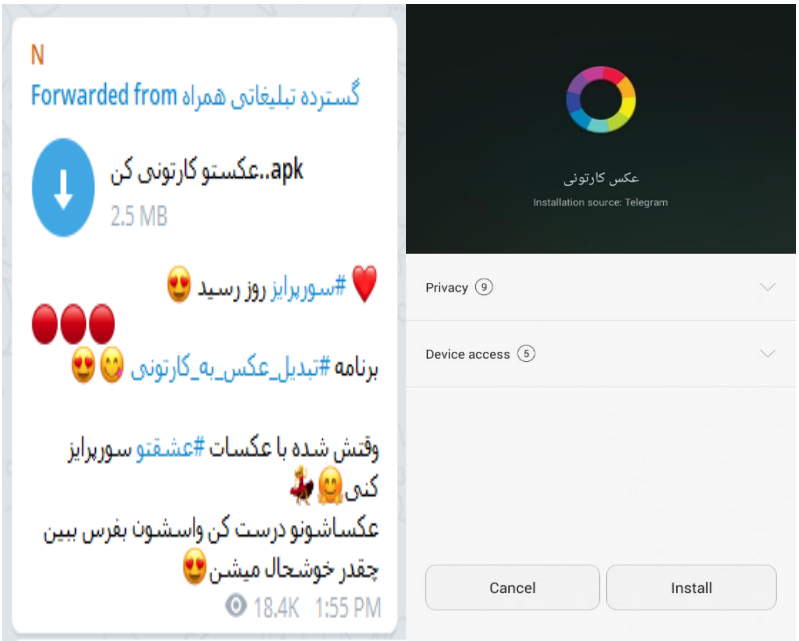
بدافزار موبایلی عکستو کارتنی کن

با گسترش برنامه‌های اندرویدی و در دسترس بودن راحت گوشی‌های هوشمند، این زمینه را برای افراد سودجو فراهم کرده تا با استفاده از برنامه‌های مخربی که تولید می‌کنند باعث آلودگی این گوشی‌ها شوند. یکی از این فایل‌های مخرب و بدافزار، برنامه اندرویدی **عکستو کارتونی کن** می‌باشد که برای پلتفرم‌های اندرویدی طراحی گشته و با استفاده از منابع ناامن دانلود نرم‌افزار در دسترس همگان قرار گرفته‌است. این برنامه بیشتر از طریق تلگرام که هیچ‌گونه فرآیند کنترل و تشخیص برنامه‌های ناامن ندارد و براحتی در اختیار همگان می‌باشد انتشار یافته‌است.

این برنامه در برخلاف کار اصلی خود که تبدیل عکس به حالت نقاشی می‌باشد، از شماره سیم‌کارت بدون متوجه شدن خود کاربر، استفاده کرده و آن‌ها را در سرویس‌های پیام کوتاه که هزینه‌های زیادی حدودا ۳۰۰ تا ۵۰۰ تومان برای هر پیامک دریافتی دارد، ثبت نام می‌کند.



شکل ۱

نحوه فعالیت بدافزار

این برنامه بعد از نصب توسط کاربر، قصد ارتباط با شبکه و اتصال به یکی از صفحات اینستاگرام را دارد که در این صفحه کلیپ‌ها انیمیشن نشان داده می‌شود. برنامه بعد از نصب با اتصال به سرورهایی

از شماره کاربر استفاده کرده و در سرویس‌های پیامکی ثبت نام می‌کند. این سرویس‌ها، سرویس‌های **زعفران** و **پرسپولیس** می‌باشد که هزینه‌ای **۵۰۰** تومنی برای هر پیامک دارد.

راه‌های مراقبت و پیشگیری

برای اینکه گوشی موبایل خود را ایمن نگه داریم و از افشای اطلاعات و سواستفاده از آن مراقبت کنیم باید راهکارهای زیر را در نظر بگیریم:

۱- از آنتی‌ویروس‌های قوی و معتبر استفاده کنیم.

بیشتر برنامه‌های آنتی‌ویروس قدرت لازم را برای تشخیص یک فایل بدافزار را ندارند و فقط اسم یک آنتی‌ویروس را بر روی خود دارند. هنگام استفاده از آن‌ها، بعد از تحقیق مختصری در می‌توان یک آنتی‌ویروس موبایلی قوی و خوبی را انتخاب کرد.

۲- از دانلود و نصب برنامه از منابع نامعتبر جلوگیری کنیم.

برنامه‌هایی که در منابع دانلود معتبر همچون Google Play عرضه می‌شوند با استفاده از محافظ‌هایی یکبار برنامه‌ها را بررسی می‌کنند. ولی بیشتر این برنامه‌ها هم امن نیستند. منابع نامتعبر شامل کانال‌های تلگرامی، مارکت‌های غیررسمی و ناشناخته شده، دریافت برنامه از یک شخص دیگر از طریق برنامه‌های اشتراک‌گذاری و غیره می‌باشد.

۳- هنگام نصب برنامه‌های موبایلی به دسترسی‌های درخواستی دقت کنیم.

یشتر برنامه‌ها برای کار خاصی طراحی شده‌اند مثلا برنامه‌ای برای تبدیل عکس به نقاشی می‌باشد ولی در صورتیکه به دسترسی‌های آن نگاه می‌کنیم امکان ارسال و دریافت پیامک هم وجود دارد. این نوع دسترسی‌ها غیرمعقول می‌باشند. لذا هنگام نصب برنامه‌ها به دسترسی‌های درخواستی توجه کرده و در صورتیکه برنامه‌ای قبلا نصب شده باشد می‌توان در تنظیمات مربوط به برنامه، دسترسی‌های غیرعادی را غیرفعال کرد.

۴- پشتیبان‌گیری مداوم از فایل‌ها و اطلاعات

بیشتر بدافزارها از نوع باج‌افزار می‌باشند و می‌توانند فایل‌ها و اطلاعات موجود بر روی گوشی موبایل را رمز کرده و دسترسی به آن‌ها را ناممکن کنند و یا در برخی از بدافزارها امکان حذف یا خرابکاری بر روی اطلاعات وجود دارد. لذا برای درمان بعد از آلوده شدن به بدافزار به فایل‌های پشتیبان نیاز پیدا می‌کنیم. برای این‌کار بصورت مداوم (هفتگی یا ماهانه) از فایل‌ها و

اطلاعات حساس و مورد نیاز فایل پشتیبان ایجاد کرده و آن‌ها را در یک دستگاه دیگر مانند کامپیوترهای شخصی نگهداری کنیم.

۵- عدم استفاده از نسخه‌های غیررسمی برنامه‌ها

برنامه‌هایی مانند تلگرام نسخه‌های غیررسمی زیادی مانند موبوگرام دارند که توسط توسط اشخاص دیگری توسعه داده شده‌اند و در منابع غیرمعتبر بیشتری ارائه شده‌اند. بیشتر این برنامه یک برنامه قانونی و امن نبوده و امکان آلوده‌سازی را دارند. لذا از نصب چنین برنامه‌هایی باید خودداری گردد و از نسخه‌های رسمی که توسط خود شرکت‌ها ارائه می‌گردد استفاده شوند.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

شماره تماس: ۰۴۵ – ۳۱۵۰۵۷۱۸

آدرس اینترنتی: cert.uma.ac.ir

آدرس: اردبیل – خیابان دانشگاه- دانشگاه محقق اردبیلی – دانشکده فنی – مرکز آپا محقق اردبیلی