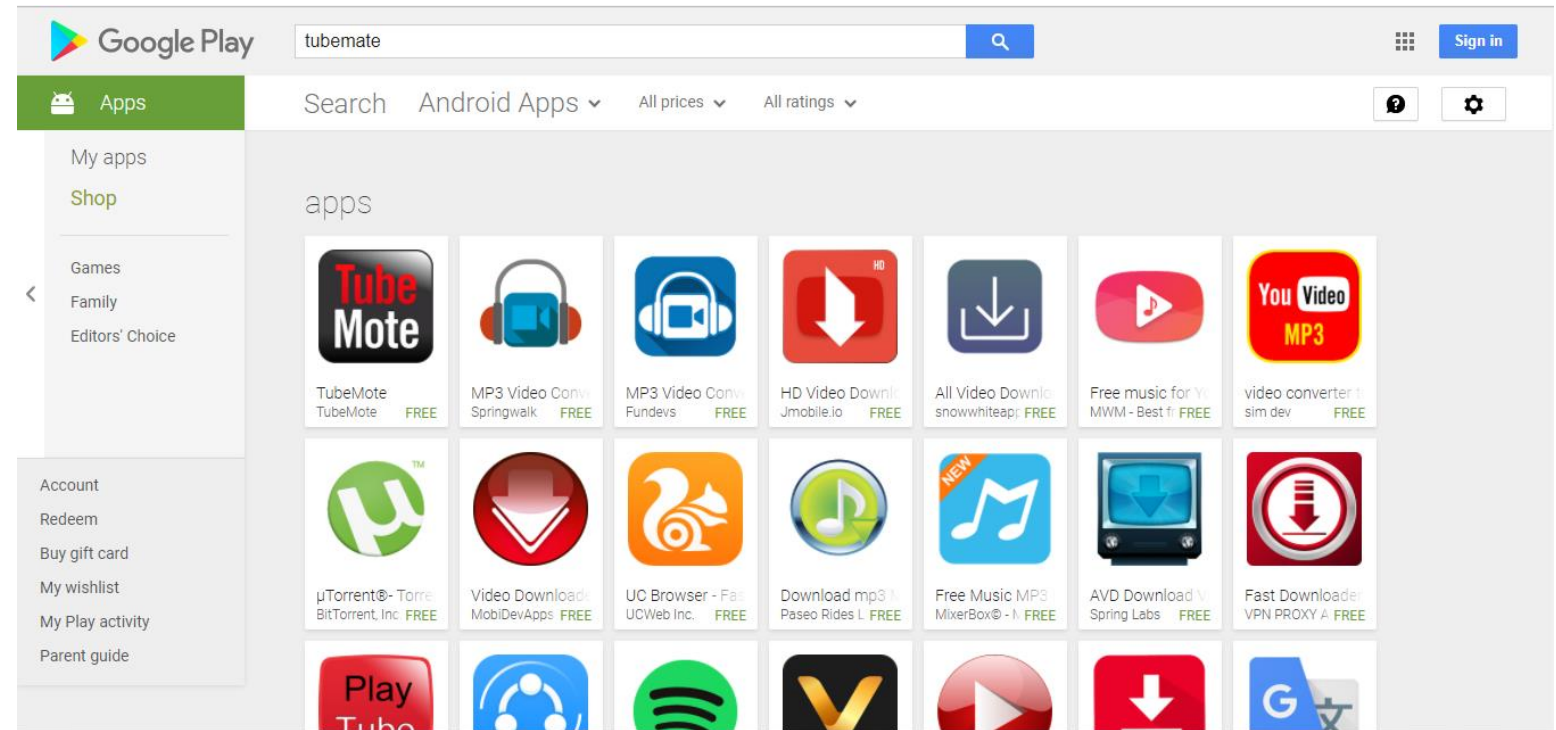


Malicious App



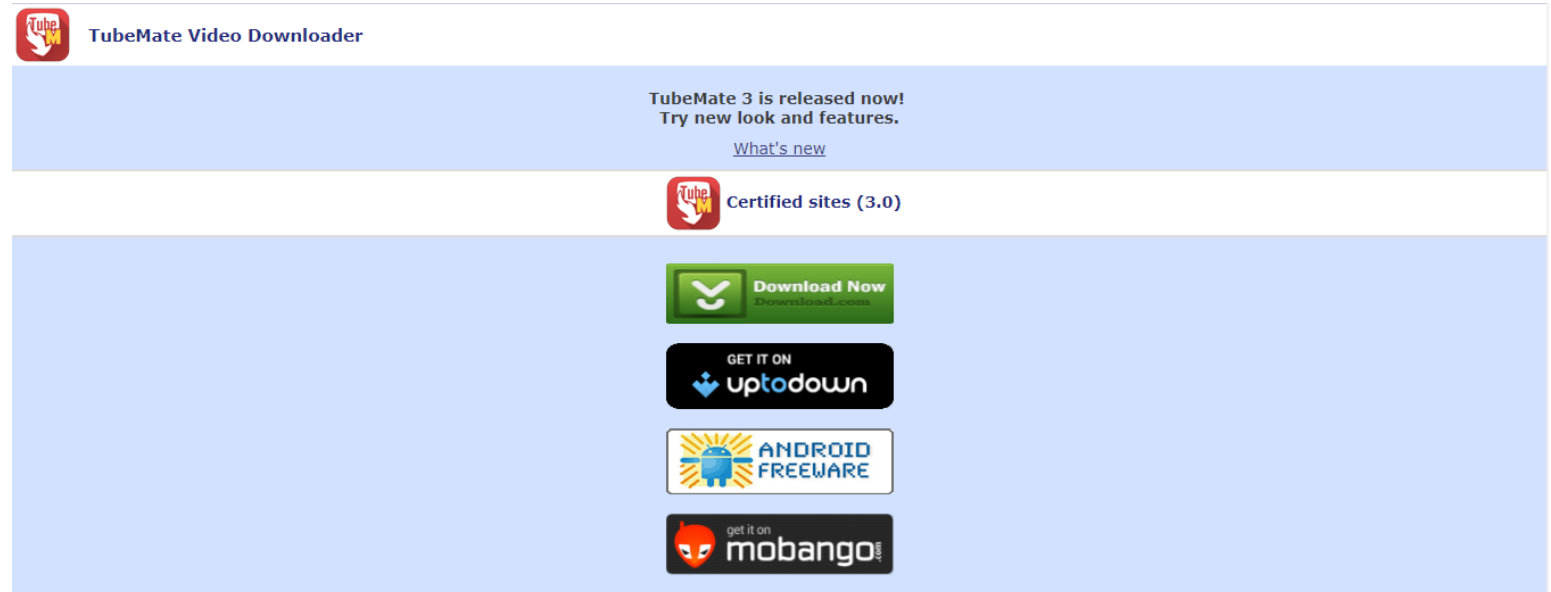
Google Play Store

TubeMate is not listed in Google Play Store




TubeMate Official Website

App download is directed to
3rd party App Stores


















APKMirror

**APKMirror**
Download Free Android APKs #APKPLZ




[All Developers](#) [Latest Uploads](#) [FAQ](#) [Contact](#)


Advertisement

October 26

	Gfycat Loops: GIF Cam+Recorder 0.2.21 by Gfycat, Inc.	 
	Mi FileExplorer V1-171025 beta by Xiaomi Inc.	 
	Skype Lite - Chat & Video Call 1.22.0.28740-release by Skype	 
	Starbucks 4.4.3 by Starbucks Coffee Company	 
	Action Launcher - Oreo + Pixel on your phone 29.1-beta1 by Action Launcher	 

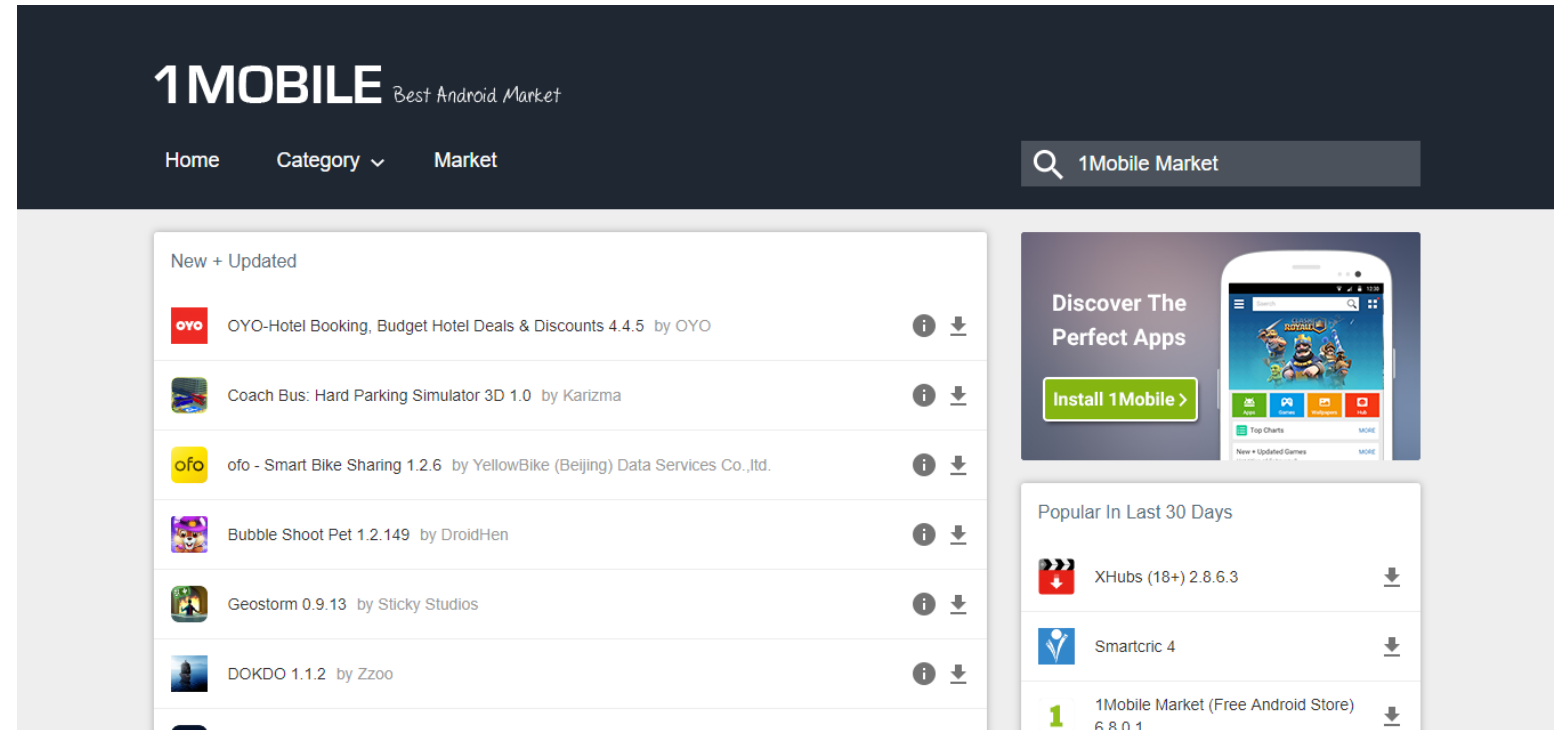
Follow APK Mirror

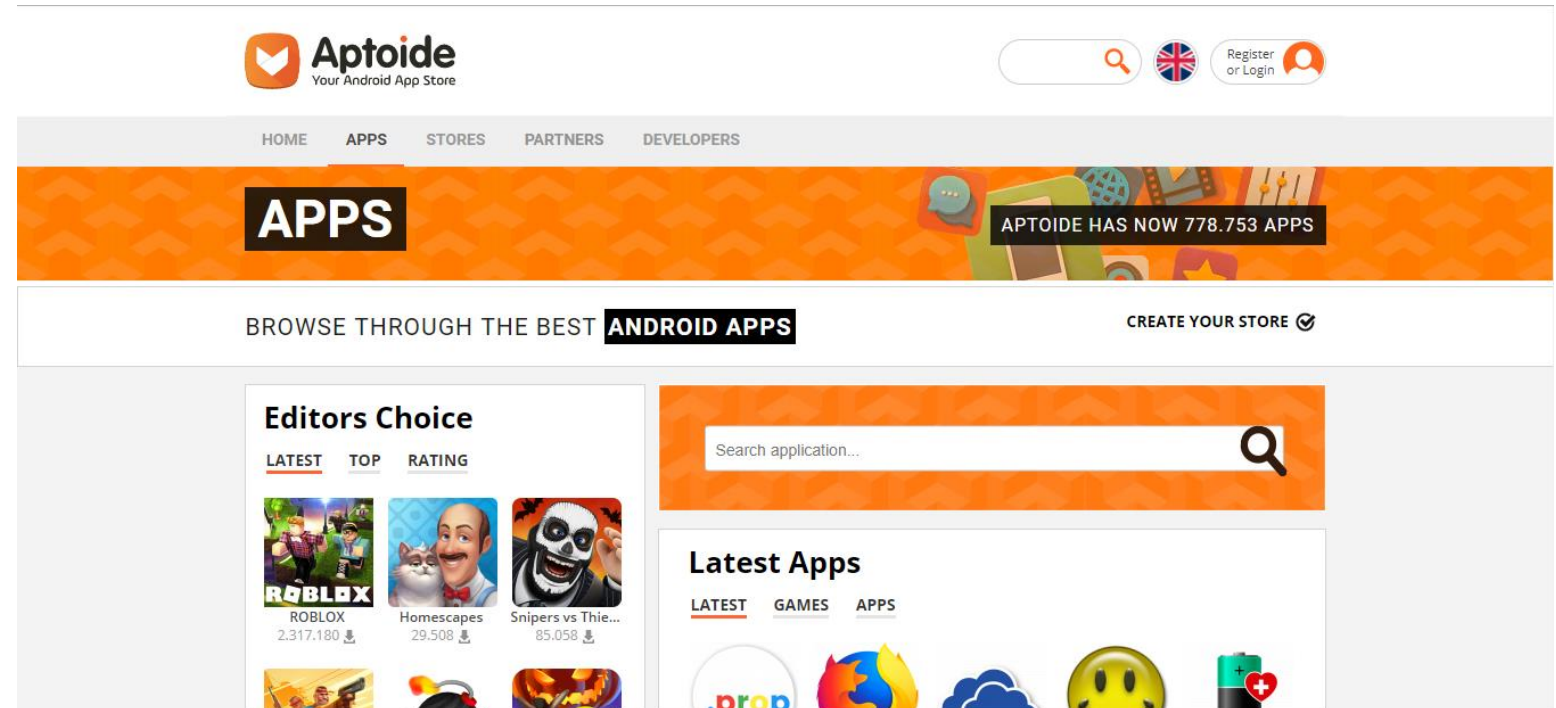
 Follow APK Mirror Updates

Advertisement

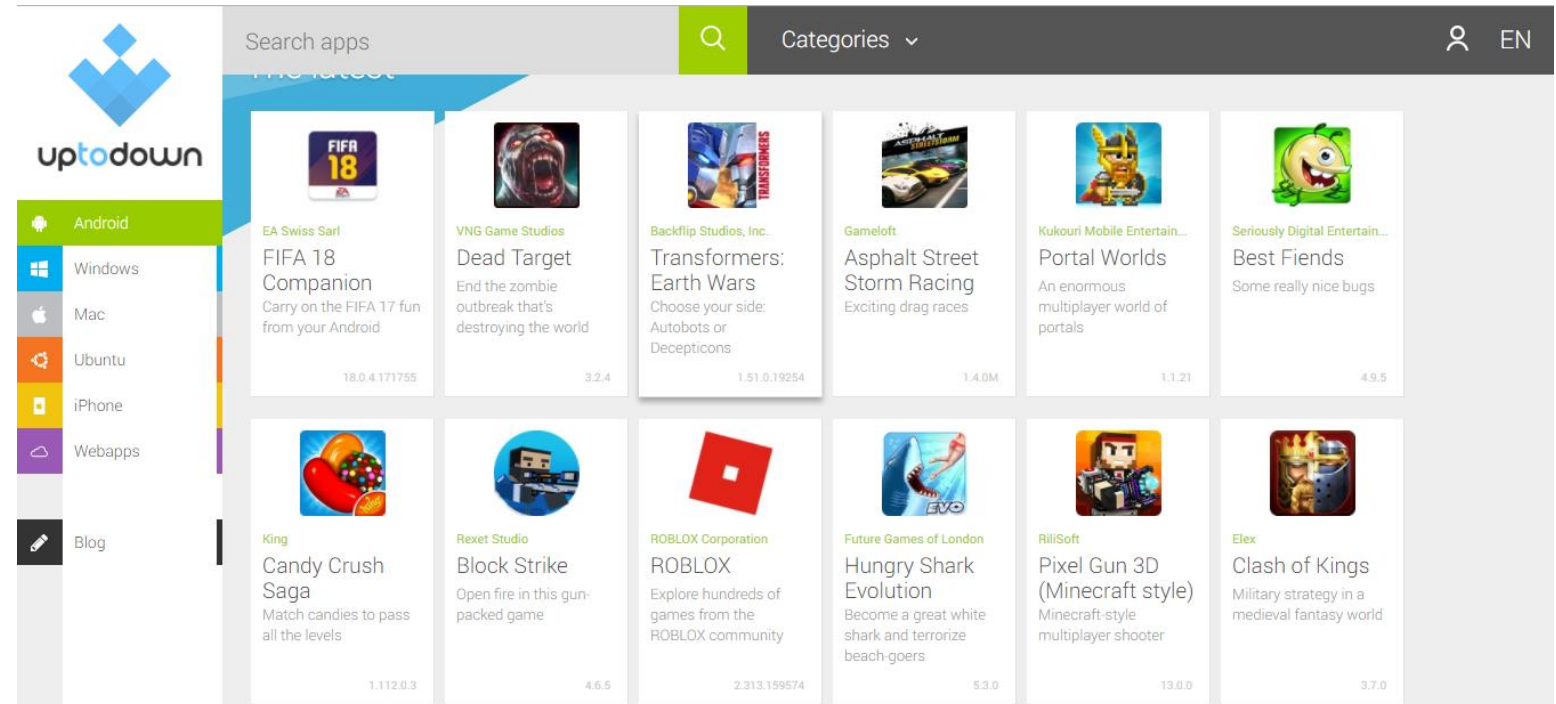
1Mobile



Aptoide



Uptodown



DoubleLocker

The First Ever Ransomware
**Misusing Android
Accessibility Services**

Spreading as a fake Adobe Flash
update via compromised websites
(Drive by Download)

Malware uses the activation of
'Google Play Services' accessibility
feature

Once executed, it first changes the
device PIN then encrypts all the
files using AES

[ESET Researchers Discover First-Ever Ransomware Misusing
Android Accessibility Services](#)

BlueBorne

Critical Bluetooth Attack on **zero-day vulnerabilities** in Bluetooth protocol

Take over Bluetooth-enabled devices, spread malware, or even establish a "man-in-the-middle" connection

No user interaction required to deploy the attack

Not required the victim's device to be paired with the attacker's device

The graphic features a light gray background with a subtle, abstract pattern of overlapping geometric shapes, including circles and triangles, creating a sense of depth and movement. Centered on this background is the text "Armish Labs" in a bold, dark blue font, with "Security Alert" in a smaller, lighter gray font directly beneath it.

Armish Labs
Security Alert

[Armish - BlueBorne Explained](#)

Best Practices

- Only use Google Play Store/ iTunes/ App Store to download apps
- Use a proper mobile security app and regularly scan your mobile device
- Make sure not to enable “Unknown Sources” feature on your mobile device
- Always check the permissions requested by apps before installation and disable unnecessary permissions
- Never download/open suspicious docx, xlsx, pdf files etc.
- Don’t click any random links and avoid opening any suspicious links in emails/text messages etc.
- Do not keep wireless technologies always enabled (Wi-Fi, Bluetooth)
- Keep your mobile device up-to-date (Install security patches/ update installed apps)
- Do not “root/ jailbreak” your mobile device (makes it more vulnerable)
- Keep your phone in your possession at all times.

Q & A

Thank You