گزارش بررسی بدافزار اندرویدی اینستا پلاس

com.miladaziziapps.instaplus

فهرست مطالب

۱- مقدمه

یکی از مسائلی که در دنیای تلفن‌های هوشمند همواره جای نگرانی بوده، موضوع حریم خصوصی است که در این رابطه، کارشناسان آزمایشگاه امنیت موبایل مرکز ماهر با رصد شبکه‌های اجتماعی یک بدافزار اندرویدی تحت عنوان «اینستا پلاس» را کشف کردند که IP کاربر را برای یک وب‌سرور ارسال می‌کند و موقعیت مکانی او را دریافت می‌کند. در ادامه به توضیح نحوه عملکرد این برنامک می‌پردازیم.

۲- معرفی برنامک

این برنامک در ابتدا دسترسی‌های موقعیت مکانی، تماس تلفنی و خواندن و نوشتن در حافظه گوشی را از کاربر می‌گیرد. اما **بدون اطلاع کاربر**، IP او را ارسال می‌کند و در پاسخ موقعیت مکانی کاربر را دریافت می‌کند. لازم به ذکر است این برنامک در مایکت ۶ هزار نصب فعال دارد و از طریق آدرس "https://myket.ir/app/com.miladaziziapps.instaplus" با عنوان «اینستا پلاس» در دسترس است (شکل ۱).

شکل ۱ برنامک اینستا پلاس در مایکت

در بخش بعدی با بررسی ترافیک برنامه به شرح درخواست‌های ارسال شده توسط برنامک به وب‌سرور می‌پردازیم.

۲-۱- بررسی ترافیک برنامک

پس از نصب برنامک، در بازه‌های زمانی نامشخص، IP کاربر برای یک وب‌سرور به آدرس "http://ip-api.com" ارسال می‌شود (شکل ۲).

شکل ۲ بسته ارسالی توسط برنامک به ip-api.com

در مرحله بعدی اطلاعات موقعیت مکانی کاربر از سمت وب‌سرور دریافت می‌شود (شکل ۳).

شکل ۳ بسته دریافتی از سمت وب‌سرور ip-api.com

سپس یک بسته حاوی اطلاعات گوشی کاربر مانند نام، مدل گوشی و ... به آدرس "http://adad.ir" ارسال می‌شود (شکل ۴).

شکل ۴ بسته ارسالی برنامک به سمت وب سرور adad.ir

۳- نتیجه‌گیری

در این گزارش به معرفی بدافزار اندرویدی «اینستا پلاس» پرداختیم. این برنامک IP کاربر را برای یک وب‌سرور ارسال می‌کند و موقعیت مکانی کاربر را دریافت می‌کند. سپس اطلاعات گوشی کاربر را به وب‌سرور "http://adad.ir" ارسال می‌نماید.