مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

تروجان ANDROIDOS_HIPPOSMS.A

تنظیم کننده:

مریم باصری

ویرایش: ۱

شماره سند: V-90/5-2

www.ircert.cc

ITRC
مرکز تحقیقات مخابرات ایران

کد آسیب پذیری: V-90/5-2

نام محصول آسیب پذیر: تروجان ANDROIDOS_HIPPOSMS.A

نوع سیستم عامل: Android

کشف توسط: Trend Micro

تاریخ کشف: 21 Jul 2011

سطح خطر: کم

شرح:

این تروجان پیام کوتاهی را به شماره حق بیمه چینی می فرستد. در نتیجه، کاربران آسیب دیده بدون دانش خود متهم می شوند.

برای بدست آوردن دید جامعی از این تروجان را به نمودار تهدید که در زیر نشان داده شده است توجه کنید.

این تروجان می تواند از فروشگاه های ثالث برنامه Android دریافت شود و کاربران چینی را مورد هدف قرار دهد. این برنامه های مخرب یک پیام از پیش تعریف شده به افراد موجود در لیست تماس کاربر ارسال می کند. به لینک متصل به یک کپی از نرم افزارهای مخرب راه دور اشاره می کند. همچنین برنامه فوق دارای قابلیت ارسال همین پیام به شماره حق بیمه است.

این تروجان برای دریافت یک فایل پیکربندی XML به یک URL خاص متصل می شود. فایل پیکربندی شامل یک URL دیگر است که در آن یک نسخه بروز شده از خود را می تواند دریافت کند.

این تروجان با عنوان ANDROIDOS_HIPPOSMS.A توسط Trend Micro کشف و نامگذاری شده است. این تروجان ممکن توسط دیگر بدافزارها، جاسوس افزار ها از یک سایت راه دور دانلود شود. همچنین ممکن است به طور ناخواسته توسط کاربران در هنگام بازدید از سایت های مخرب دانلود شود.

دستورالعمل حذف :

۱- کامپیوتر خود را با محصولات Trend Micro اسکن کنید و فایل کشف شده تحت عنوان ANDROIDOS_HIPPOSMS.A را پاک کنید.

منبع:

http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_HIPPOSMS.A