بدافزاری پیچیده

# 500 میلیون دستگاه اندرویدی در تیررس بدافزاری جدید + راه‌کار مقابله

اندروید، سیستم‌عامل موفقی که این روزها میزبان بسیاری از گجت‌ها شده و بسیاری از کاربران و شرکت‌های بزرگ به صورت شخصی یا حرفه‌ای از آن استفاده می‌کنند؛ درگیر مشکل امنیتی تازه‌ای شده است. آن‌گونه که شرکت Skucrue گزارش داده است، گونه جدیدی از بدافزارهای مخرب که بر مبنای تکنیک accessibility clickjacking (دسترسی کلیک دزدی) رفتار می‌کنند، نزدیک به 500 میلیون دستگاه اندرویدی را در معرض تهدید قرار داده‌اند.

گزارش منتشر شده از سوی مؤسسه امنیتی Skycure نشان می‌دهد، هکرها با تکیه بر روش دسترسی کلیک دزدی (accessibility clickjacking ) توانایی هک کردن دستگاه‌های اندرویدی را دارند. در این ساز و کار، قربانی روی لینکی که به ظاهر بی خطر نشان داده می‌شود، کلیک کرده و به سایت آلوده‌ای وارد می‌شود. در حالی که قربانی چنین می‌پندارد که سایت مورد بازدید بی خطر است، اما در پشت پرده سایت با سرویس دیگری ارتباط برقرار کرده و به این شکل هکر به درون دستگاه اندرویدی کاربر وارد می‌شود.

## مطلب پیشنهادی

بیگانه‌ای پرسه می‌زند!

**خطر در کمین دستگاه‌های اندرویدی مبتنی بر تراشه‌های مدیاتک**

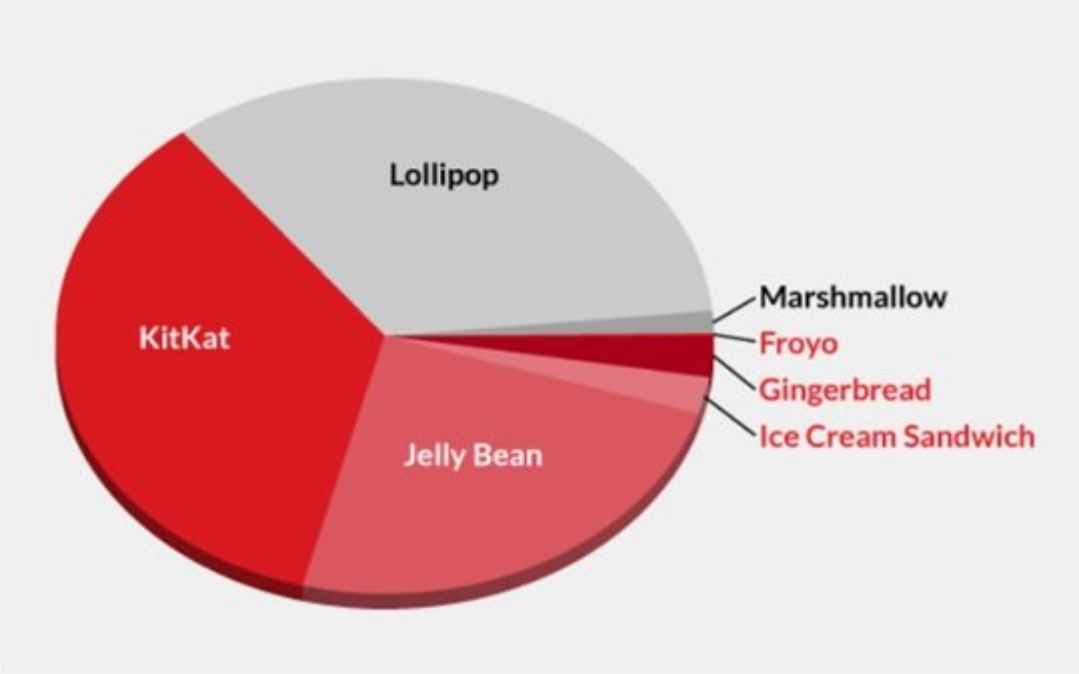
زمانی که کاربر صفحه آلوده‌ای را بارگذاری می‌کند، هکر این توانایی را پیدا می‌کند تا اطلاعات متنی حساس را مورد ربایش قرار داده و حتی کنترل گوشی را از طریق برنامه‌های تایید نشده یا مؤلفه‌های تأیید نشده سیستم‌عامل و به دور از دید کاربر به دست آورد. در این روش هکر بدون هیچ‌گونه مشکلی به ایمیل‌ها، داده‌های موجود در برنامه‌های پیام‌رسان و داده‌های شخصی کاربر دسترسی خواهد داشت. زمانی که هکر به دستگاه اندرویدی وارد می‌شود، این توانایی را خواهد داشت تا دسترسی‌های سطح مدیر را دستکاری کرده و حتی حساب مدیریتی جدیدی در سیستم ایجاد کند. این‌کار به او این توانایی را می‌دهد تا از راه دور گذرواژه دستگاه قربانی را غیر فعال کرده یا اطلاعات روی دستگاه قربانی را پاک کند. یک سرویس دسترسی (accessibility service) یک برنامه کاربردی بوده که به کاربران این توانایی را می‌دهد با سرعت بیشتری با دستگاه خود به تعامل بپردازند.

این توابع به‌طرز گسترده‌ای در اندروید 4.0 مورد استفاده قرار می‌گیرند. این توابع به سرویس‌های خدمت‌رسان این توانایی را می‌دهند تا به محتوای رابط‌هایی که کاربر با آن‌ها به تعامل می‌پردازد دسترسی پیدا کرده و همچنین بر مبنای رفتار کاربر عملی روی این محتوا انجام دهند. ( این توابع توانایی پاسخ‌گویی به ایمیل، مشاهده یا کار کردن با

اسناد را دارند.) این قابلیت‌ها برای افرادی که دارای معلولیت هستند یک توان‌مندی بسیار مناسب ارائه می‌کنند. اما از طرفی این توابع به شدت مورد علاقه بدافزارنویسان نیز قرار دارد. بدافزاری که به تازگی توسط این مؤسسه شناسایی شده است، در نوع خود جدید نیست. تقریبا یک ماه پیش شرکت سیمانتک باج‌افزاری به نام Android.Lockdroid.E را شناسایی کرد که با ربایش کلیک توانایی دریافت مجوزهای سطح مدیریتی را داشت. گزارش منتشر شده از سوی این مؤسسه نشان می‌دهد نزدیک به 65 درصد از دستگاه‌های اندرویدی که از اندروید نسخه 2.2 تا 4.4 استفاده می‌کنند در معرض این تهدید قرار دارند.

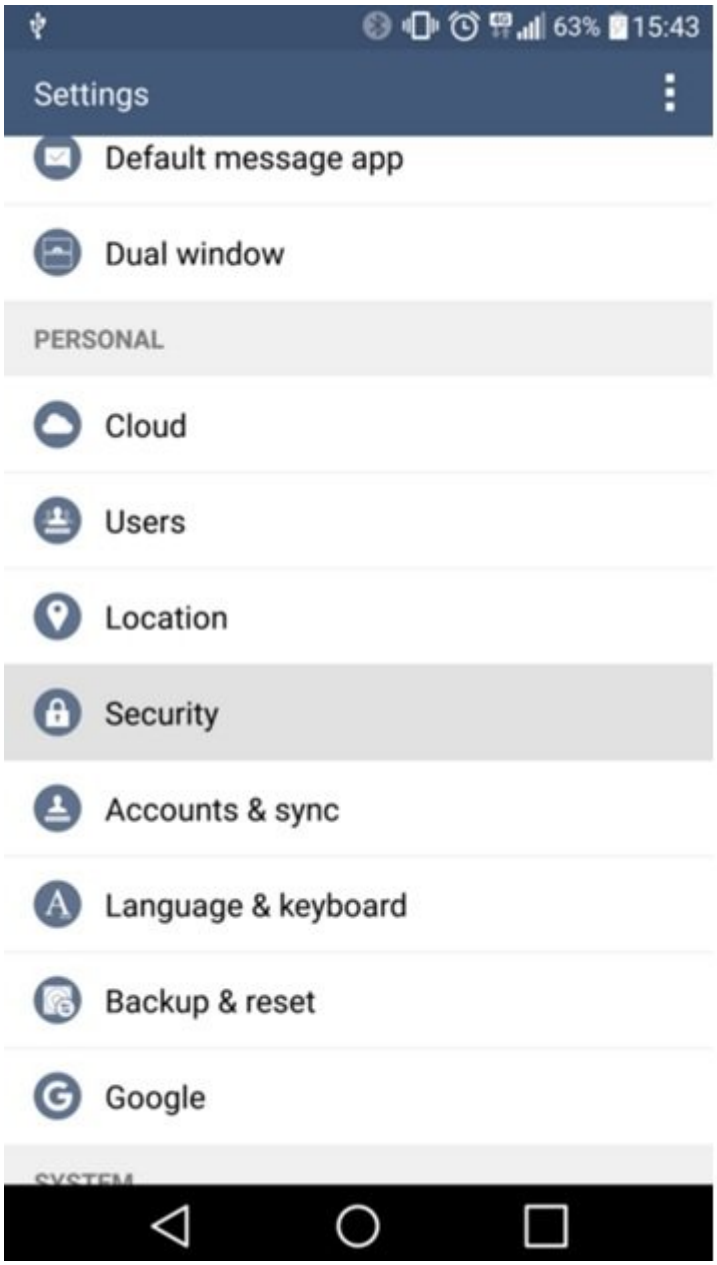
| Version | Codename | API | Distribution |
|---|---|---|---|
| 2.2 | Froyo | 8 | 0.1% |
| 2.3.3 – 2.3.7 | Gingerbread | 10 | 2.7% |
| 4.0.3 – 4.0.4 | Ice Cream Sandwich | 15 | 2.5% |
| 4.1.x | Jelly Bean | 16 | 8.8% |
| 4.2.x | | 17 | 11.7% |
| 4.3 | | 18 | 3.4% |
| 4.4 | KitKat | 19 | 35.5% |
| 5.0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

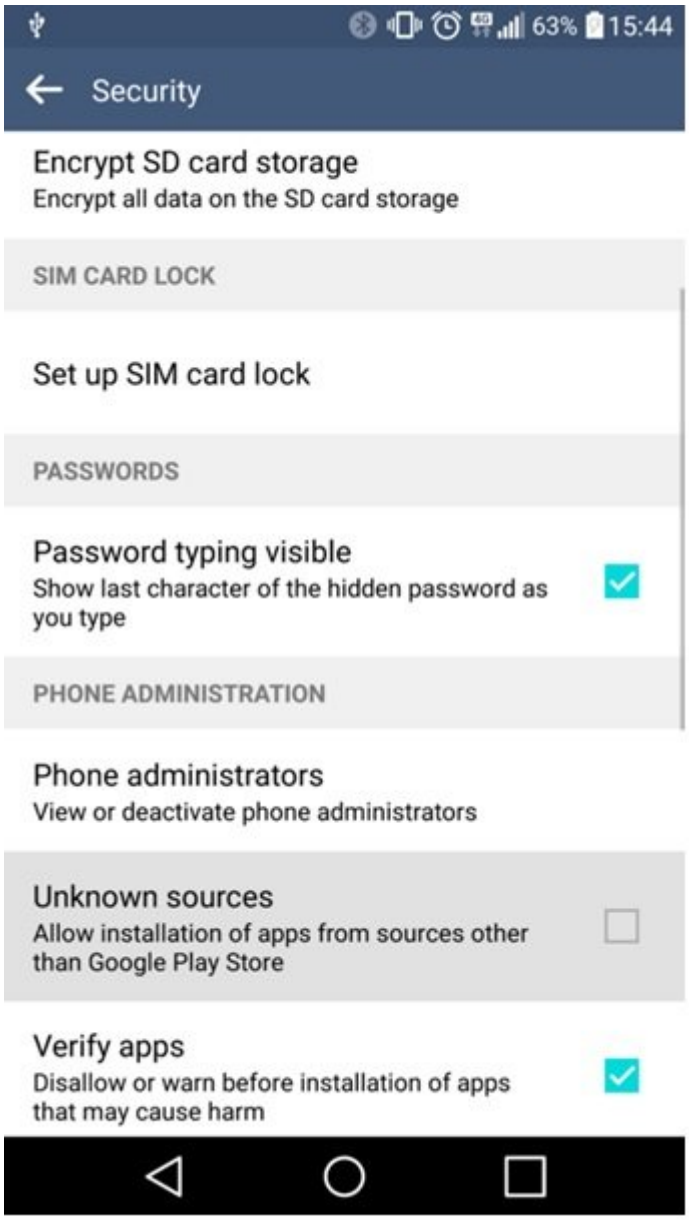
همان‌گونه که در تصویر زیر مشاهده می‌کنید، طیف گسترده‌ای از نسخه‌های مختلف به استثنای اندروید نسخه‌های 5 و 6 در معرض این تهدید قرار دارند.



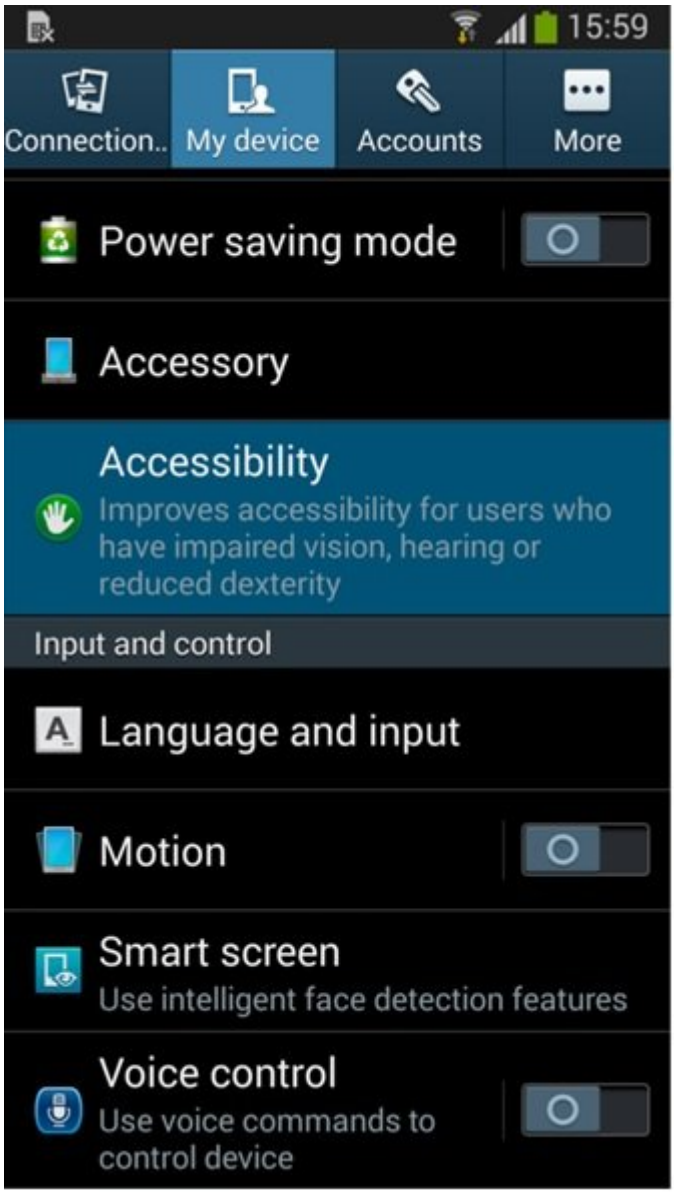

## اما چه کنیم که از این تهدید به دور باشیم؟

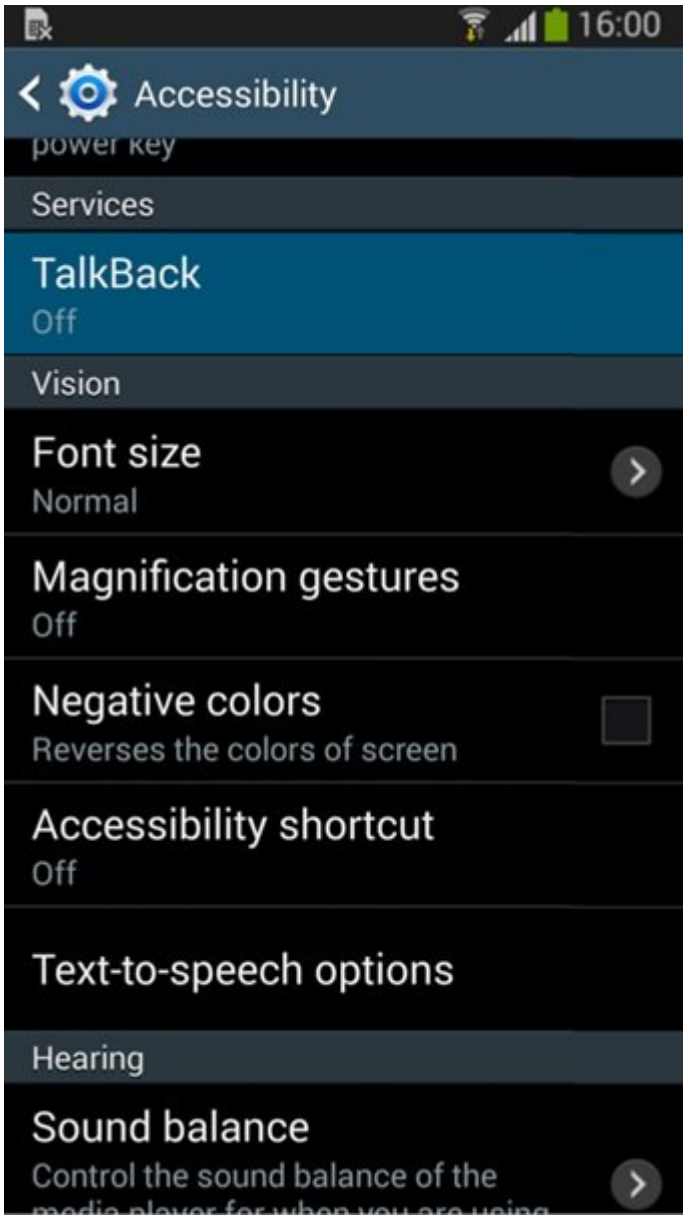
اگر جزء آن گروه از کاربران هستید که از نسخه‌های پایین اندروید استفاده می‌کنید، به شما توصیه می‌کنیم به اندروید نسخه 5 به بالا مهاجرت کنید. SkyCrue توصیه کرده است در اولین فرصت ممکن سیستم‌عامل دستگاه خود را ارتقا دهید، اما اگر شانس این‌کار را ندارید، بهتر است روی لینک‌های ناشناس کلیک نکرده و حتی‌المکان برنامه‌های کاربردی خود را از فروشگاه پلی استور گوگل دریافت کنید. همچنین به بخش تنظیمات (Settings) اسمارت‌فون خود رفته، به Security رفته و سپس گزینه Unknown sources را غیر فعال کنید.


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




مجوز برنامه‌هایی که روی دستگاه‌تان نصب شده‌اند را مورد بررسی قرار داده و اگر نیازی به گزینه accessibility ندارید آن‌را غیر فعال کنید. برای این منظور به Settings و سپس به بخش Accessibility بروید. اطمینان حاصل کنید گروهی به نام Services وجود نداشته یا اگر چنین گروهی وجود دارد، هیچ موجودیت فعالی در آن وجود نداشته باشد.


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




در نهایت از یک برنامه شناسایی تهدیدات موبایلی برای اسکن دستگاه خود و شناسایی برنامه‌های مخرب یا بدافزارهای احتمالی استفاده کنید.

**تاریخ انتشار:**
22 اسفند 1394

---

**نشانی منبع:** https://www.shabakeh-mag.com/security/3061