اطلاع رسانی ای اسکن در خصوص جدیدترین ویروس تروجان بر روی دستگاه های اندروید

شرکت ای اسکن در مسیر پیشرفت خود در ارائه راه حل های امنیتی جهت محافظت و برقراری امنیت در دستگاه های اندروید در خصوص جدیدترین بدافزار (تروجان) یافت شده بر روی سیستم عامل های اندروید طی متن زیر اطلاع رسانی کرده است:
آخرین تحقیقات صورت گرفته حاکی از آن است که تروجانی به نام Android/Smssend بر روی دستگاه های اندروید یافت شده است که به عنوان یک نرم افزار (بدافزار) برروی دستگاه ها نصب شده و اطلاعات حیاتی دستگاه را سرقت می کند. این بدافزار یک سرویس پیشرفته از خانواده نرم افزارهای مخرب و مزاحم است که از طریق بازارهای برنامه های اندرویدی در حال عرضه و گسترش است.
پس از نصب ، این بدافزار بر روی دستگاه اندرویدی ، بلافاصله شروع به ارسال پیامک به لیست مخاطبین نموده که این پیامک حاوی لینک هایی است که دریافت کننده با کلیک بر روی آنها به این بدافزار آلوده شده و به این طریق آلودگی از دستگاهی به دستگاه دیگر منتقل خواهد شد. CERT-In در این خصوص می گوید پس از نصب این بد افزار بر روی دستگاه اطلاعات اولیه در خصوص آن دستگاه مانند IMEI ، مشخصه دستگاه (Device ID) ، نوع دستگاه و ... در معرض خطر قرار گرفته و حتی ممکن است یه نرم افزار جاسوسی بر روی آن دستگاه نصب و فعال شود.
علاوه بر این جدا از ارسال پیامک ، این برنامه شروع به سرقت اطلاعات مخاطبین، عکس ها، رمزهای عبور و گزارش موقعیت مکانی دستگاه می کند و همچنین ضمن آسیب رساندن به دستگاه اطلاعاتی نظیر اطلاعات بانکی و رمزهای بانکی سایتهای بانک که کاربر به آنها وارد می شود را نیز به سرقت می برد. همچنین با نصب برنامه های جاسوسی و خراب کردن فایروال آنتی ویروس نصب شده بر روی دستگاه امکان محافظت دستگاه از خود را نیز از بین می برد.

برای اطمینان از سلامت دستگاه خود و جلوگیری از آلوده شدن آن راه های زیر به شما پیشنهاد می شود:

۱. دستگاههای اندرویدی همیشه در معرض حمله قراردارند، بنابراین همیشه با یک آنتی ویروس مطمئن آنها را ایمن نگه دارید
۲. تمام نرم افزارهای نصب شده بر روی دستگاه خود را هر چند وقت یک بار به روز رسانی کنید.
۳. هنگام دانلود کردن برنامه ها هیچ گاه از سایت ها و منابع غیر معتبر استفاده نکنید.
۴. پیش از دانلود یک نرم افزار حتما به درجه بندی آن ، نظرات ارائه شده در خصوص آن و اعتبار آن نظرات توجه کنید.
۵. همچنین پیش از دانلود، کلیه مجوزهای مربوط به آن نرم افزار را بررسی کنید و بدانید به کدام قسمت از دستگاه شما دسترسی دارد.
۶. هیچ گاه به پیامک ها یا پیامهایی که از طرف شماره های ناشناس برای شما ارسال می شود توجه نکرده و پاسخ ندهید.
۷. هیچ گاه بر روی لینک هایی که از طریق پیامک برای شما ارسال می شوند کلیک نکنید.
۸. بهترین پیشنهاد این است که اطلاعات حافظه دستگاه خود را رمزگذاری نمایید تا امنیت کاملتر و بیشتری برای اطلاعات مهم و حیاتی موجود بر روی تلفن هوشمند شما ایجاد شود.
۹. همیشه به خاطر داشته باشید که از اتصال به شبکه های وایرلس غیر امن که ممکن است امنیت دستگاه شما را به خطر بیندازد جداً خودداری کنید.