هک آیفون ده‌ها کارمند شبکه الجزیره از طریق یک آسیب‌پذیری روز صفر - دیجیاتو

محمد قریشی | دوشنبه، ۰۱ دی ۱۳۹۹

یک گروه از محققان از هک آیفون حداقل ۳۶ خبرنگار، تهیه‌کننده، مجری و مدیر اجرایی خبرگزاری «الجزیره» به همراه یک خبرنگار شبکه «العربی» به وسیله یک آسیب‌پذیری روز صفر بدون نیاز به تعامل کاربر در اپ iMessages سیستم عامل iOS خبر داده است.

طبق گفته گروه حقوق بشر و امنیت سایبری «Citizen Lab» در دانشگاه «تورنتو»، این آسیب‌پذیری روز صفر به عنوان بخشی از اکسپلویت «Kismet» شناخته می‌شود که توسط شرکت «NSO Group» تولید و فروخته شده. این کمپانی در زمینه تولید جاسوس افزار و محصولات نظارتی نامی شناخته شده است.

محققان ادعا می‌کنند که NSO این ابزار هک را حداقل به چهار فرد یا سازمان فروخته که برای حمله سایبری به آیفون شخصی ۳۶ کارمند الجزیره در ماه‌های ژوئیه و آگوست ۲۰۲۰ استفاده شده. Citizen Lab توانسته دو خریدار را شناسایی کند که در عربستان سعودی و امارات متحده عربی قرار دارند. ظاهرا این فعالیت‌ها مربوط به گروه‌های «Monarchy» و «Sneaky Kestrel» می‌شود.

Citizen Lab با تحقیقات بیشتر به این موضوع پی برده که این حملات حداقل از اکتبر ۲۰۱۹ در جریان است. ابزار اکسپلویت Kismet روی گوشی‌های جدید اپل هم کارایی دارد که برای مثال می‌توان به آیفون ۱۱ با سیستم عامل iOS 13.5.1 اشاره کرد. با وجود این موضوع، این آسیب‌پذیری پس از ارائه سیستم عامل iOS 14 دیگر کارایی ندارد.

محققان این مشکل امنیتی را به اپل گزارش کرده‌اند و این کمپانی در حال تحقیق درباره این گزارش است.

سخنگوی NSO گزارش اخیر را حدس و گمان اعلام کرده و آن را فاقد هرگونه مدرکی مبنی بر استفاده از ابزار NSO دانسته است. این کمپانی به فروش ابزارهای نظارتی به آژانس‌های قانونی اشاره کرده و گفته نمی‌تواند نحوه استفاده مشتریان از این ابزارها را تشخیص دهد.

Citizen Lab تا به امروز گزارش‌های زیادی منتشر و در آن‌ها ادعا کرده که ابزارهای هک NSO توسط سازمان‌های مختلفی برای ردیابی رقبای سیاسی، خبرنگاران و فعالان در کشورهایی مانند مراکش، مکزیک، عربستان سعودی و امارات متحده عربی مورد استفاده قرار گرفته است.

دیجیاتو