iOS نیز در امان نیست

پنج میلیارد برنامه آندروید در معرض هک

نزدیک به چند سال متوالی بود که اخبار دنیای امنیت، حفره‌های امنیتی، وصله‌ها و آسیب‌پذیری‌ها همواره مایکروسافت را نشانه می‌رفتند، اما مدتی است کارشناسان امنیتی درباره آسیب‌پذیری‌های موجود در برنامه‌های آندروید و iOS هشدار می‌دهند. طبیعت منبع‌باز بودن یکی از نقاط ضعف برنامه‌های محبوب آندروید به‌شمار می‌رود.

محققان امنیت سایبری بیش از پنج میلیارد برنامه آندروید دانلود شده دارای آسیب‌پذیری را کشف کرده‌اند که هکرها با استفاده از اکسپلویت‌های موجود روی آن‌ها می‌توانند به سیستم‌عامل گوگل حمله کنند. یک Exploit یک قطعه نرم‌افزاری یا مجموعه‌ای از دستورات است که برای شناسایی خطاها یا آسیب‌پذیری‌های ناخواسته یا پیش‌بینی نشده روی یک برنامه کامپیوتری، سخت‌افزار یا یک وسیله الکترونیکی مورد استفاده قرار می‌گیرد.

مطابق با گفته‌های مؤسسه FireEye که تحقیقات و تجزیه و تحلیل‌هایی را حدفاصل ماه‌های ژانویه تا اکتبر سال 2014 روی بیش از هفت میلیون برنامه موبایل تحت سیستم‌عامل‌های آندروید و iOS انجام داده، نزدیک به 96 درصد از بدافزارها یا نرم‌افزارهای مخرب توسط هکرها برای حمله به آندروید گوگل مورد استفاده قرار می‌گیرند. محققان دریافته‌اند که این نرم‌افزارها به گونه‌ای طراحی شده‌اند که برای سرقت داده‌های محبوب که عمدتا داده‌های مالی هستند، مورد استفاده قرار می‌گیرند. طبیعت منبع‌باز بودن آندروید به هکرها این امکان را می‌دهد تا به کدهایی که در پس‌زمینه یک نرم‌افزار محبوب قرار دارد، دسترسی پیدا کرده و برنامه را از نو با ظاهری تقریبا یکسان اما با کدهای مخرب که کاربران را آلوده می‌سازد ایجاد کنند.

جیسون استیر، مدیر فن‌آوری استراتژیک FireEye به CNBC می‌گوید: «شما می‌توانید همه این کدها را دریافت کرده و سپس دستورالعمل‌های اضافی را درون آن‌ها وارد کنید. در حالی‌که به نظر برسد که برنامه، همان برنامه اصلی بوده و هیچ راهی برای مصرف‌کننده برای تشخیص برنامه اصلی زمانی که آن‌را دانلود می‌کند وجود ندارد.» گوگل هنوز در این باره اظهارنظری نکرده است. مطابق بررسی‌های انجام شده، بدافزارهایی که هدف نهایی آن‌ها سیستم‌عامل گوگل است از 240 هزار نمونه به دست آمده در سال 2013 به 390 هزار نمونه در سه ماه نخست سال 2014 افزایش پیدا کرده‌اند.

FireEye می‌گوید: «یکی از بزرگ‌ترین آسیب‌پذیری‌های آندروید در روشی است که برنامه‌های‌همراه از آن برای برقراری ارتباط و ارسال مجدد اطلاعات به سرور استفاده می‌کنند.» FireEye کشف کرده است که بیشتر این ارتباطات به صورت غیررمزنگاری شده بوده که همین موضوع به هکرها اجازه می‌دهد که آن‌ها را جدا کرده و کدهای مخرب که می‌تواند کاربران را آلوده سازد در آن‌ها اضافه کنند. تبلیغات نیز بعضی از کاربران را در معرض خطر قرار می‌دهد. بیشتر برنامه‌ها از نرم‌افزارهای تبلیغی ثالث برای نمایش تبلیغات و کسب درآمد از کاربران استفاده می‌کنند. اما استیر می‌گوید: «این نوع جمع‌آوری داده‌ها اغلب تجاوزکارانه است» و هشدار می‌دهد که اغلب نرم‌افزارها این داده‌ها را به شیوه غیرایمن انتقال می‌دهند که همین موضوع داده‌ها را به راحتی در اختیار هکرها قرار می‌دهد.

آسیب‌پذیری‌های iOS

تنها برنامه‌های آندروید نیستند که آسیب‌پذیر هستند.آسیب‌پذیری در برنامه‌های روی دستگاه‌های iOS که به نظر می‌رسید خیلی امن است، نیز شناسایی شده است. در گذشته، هکرها فقط می‌توانستند به دستگاه‌های قفل‌شکسته

iOS با برنامه‌های مخرب نفوذ کنند. دستگاه‌های قفل‌شکنی شده به کاربران اجازه می‌دهد به نصب برنامه‌هایی اقدام کنند که از طریق فروشگاه برنامه‌های اپل دریافت نشده‌اند. اکنون محققان FireEye می‌گویند هکرها توانایی ساخت بدافزارهایی را دارند که می‌تواند دستگاه‌های قفل‌شکنی نشده را مورد حمله قرار دهند. اپل هنوز در این باره واکنشی نشان نداده است. هکرهای فرصت‌طلب در حال بررسی فرآیند تصدیق هویت برنامه‌های اپل هستند.
توسعه‌دهندگان اپل به طور معمول ساخت و آزمایش یک برنامه را در وضعیت بتا روی برنامه توسعه سازمانی اپل انجام می‌دهند. این آزمایش‌های دقیق اپل برای امنیت بیشتر قبل از آن‌که برنامه به فروشگاه اپل منتقل شود انجام می‌شود. اما هکرها اکنون در حال ساخت برنامه‌هایی به این شکل و سپس ارسال این برنامه‌ها برای مردم از طریق پیام‌های متنی یا ایمیل در قالب یک لینک هستند. زمانی‌که کاربر روی لینک کلیک می‌کند برنامه مخرب روی دستگاه او دانلود می‌شود. استیر می‌گوید: «به دلیل این‌که دستگاه‌های اپل بسیار محبوب هستند، هکرها آن‌ها را هدف‌های ارزشمندی می‌بینند.»

منبع:

سی‌ان‌بی‌سی

تاریخ انتشار:
11 اسفند 1393

نشانی منبع: https://www.shabakeh-mag.com/news/world/339