“Accessibility Clickjacking” - The Next Evolution in Android Malware that Impacts More Than 500 Million Devices [update – 1.34 Billion Devices!] »

By 03 Mar, 2016 | By Yair Amit

Published: 2016-03-04 · Archived: 2026-04-06 00:10:22 UTC

Update: After presenting this research at RSA, confirmed on all Android versions through KitKat, it occurred to me that there may be a way to also run this on Android devices running Lollipop. My team was then able to test this and verify that Lollipop is also vulnerable to Accessibility Clickjacking, elevating the total exposure to **95.4% of all Android devices.**

After reading this blog, please see my new blog where I explain the additional steps hackers can take to use this exploit on almost any Android device in use today.

———

During our RSA Conference presentation today (Thursday, March 03, 2016 | 9:10 AM | West | Room: 3009), we covered the ongoing transition of mobile malware from being an inconvenience to consumers to a weapon that can be used by the hacker marketplace to steal sensitive corporate data.

We showed how modern mobile malware can evade detection by malware scanners that rely on signatures, static and dynamic analysis approaches. Then, we uncovered a working Android malware PoC that can persistently monitor all of a victim’s activity, and allow attackers to read and possibly compose corporate emails and documents via the victim’s device, as well as elevate their permissions to remotely encrypt or wipe the device.

One of the most interesting traits of this kind of malware is its low footprint: it does not require rooting the device and asks for limited permissions upon installation. Yet, this malware is able to circumvent many of the protections that most users assume are reliably protecting their Android devices and compromise corporate resources used via the device.

What are Accessibility Services and Why Are They Interesting?

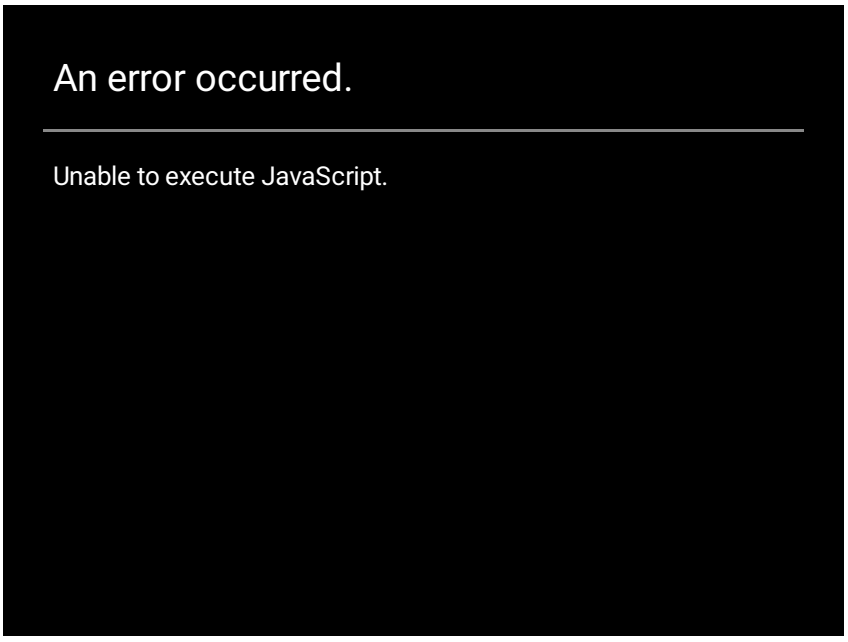
“An accessibility service is an application that provides user interface enhancements to assist users with disabilities, or who may temporarily be unable to fully interact with a device.” (Android’s Developer Documentation).

Accessibility APIs, which were introduced in Android 1.6 and significantly enhanced in Android 4.0, allow *Accessibility Services* to have access to the contents of the interfaces that a user interacts with (e.g., reading or composing an email, browsing or working on a document), as well as perform actions on the behalf of the user. These capabilities are great for aiding users with disabilities, as they can allow the creation of system-wide text to

speech tools, for example. However, these capabilities are also extremely attractive to malicious malware writers. Yet we don't see major malware utilize Accessibility APIs "in the wild." Why?

Android was built with the pre-ingrained understanding that *Accessibility Services* pose a clear threat to users. Consequently, in order for an Android App to gain Accessibility permissions, the user has to explicitly go through a rather long and unnatural process with a security warning at the end of it.

Demonstration of the Accessibility Permissions Approval Process



As you can see in this video, a malware that requires this process to be manually done by a victim is unlikely to get a major traction.

Introducing "Accessibility Clickjacking" Malware

Clickjacking is a term for a malicious UI redressing technique that tricks a victim into clicking on an element that is different than the one the victim believes to be clicking on. This technique, which relied on the ability of malicious websites to load a seemingly benign webpages with an invisible overlay from another service (attacked service), used to be a major concern in the web-application security world and yielded a variety of attacks against important services or frameworks, such as Facebook, Twitter and Flash.

While a variety of capabilities have been implemented into web browsers and web servers in order to mitigate the risk of clickjacking, mobile still remains vulnerable and it turns out that Android is susceptible to a similar kind of a threat.

It is worth noting that Clickjacking is not a theoretical threat – just a month ago, a ransomware named Android.Lockdroid.E that utilized Android Clickjacking to gain Admin rights was found by Symantec.

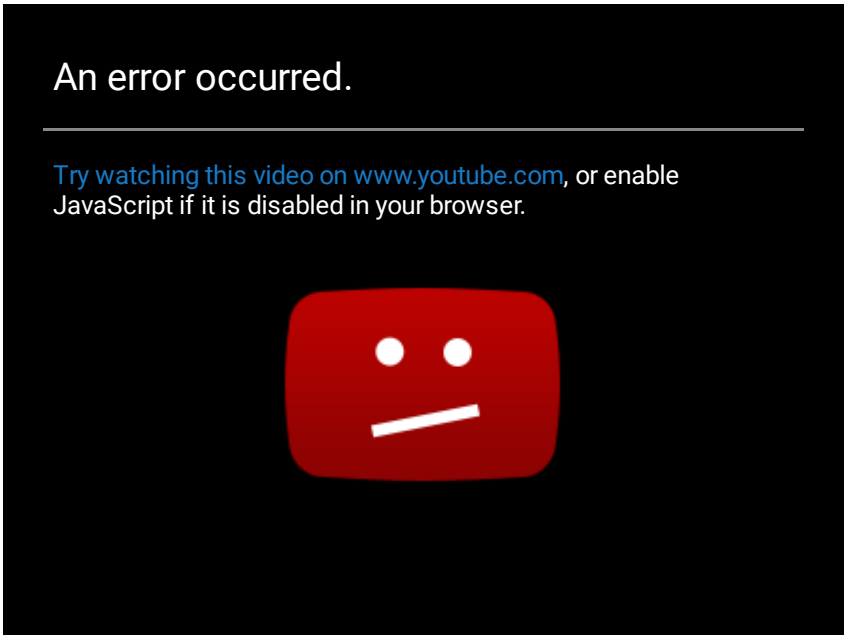
As we were trying to come up with an effective way to get victims to go through the series of clicks required to approve Accessibility permissions, we decided to utilize Clickjacking for the task.

We will be covering additional details in an upcoming webinar on this topic. Register to attend here.

Demonstration of the Attack Flow

The following video demonstrates:

- The victim plays a naive “Rick and Morty” themed rat-hitting game, which looks benign (yes, we can certainly improve on the graphics side – if we had time and resources to focus on non-customer-centric problems). What actually happens in the background might come as a surprise to the victim – his/her clicks are actually propagated to an underlying and invisible layer of the operating system – the Accessibility approval dialog. Completing the game means that the victim unknowingly approved Accessibility permissions for the “benign game”!
- The victim then continues using his/her Android device and composes an email to his/her CEO via the Gmail app. Every action from now on is recorded by the “Rick and Morty” game.

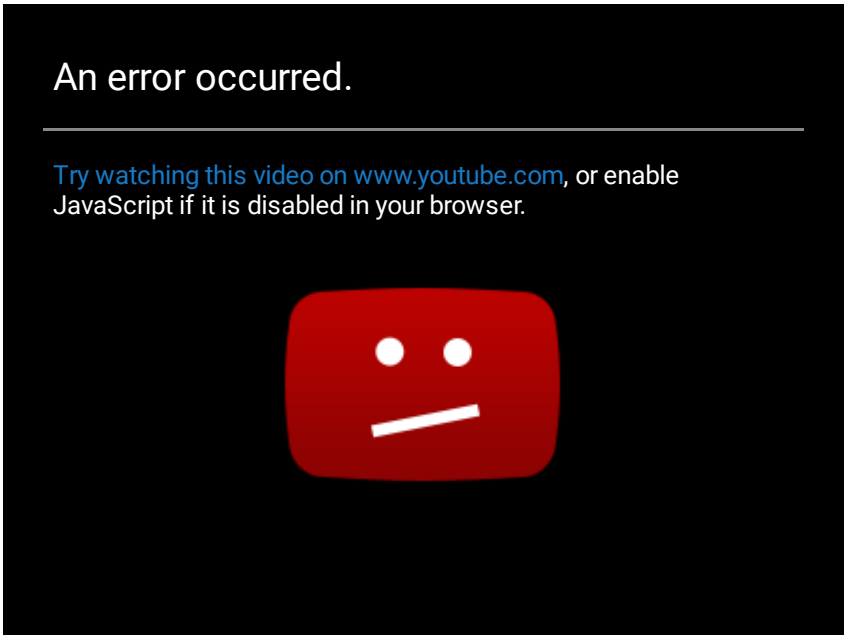


The Impact of “Accessibility Clickjacking”

Accessibility Clickjacking can allow malicious applications to access all text-based sensitive information on an infected Android device, as well as take automated actions via other apps or the operating system, without the victim's consent. This would include all personal and work emails, SMS messages, data from messaging apps, sensitive data on business applications such as CRM software, marketing automation software and more.

Taking it to The Next Level

Once Accessibility has been enabled on the device, hackers can even change admin permissions. No only that, the hacker can do so without having the victim click on anything or be aware of it happening. For example, the following video allows Rick and Morty game to enable a new Device Admin. This can have extreme implications including hacker's ability to encrypt the device's storage, change or disable its passcode or even wipe the device remotely.



Technical Details

This attack consists of a combination of permissions an Android app can request.

1. The SYSTEM_ALERT_WINDOW ("draw over other apps") permission. This permission allows an Android app to create any view over other apps. A great example of using this feature is Facebook Messenger's "Chat Heads" feature: allowing a user to read and reply to messages while using other apps. When creating an overlay view, a variety of flags can be used to specify the view's position and behaviour. In our example, we use TYPE_SYSTEM_OVERLAY to position the view over everything else with FLAG_NOT_FOCUSABLE, passing touch events to the view under the overlay.
2. An accessibility service implementation. An app can implement an accessibility service to assist a user with "visual, physical or age-related limitations".
   These apps receive rendering, touch, text and notifications events and respond to them.

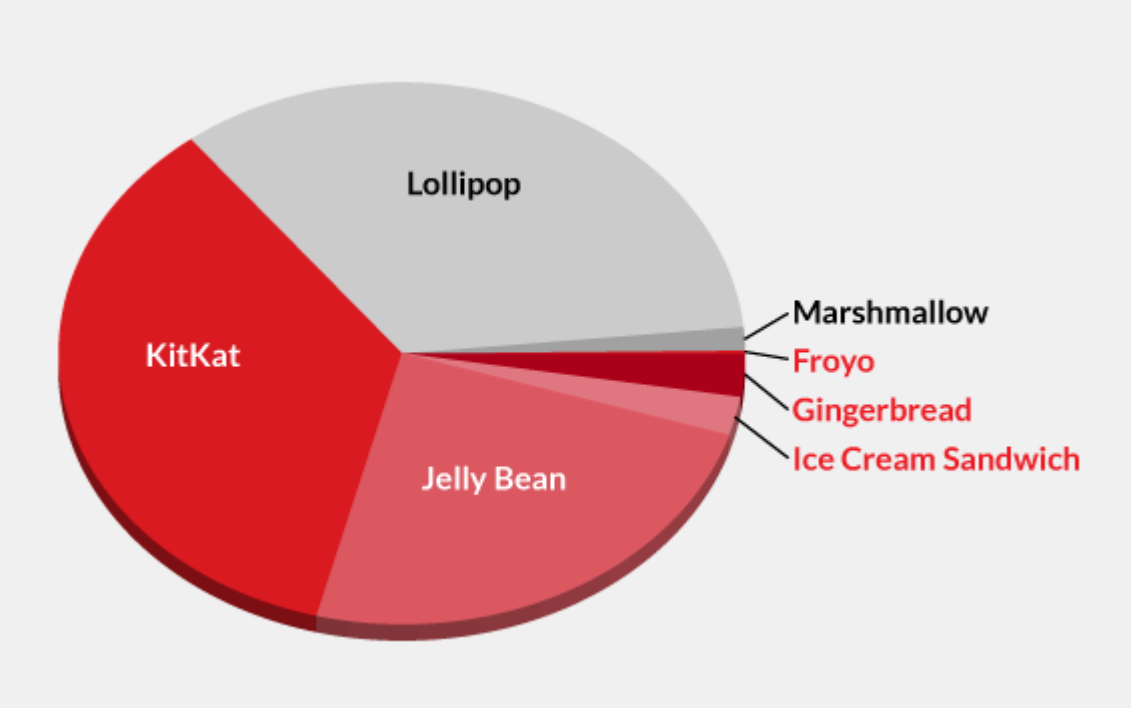
> Enabling an accessibility service shows the user a clear warning of what it will be able to do with the new permissions.

Our PoC shows what an attacker can do when combining these two Android features: a user can enable an accessibility service, without his/her consent or understanding of the risks involved in this action just by playing a simple game.

List of Android Versions Affected by Accessibility Clickjacking

We were able to demonstrate that the issue impacts all versions of Android except the last two versions – 5.x and 6.x. This would account for about 65% of the devices at this point of time – a staggering number of more than 500 Million Android devices being vulnerable.

Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 – 2.3.7	Gingerbread	10	2.7%
4.0.3 – 4.0.4	Ice Cream Sandwich	15	2.5%
4.1.x	Jelly Bean	16	8.8%
4.2.x		17	11.7%
4.3		18	3.4%
4.4	KitKat	19	35.5%
5.0	Lollipop	21	17.0%
5.1		22	17.1%
6.0	Marshmallow	23	1.2%



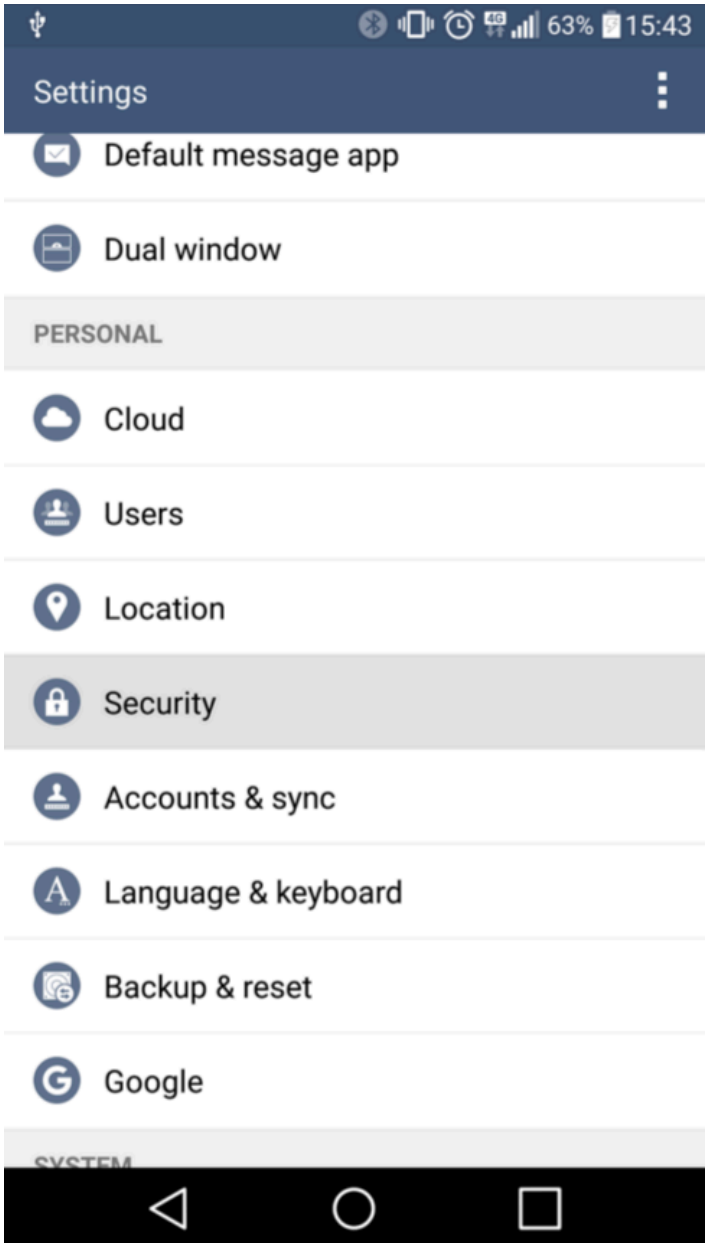
Source: Android.com

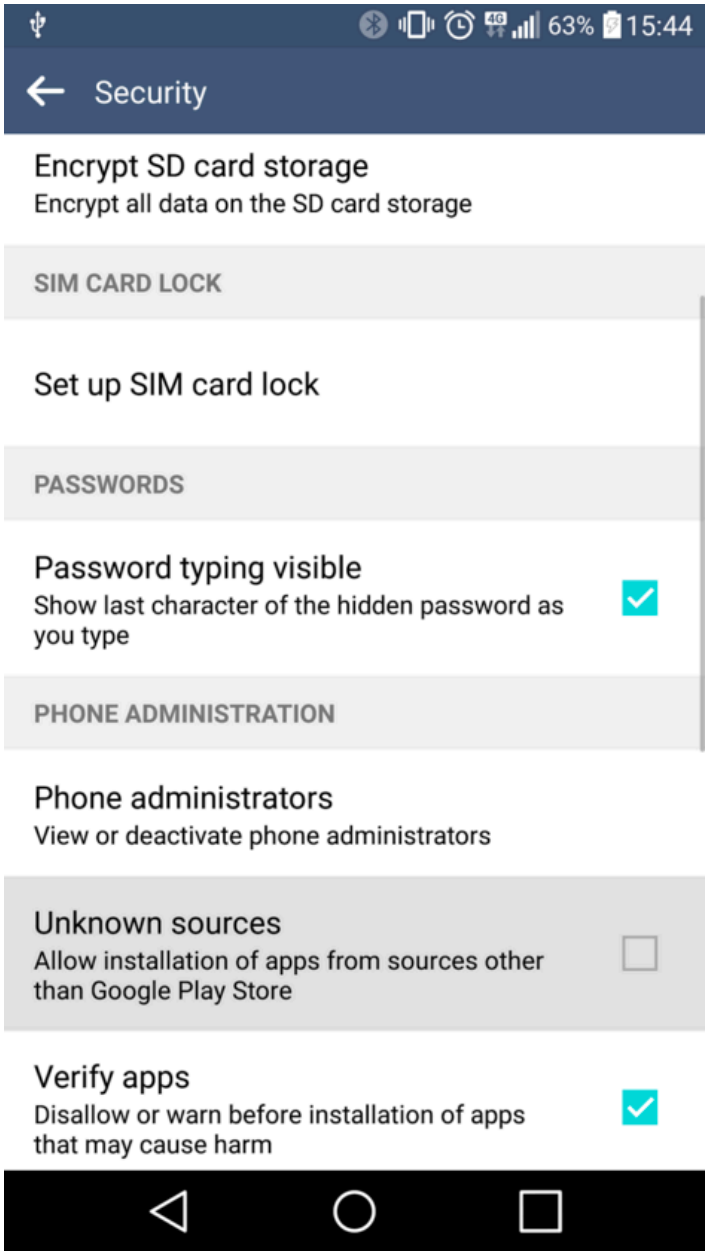
Remediation

With the Skycure App, one could persistently detect threats across all mobile attack vectors, including malware, and automatically apply relevant security and compliance policy to alert on, quarantine, or block infected devices.

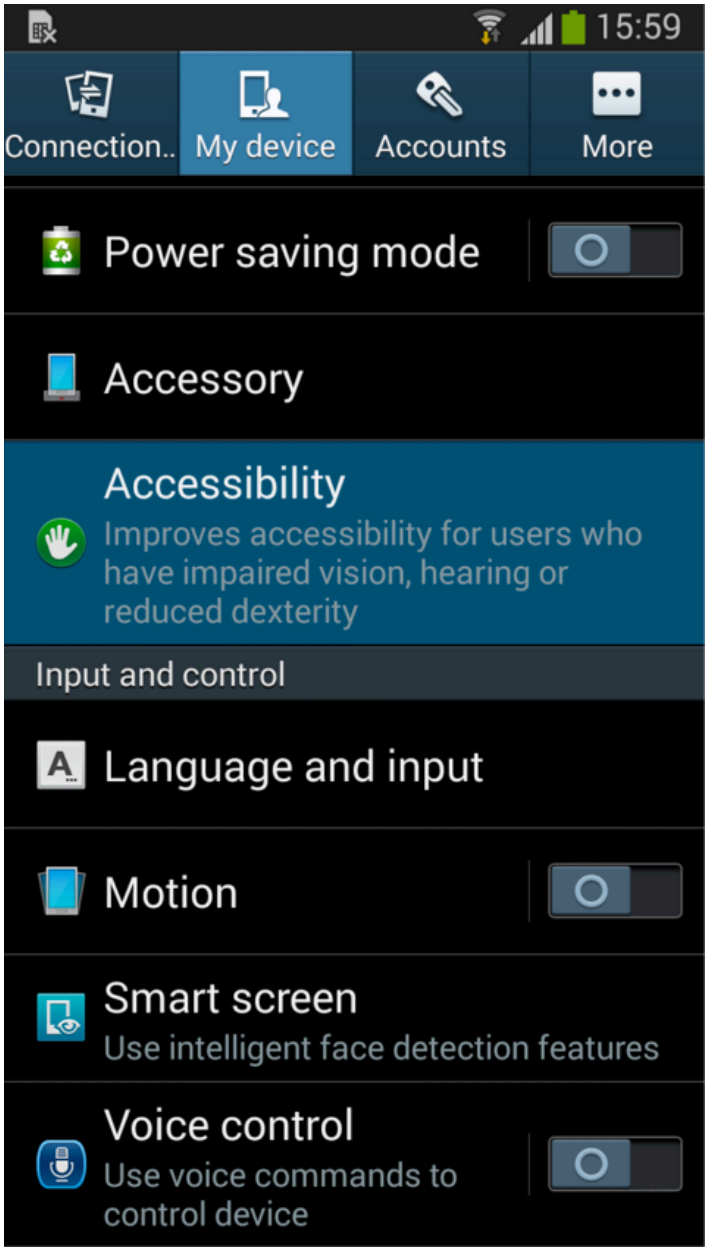
The following is a list of user behavior recommendations to better protect end users from mobile threats:

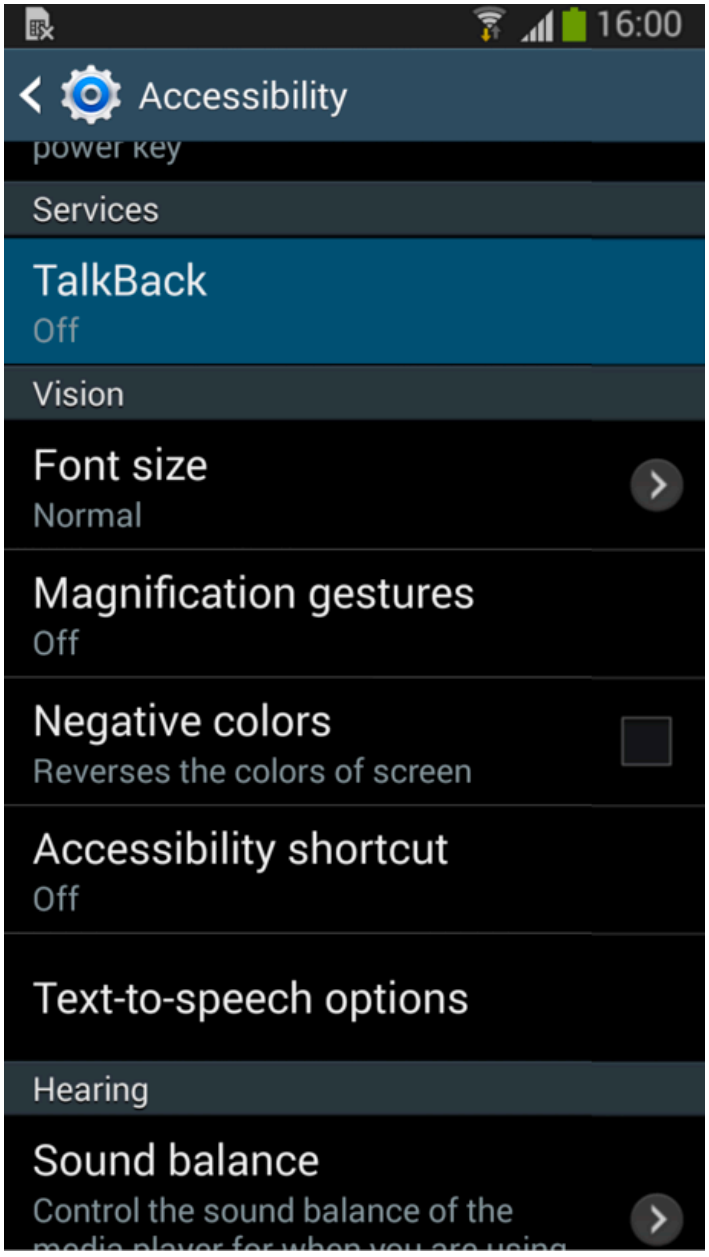
1. Update the operating system to the latest as soon as an update becomes available
2. Do not click on any dialogue boxes popping up on your phone unless and until you are sure about the action that caused them to appear
3. Do not install applications from third-party app stores if you do not trust them (while in many cases this is not a realistic option, try to switch off the setting that allows third-party app installation)
   (a) Step 1 – Open “Settings” app.
   (b) Step 2 – Navigate to “Security” settings
   (c) Step 3 – Uncheck “Unknown sources”


63% 15:43
Settings
Default message app
Dual window
PERSONAL
Cloud
Users
Location
Security
Accounts & sync
Language & keyboard
Backup & reset
Google



4. Check for apps that utilize accessibility permissions on your device and turn this option off if you don't recall turning it on or if you do not require that functionality.
   (a) Open "Settings" app.
   (b) Navigate to "Accessibility" settings
   (c) Make sure there is either no there is no group named "Services", or the group has no enabled entries.


15:59
Connection..
My device
Accounts
More
Power saving mode
Accessory
Accessibility
Improves accessibility for users who have impaired vision, hearing or reduced dexterity
Input and control
Language and input
Motion
Smart screen
Use intelligent face detection features
Voice control
Use voice commands to control device



5. Download a mobile threat defense app to scan your device for any existing and future malicious applications.

If you need help with assessing whether your organization is at risk because of any mobile vulnerability, threat or attack, you can request a free trial of Skycure Enterprise Edition here.

Acknowledgments

I'd like to thank Elisha Eshed from Skycure Research for his great contribution to this research.

Are your mobile devices impacted? Find out with a free assessment.

FIND OUT NOW
