بتقنيات إسرائيلية.. كشف فضيحة تجسس جديدة للنظام السعودي

التغيير

كشفت صحيفة بريطانية تفاصيل فضيحة تجسس جديدة لنظام آل سعود عبر ملاحقة ناشط معارض يقيم في الخارج بتقنيات إسرائيلية.

وقالت صحيفة Times NewYork إن برامج تجسس شركة Group NSO الإسرائيلية تكرر اختراق جهاز الـ iPhone الخاص بناشط من المملكة، مما يجعل شركة Apple تصدر تحديثات برامج طارئة الثغرة الأمنية والخلل في النظام.

ونقلت الصحيفة عن مجموعة سيتزن لاب لمراقبة أمن الإنترنت، قولها إن شركة متخصصة في مراقبة الإنترنت مقرها إسرائيل طورت أداة من أجل اختراق أجهزة آيفون التي تنتجها آبل بتقنية غير مسبوقة تُستخدم

منذ فبراير/شباط على أقرب تقدير.

تأتي أهمية الاكتشاف من خطورة طبيعة الثغرة التي لا تتطلب أي تفاعل من المستخدِم وتؤثر على جميع نسخ آي.أو.إس وأو.إس.إكس ووتش أو.إس في أجهزة آبل باستثناء تلك المحدَّثة يوم الإثنين.

الشركة الإسرائيلية المتهمة باختراق أجهزة آيفون هي ذاتها التي طورت برنامج بيغاسوس للتجسس، الذي باعته لمجموعة من الحكومات العربية بينها المملكة والتي استخدمته لاختراق هواتف المعارضين وبعض الشخصيات المهمة.

والثغرة التي طورتها الشركة الإسرائيلية (إن.إس.أو جروب) تتغلب على أنظمة الأمان التي صممتها آبل في السنوات الأخيرة.

وقالت آبل إنها أصلحت الثغرة في تحديث أجرته الإثنين لنظام التشغيل، وهو ما يؤكد اكتشاف سيتزن لاب.

إذ قال إيفان كرستيتش، رئيس الهندسة الأمنية بآبل، في بيان: "بعد تحديد الثغرة التي يستخدمها هذا الهجوم على آي.مسيدج، طورت آبل بسرعة إصلاحاً لآي.أو.أس 14.8 لحماية مستخدمينا".

وأضاف: "مثل هذه الهجمات معقدة للغاية، ويتكلف تطويرها ملايين الدولارات، وغالباً ما تكون لها مدة صلاحية قصيرة، وتستخدم لاستهداف أفراد معينين".

ومضى قائلاً: "رغم أن هذا لا يعني أنها تشكل تهديداً للغالبية العظمى من مستخدمينا، فإننا نواصل العمل بلا هوادة لحماية جميع عملائنا، ونضيف باستمرار وسائل حماية جديدة لأجهزتهم وبياناتهم".

فيما رفض متحدث باسم آبل التعليق على ما إذا كانت تقنية اختراق أجهزة آيفون أتت من "إن.إس.أو جروب".

في بيان لها لم تؤكد "إن.إس.أو" أو تنفِ أنها كانت وراء هذه التقنية، واكتفت بقول إنها سوف "تستمر في تزويد وكالات الاستخبارات وإنفاذ القانون حول العالم بتقنيات إنقاذ لمكافحة الإرهاب والجريمة".

إذ قالت سيتزن لاب إنها عثرت على هذا النوع من البرمجيات الضارة على هاتف ناشط من المملكة لم تذكر اسمه، وإن الهاتف تم اختراقه باستخدام برامج تجسس في فبراير/شباط. وعدد المستخدمين الآخرين الذين ربما يكونون قد تضرروا به غير معروف.

كما أوضحت أنه لا يتطلب نجاح اختراق أجهزة آيفون أي نقرة من الضحية المستهدفة. وقال باحثون إنهم لا يعتقدون في وجود أي مؤشر مرئي على حدوث اختراق.

تكمن الثغرة في كيفية الاستخلاص التلقائي للصور في تطبيق آبل للرسائل (آي.مسيدج). واستهدفت "إن.إس.أو" وغيرها من المتعاملين في برمجيات الهجوم الإلكتروني تطبيق آي.مسيدج مراراً، وهو ما دفع آبل لتحديث بنيته. لكن هذا لم يوفر حماية كاملة للنظام.

نفس الشركة الإسرائيلية كانت وراء تسويق برنامج بيغاسوس Pegasus وهو برنامج اختراق -أو برنامج تجسس- طورته شركة Group NSO الإسرائيلية وتسوقه لحكومات دول العالم. ولديه القدرة على اختراق مليارات الهواتف التي تعمل بأنظمة تشغيل iOS أو أندرويد.

كانت أقدم نسخة مكتشفة من بيغاسوس حصل عليها باحثون عام 2016، تخترق الهواتف من خلال ما يسمى التصيد الاحتيالي، أي الرسائل النصية أو رسائل البريد الإلكتروني التي تدفع الهدف للنقر على رابط اختراق.

لكن بعدها، ازدادت قدرات برنامج بيغاسوس تقدماً. وأصبح بإمكانه الوصول إلى أهدافه عن طريق ما يسمى الهجمات "الخالية من النقر" click-zero، التي لا تتطلب أي تفاعل من مالك الهاتف ليتمكن من اختراقه.

غالباً ما تستغل هذه الهجمات ثغرات "الهجمات دون انتظار" day zero، وهي عيوب أو أخطاء في نظام التشغيل لا تكون الشركة المصنعة للهاتف المحمول قد اكتشفتها، وبالتالي لا تتمكن من إصلاحها.

وعام 2019، كشفت شركة واتساب أن برنامج بيغاسوس اُستخدم لإرسال برامج اختراق إلى أكثر من 1400 هاتف عن طريق استغلال ثغرة الهجمات دون انتظار.

ذلك ببساطة عن طريق إجراء مكالمة واتساب للجهاز المستهدف تُمكِّن برنامج بيغاسوس من تثبيت رمز

خبيث على الهاتف، حتى لو لم يرد الهدف على المكالمة مطلقاً.

في الآونة الأخيرة، بدأت NSO في استغلال الثغرات الأمنية في برنامج iMessage المثبّت على هواتف آبل، وهو ما مكّنها من اختراق مئات الملايين من أجهزة آيفون. وتقول شركة آبل إنها تحدّث برامجها باستمرار لمنع هذه الهجمات.