یک تولید کننده چینی هزاران موبایل آلوده به بدافزار فروخته است - دیجیاتو

پیمان حسنی | سه شنبه، ۰۴ شهریور ۱۳۹۹

محققان امنیتی در هزاران گوشی اقتصادی برند چینی Transsion دو بدافزار کشف کردند. به گفته آنها این بدافزارها به شکل پنهانی کاربران را در سرویس‌های اشتراکی پولی ثبت نام کرده و هزینه‌ای گزاف روی دست آنها گذاشته اند.

شرکت امنیتی Secure-D اواسط اسفند ماه سال ۹۷ حجم بسیار بالایی تراکنش مالی غیرعادی را از گوشی‌های Tecno W3 ساخت شرکت Transsion در کشورهای اتیوپی، کامرون، مصر، غنا و آفریقای جنوبی شناسایی و مسدود کرد. این شرکت در ادامه تراکنش‌های مالی غیرعادی را در ۱۴ کشور دیگر کشف کرد.

شرکت امنیتی یاد شده تا به امروز در مجموع ۱۹.۲ میلیون تراکنش مالی مشکوک از بیش از ۲۰۰ هزار گوشی را ثبت کرده که هدف آنها ثبت نام پنهانی کاربران در سرویس‌های اشتراکی پولی بوده است. این شرکت به منظور بررسی بیشتر چندین گوشی Tecno W2 آکبند و دست دوم را بررسی کرد و به نتایج نگران کننده‌ای رسید.

بررسی‌ها نشان داد روی گوشی‌های Tecno W2 بدافزاری به نام Triada نصب شده است. این بدافزار در گوشی درب پشتی ایجاد کرده و بدافزارهای دیگر را دانلود می‌کند. Triada به دستور هکرها کدهای مخرب را در گوشی اجرا کرده و سپس برای جلوگیری از شناسایی در فایل‌های سیستمی پنهان می‌شود.

شرکت Secure-D پس متصل کردن یکی از گوشی‌های Tecno W2 به اینترنت متوجه دانلود تروجانی به نام xHelper شد. این تروجان جان سخت با ریبوت کردن، پاک کردن اپ و حتی فکتوری ریست نیز از بین نرفته و پاک کردن آن حتی برای کاربران حرفه‌ای نیز مشکل است. تروجان xHelper پس از محیا شدن شرایط مناسب از جمله متصل شدن گوشی به شبکه اپراتور، کاربر را به شکل پنهانی در سرویس‌های اشتراکی پولی ثبت نام می‌کند.

Transsion می‌گوید نصب بدافزار روی گوشی‌های این شرکت توسط فروشنده‌ای ناشناس در پروسه زنجیره تأمین انجام شده و از برطرف کردن Triada در مارس ۲۰۱۸ و xHelper در اواخر سال ۲۰۱۹ خبر داده است. با این حال شرکت Secure-D می‌گوید همچنان تا آوریل ۲۰۲۰ در حال مسدودسازی آنها بوده و احتمالاً برای مدتی غیرفعال شده بودند.

دیجیاتو