بانک‌بات، بدافزار اندرویدی

بدافزار اندرویدی بانک‌بات بر اساس کدهای افشاشده بدافزارها نوشته شده است.

به گزارش واحد متخصصین سایبربان، محققان امنیتی بدافزار جدیدی به نام بانک‌بات (BankBot) را شناسایی کردند که با استفاده از کدهای افشاشده در اینترنت نوشته شده است.
کدهای مخرب که به‌صورت زیرزمینی در اینترنت منتشر می‌شوند، سریعاً توسط هکرها مورداستفاده قرارگرفته و ویژگی‌های بهتر و خاص‌تری به آن‌ها اضافه می‌شود؛ بدین ترتیب در حمله‌های سایبری قوی‌تر عمل خواهند کرد.

بدافزار بانک‌بات از همین نوع بدافزارها است که بر اساس کدهای منبع منتشرشده در اینترنت، توسعه یافته است. کد منبع این بدافزار به‌منظور سرقت پول کاربران، دسترسی مدیریت (Root) از اندروید گرفته و آن‌ها را کنترل می‌کند.

بدافزار بانک‌بات بر اساس همان روش کد افشاشده در بستر اینترنت رفتار می‌کند ولی پس از نصب و گرفتن کنترل سامانه کاربر، آیکون نرم‌افزار خود را پاک می‌کند.

بدافزار تا زمان ارتباط قربانی به بانک، منتظر می‌ماند؛ سپس صفحه فیشینگ خود را نمایش داده تا کاربر اطلاعات خود را وارد کند. البته این بدافزار اطلاعات شبکه‌های اجتماعی قربانی مانند فیس‌بوک، واتس‌اپ، اینستاگرام، توییتر، یوتیوب، اسنپ‌چت، وی‌چت، ایمو، اوبر و گوگل‌پلی را نیز سرقت می‌کند.بانک‌بات می‌تواند پیامک‌های کاربر را خوانده و آن‌ها را پاک کند. بدین ترتیب بدافزار می‌تواند حتی از احراز هویت دووجهی نیز عبور کند.

اداره حراست آموزشکده شهید یزدانپناه سنندج