سرقت اطلاعات ۲۲۵ هزار کاربر توسط بدافزار ساخته شده برای دستگاه های جیلبریک شده مبتنی بر iOS - دیجیاتو

مریم موسوی | سه شنبه، ۱۰ شهریور ۱۳۹۴

حتما تا به حال در مورد خطرات امنیتی جیلبریک کردن دستگاه های آیفون مطالب متعددی را شنیده اید. اما آیا از خود سوال کرده اید که این کار چرا خطرناک است؟ دو شرکت Palo Alto Network و WeipTech اعلام کرده اند که توانسته اند 92 نمونه ی خانواده جدیدی از یک بدافزار iOS را شناسایی نمایند.

این بدافزار که تحت عنوان KeyRaider از آن یاد گردیده دستگاه های جیلبریک شده مبتنی بر iOS را با استفاده از اپلیکیشن سیدیا هدف حمله قرار داده و اطلاعات مربوط به اکانت اپل کاربران آنها را به سرقت می برد.

طبق آمارهای ارائه شده، این دستگاه تا به حال دست کم 225000 اپل آی دی و پسورد را از کاربران دستگاه های جیلبریک شده در بیش از 18 کشور دنیا به سرقت برده است.

در ادامه این مطلب با دیجیاتو همراه باشید.

آنطور که شرکت Palo Alto Network گفته بدافزار یاد شده از طریق سیدیا فرایندهای در حال اجرا روی سیستم را به دام انداخته و با رهگیری ترافیک آیتونز، نام کاربری اکانت اپل و پسوردها و شماره سریال دستگاه را به سرقت می برد.

به گفته کلاود ژیائو KeyRaider مجوزهای سرویس اعلان های اپل و همچنین گذرواژه های خصوصی را سرقت کرده و اطلاعات خرید کاربران از اپ استور را به اشتراک عمومی می گذارد. این بدافزار همچنین قادر است که کارکردهای قفل گشایی بومی و همچنین از راه دور دستگاه های آیفون و آیپد را از کار بیاندازد.

این نرم افزار مخرب پس از سرقت داده های یاد شده آنها را روی سرور خود آپلود می کند. اما خبر خوب این است که KeyRaider تنها آیفون های جیلبریک شده را هدف حمله خود قرار می دهد.

زمانی که حرف از بدافزار در دستگاه های موبایل به میان می آید بسیاری تصور می کنند که منظور

تلفن های همراه اندرویدی هستند که این مساله هم از ماهیت عملکردی این سیستم عامل و همچنین طریقه نصب اپلیکیشن های شخص ثالث روی آن نشات می گیرد؛ این یعنی کاربران می توانند بدافزارها را با سرعت و سهولت بیشتری نسبت به سایر پلتفرم ها روی اندروید توزیع و نصب کنند.

نحوه سندباکس شدن اپلیکیشن های iOS و همچنین فرایند تایید آنها در اپ استور بدان معناست که امکان توزیع شدن بدافزار روی iOS استاندارد وجود ندارد.

اما زمانی که کاربری دستگاه خود را جیلبریک می کند می تواند اپلیکیشن هایی غیر از موارد تایید شده توسط اپل را روی آن نصب نماید و همین مساله سیستم عامل دستگاه را آسیب پذیر می کند.

KeyRaider از طریق اپلیکیشن هایی پخش شد که در فهرست سیدیا موجود بودند؛ نوعی اپ استور برای آیفون های جیلبریک شده که به کاربران امکان می دهد اپلیکیشن های پولی را دانلود کرده و بدون آنکه هزینه ای بپردازند از داخل آن اپ ها خریدهای مختلف را انجام دهند.

این مساله می تواند هشدار دیگری باشد مبنی بر خطرناک بودن جیلبریک و چنانچه توجه کافی را به اپ های نصب شده نداشته باشید، خطر بیشتر هم می شود.

ناگفته نماند که جیلبریک نقش بسیار مهمی در توسعه اولیه آیفون داشت؛ پیش از آنکه اپل نخستین نسخه از کیت توسعه نرم افزاری سیستم عامل اختصاصی اش را در سال 2008 معرفی نماید، این تنها راهی بود که توسعه دهندگان می توانستند اپلیکیشن هایی کامل و قابل اعتماد برای آیفون بسازند.

و البته این هم درست است که گفته می شود بخش اعظمی از قابلیت های مفید iOS نظیر کیبوردهای شخص ثالث، امکان پاسخگویی به اعلان پیام های متنی در اپلیکیشن های دیگر و حتی فولدرهای ویژه اپلیکیشن ها نخستین بار در جامعه جیلبریک ابداع شدند.

اما دیگر از سال 2007 و 2012 زمان زیادی گذشته و با تبدیل شدن دستگاه های موبایل به پلتفرم اولیه کاربران برای انجام امور محاسباتی، دست های آلوده بیشتری چشم به این پلتفرم دوخته و قصد خرابکاری در آن را دارند. به بیان دیگر جیلبریک کردن آیفون روشی بسیار خوب برای افزایش تهدیدات علیه اطلاعاتی است که در داخل آن نگهداری می شوند.

دیجیاتو