

آیا اندروید به آنتی‌ویروس نیاز دارد؟



از همان ابتدای ورود دو سیستم عامل اندروید و iOS به بازار، بحث امنیت جزء لاینفک رقابت میان این دو بوده است. اپل و طرفدارانش همیشه روی امنیت بالای آیفون در مقابل گوشی‌های اندروید مانور داده و بدافزارهای اندرویدی را به عنوان شاهد مثال آورده‌اند!

این امر سبب شده عده زیادی اندروید را به مثابه ویندوز به همراه ویروس‌های متعددش ببینند و این سیستم عامل وجه خودش را در زمینه امنیت در میان درصد قابل توجهی از کاربران از دست بدهد. بر این اساس، بسیاری این سوال در ذهنشان شکل گرفته که اندروید واقعا تا چه میزان امن است؟ آیا یک کاربر عادی اندروید باید نگران «ویروس» گرفتن گوشی یا تبلتش باشد و بنابراین به دنبال یک آنتی‌ویروس خوب؟

پاسخ سوالات مطرح شده بنا به گفته مسئولان ارشد اندروید، منفی است. کمی پیش از کنفرانس سالانه گوگل در اوایل امسال، ایدرین لودویگ (Adiran Ludwig) مسئول امنیت اندروید به خبرنگاران این‌طور گفته بود: «آیا من فکر می‌کنم کاربران عادی اندروید نیازی به نصب آنتی‌ویروس دارند؟ قطعاً خیر. من فکر نمی‌کنم بیش از ۹۹ درصد کاربران نفعی از یک اپ آنتی‌ویروس ببرند.» علاوه بر این، لودویگ معتقد است روی تهدیدات بدافزارهای اندروید زیادی تاکید شده است.

از سوی دیگر، شرکت‌های امنیتی و سازندگان اپ‌های آنتی‌ویروس برای اندروید چندان با این ادعا موافق نیستند. از نظر آنها ماجرا مانند بقال و ماست ترش می‌ماند و گوگل قاعدتا هیچ‌گاه به ایرادات فروشگاه پلی‌استور و اپ‌های مشکوک در آن اعتراف نخواهد کرد، اما اجازه دهید قضیه را کمی دقیق‌تر بررسی کنیم.



انواع ویروس‌های اندرویدی

در اصطلاح کامپیوتری، ویروس به‌طور ساده نوعی برنامه مخرب است که خودش را بین دستگاه‌های مختلف تکثیر کرده و گسترش می‌دهد. این نوع برنامه‌های مخرب سالیان سال کاربران ویندوز را آزار داده و می‌دهد. در مورد اندروید نیز با توجه به محبوبیت و توسعه فوق‌العاده آن، تهدیدات آن نیز رو به فراوانی گذاشته است. از نظر فنی نمی‌توان به بدافزارهای اندروید ویروس گفت، زیرا امکان تکثیر ندارند، با این وجود، این اصطلاح کماکان برای هر نوع بدافزاری به کار می‌رود.

در حالت کلی، بدافزارهای اندرویدی را می‌توان در پنج نوع تقسیم کرد: دسته اول، کپی‌کارها هستند یعنی نرم‌افزارهای تقلبی هم‌شکل و هم‌نام بازی‌ها و نرم‌افزارهای مشهور که کاربران به اشتباه آنها را نصب می‌کنند. این بدافزارها پس از نصب، ممکن است اقدام به جمع‌آوری و ارسال داده‌ها یا استفاده از تبلیغات اپ‌های دیگر به نفع خود کنند. نرم‌افزارهای کرک‌شده نیز می‌توانند در این دسته قرار بگیرند.

دسته دوم، باج‌افزارها هستند که با قفل کردن دستگاه، سعی در اجبار کاربر به پرداخت مبلغی برای آزادسازی آن دارند!

دسته سوم، بدافزارهای رباینده (Hijacking) هستند. این بدافزارها با روش‌های مختلف مانند تبلیغات و نوتیفیکشن‌های فراوان به نحوی کنترل گوشی را از دست کاربر درمی‌آورند تا او به ناچار روی سایت یا تبلیغی که آپ می‌خواهد کلیک کند و گوشی آلوده شود.

دسته آخر نیز بدافزارهای فیشینگ (Phishing) هستند که با شبیه‌سازی صفحه ورود سایت‌های معتبر یا پیام‌هایی چون «اینجا کلیک کنید تا

باتری‌تان افزایش یابد!» کاربر را به سمت ورود اطلاعات یا دانلود نرم‌افزارهای آلوده پیش می‌برند.

منشأ بدافزارهای اندرویدی

اصلی‌ترین و مهم‌ترین دروازه ورود بدافزارهای اندرویدی، منابع غیرمعتبر توزیع نرم‌افزار هستند. سایت‌هایی که انواع و اقسام نرم‌افزارهای پولی را به‌صورت رایگان قرار می‌دهند، دانلود فایل نصبی یک نرم‌افزار (apk) از تلگرام و دیگر شبکه‌های اجتماعی، مارکت‌های عجیب و غریب چینی و غیرچینی و مسیرهایی از این دست.

البته این به آن معنا نیست که در دیگر مارکت‌ها و حتی خود پلی‌استور بدافزار وجود ندارد. درصد زیادی از هکرها و برنامه‌نویسان این بدافزارها، از ایرادات امنیتی استفاده کرده و نرم‌افزارهایشان را به اشکال مختلف وارد پلی‌استور می‌کنند. گوگل نیز به‌طور مستمر این نرم‌افزارهای مشکوک را حذف و حفره‌های امنیتی کشف‌شده را می‌بندد، اما این روند در هر حال به‌صورت یک بازی موش و گربه پیش می‌رود!

بالاخره آنتی‌ویروس نصب کنم یا نه؟

پیش از آن‌که به فکر نصب آنتی‌ویروس بيفتید، چند نکته امنیتی بسیار مهم وجود دارد که با رعایت‌شان در ردیف آن دسته کاربرانی قرار می‌گیرید که اصلاً نیازی به آنتی‌ویروس نخواهند داشت. اولین نکته آن است که مسیر ورودی بدافزارها را ببندید و تمام نرم‌افزارها و به‌روزرسانی‌هایشان را از پلی‌استور یا مارکت‌های معتبر داخلی دانلود کنید. هرگز سراغ دانلود و نصب نرم‌افزار از منبعی که نمی‌شناسید، نروید!

هنگام نصب و استفاده از نرم‌افزارها هم حواستان به درخواست اجازه‌های آنها باشد. اگر دیدید نرم‌افزاری درخواستی خارج از کارکرد متعارفش دارد یا از نصب آن خودداری کنید یا در نسخه‌های بالاتر اندروید، این اجازه را به آن ندهید.

نکته دوم، به‌روزرسانی خود اندروید است. در هر نسخه جدید اندروید، حفره‌های امنیتی بسیاری رفع می‌شود که امنیت گوشی شما را بالاتر می‌برد. بنابراین در دانلود و نصب نسخه جدید سیستم‌عامل گوشی‌تان شک نکنید!

نکته سوم ارتباطی به خود بدافزارها پیدا نمی‌کند، اما در هر صورت لازم است همیشه از داده‌های روی تلفن همراه‌تان بک‌آپ بگیرید و تا حد امکان از نگهداری داده‌های حساس روی آن خودداری کنید تا اگر اتفاقی چه نرم‌افزاری و چه سخت‌افزاری افتاد، فهرست نگرانی‌هایتان شامل از بین رفتن یا دزدی اطلاعات خصوصی نباشد!