225 هزار حساب کاربری اپل در معرض تهدید

آی‌فون‌های قفل شکسته در خطر هک شدن قرار گرفته‌اند

شکستن قفل دستگاه‌ها همیشه یک مزیت نیست و در بعضی موارد دردسرهای جدی را برای دارندگان این دستگاه‌ها به وجود می‌آورد. به لطف آی‌فون‌های قفل شکسته، بزرگ‌ترین سرقت حساب‌های کاربری اپل در انتظار دارندگان iOS قرار دارد. به تازگی این سیستم‌عامل هدف بدافزاری قرار گرفته است که روی دستگاه‌های قفل شکسته متمرکز شده است. این بدافزار باعث شده است تا حساب کاربری نزدیک به 225 هزار کاربر اپل در معرض افشا، سرقت و تهدید جدی قرار گیرد.

گوشی‌های قفل شکسته یک‌بار دیگر پیامدهای جدی را برای دارندگان آی‌فون به وجود آورده است. به تازگی بدافزاری منتشر شده است که نزدیک به 225 هزار حساب اپلی را در معرض سرقت قرار داده که در نوع خود سرقت بزرگی به شمار می‌رود. این بدافزار تنها روی دستگاه‌های قفل شکسته تأثیرگذار است، این دستگاه‌های قفل شکسته به هکرها این توانایی را می‌دهد تا از گذرواژه کاربران استفاده کرده و بدون آن‌که نیازی به دریافت مجوز از سوی کاربر داشته باشند اقدام به خرید از فروشگاه اپل کنند.

تیم تحقیقاتی Palo Alto این بدافزار وحشتناک iOS را KeyRaider نام نهاده است. این بدافزار از طریق برنامه محبوب Cydia کار می‌کند که دانلود و مدیریت برنامه‌های کاربردی روی آیفون‌های قفل شکسته را به سادگی امکان‌پذیر می‌سازد. هر زمان یک کاربر شناسایی شود، بدافزار شروع به سرقت ترافیک آی‌تونز و سرقت انواع مختلفی از داده‌ها می‌کند. بنابر گزارش شبکه Palo Alto بدافزار KeyRaider توانایی سرقت گواهی سرویس اعلان اپل و کلیدهای خصوصی را داشته و همچنین توانایی سرقت و به اشتراک‌گذاری اطلاعات مربوط به خرید از فروشگاه اپل و غیر فعال کردن ویژگی‌های آی‌فون و آی‌پاد را به صورت محلی یا از راه دور دارد.

اولین بار Wired App Store رفتار عجیب و غریبی را در این ارتباط شناسایی کرد. بعد از آن‌که گزارش‌های مختلفی از خریدهای تصدیق هویت نشده از فروشگاه اپل اعلام شد، دانشجوی دانشگاه Yangzhou در چین گوشی‌های قفل شکسته را مورد بررسی قرار داد و متوجه شد کاربرانی تحت تأثیر این حمله قرار گرفته‌اند که نرم‌افزار مذکور را نصب کرده‌اند و اعلام کرد این برنامه اقدام به آپلود داده‌های کاربران در یک بانک‌اطلاعاتی نامعلوم می‌کند. بعد از بررسی‌های دقیق‌تر معلوم شد، گذرواژه و دیگر اطلاعات هویتی نزدیک به 250 هزار کاربر اپل اکنون در این بانک‌اطلاعاتی ثبت شده است.

[illegible] [illegible]: [illegible]!

بررسی‌های بیشتر Palo Alto Networks نشان داد، ترفندی برای کمک به کاربران اپل مورد استفاده قرار می‌گیرد، تا کاربران بتوانند برنامه‌های غیر رایگان را بدون آن‌که هزینه‌ای بابت دانلود آن‌ها پرداخت کنند از فروشگاه اپل دریافت کنند. اما اوضاع زمانی بدتر می‌شود که بدانید هکرها نه تنها می‌توانند با استفاده از حساب‌های کاربری مشکوک اقدام به خرید از فروشگاه اپل کنند، بلکه آن‌ها این توانایی را دارند تا از راه دور اقدام به قفل گوشی‌های کاربران کرده و در مقابل آزادسازی گوشی مبلغی را از کاربر مطالبه کنند. Palo alto Network در این خصوص می‌گوید: « آن‌ها می‌تواند به‌طور محلی هر نوع عملیات باز کردن قفل یا تصحیح گذرواژه یا کد عبوری که وارد می‌شود را غیرفعال کنند. آن‌ها همچنین، این توانایی را دارند تا به‌طور مستقیم یک پیغام باج خواهی را با استفاده از گواهی و کلید خصوصی به سرقت رفته برای کاربر ارسال کنند. این پیغام به‌گونه‌ای ارسال می‌شود که ترافیک خاصی را روی سرور اپل بوجود نیاورد.»

منبع:

gizmodo.co.uk

تاریخ انتشار:
13 شهریور 1394

نشانی منبع: https://www.shabakeh-mag.com/security/1444