فضحة تجسس سعودية كشفت أكبر قضية قرصنة في العالم

أظهر تحقيق لوكالة رويترز العالمية للأنباء أن فضيحة تجسس سعودية استهدفت الناشطة الحقوقية لجين الهذلول كانت السبب المباشر في كشف أكبر قضية تجسس وقرصنة في العالم.

وذكرت الوكالة أن ما تعرضت له الهذلول ساهم في قلب الأمور ضد شركة "إن إس أو غروب" (Group NSO) الإسرائيلية، إحدى شركات برامج التجسس الأكثر تطورا في العالم.

وتواجه الشركة الإسرائيلية الآن سلسلة من الإجراءات القانونية والتدقيق في واشنطن بسبب مزاعم جديدة باستخدام برامجها لاختراق المسؤولين الحكوميين والمعارضين في جميع أنحاء العالم.

وقد بدأ كل شيء بخلل في برنامج التشغيل على جهاز "آيفون" الخاص بالهذلول بأوامر من ولي العهد محمد بن سلمان.

إذ أتاح خطأ خارج عن المألوف في برامج التجسس الخاصة بـ "إن إس أو" للناشطة السعودية في مجال

حقوق المرأة، لجين الهذلول، والباحثين في مجال الخصوصية لاكتشاف مجموعة من الأدلة التي تشير إلى أن مصنّعة برامج التجسس الإسرائيلية ساهمت في اختراق هاتف الناشطة الذكي، وفقا لما ذكره ستة أشخاص على علم بالواقعة لوكالة رويترز.

وأشاروا إلى أن ملف صور مزيف غامض داخل هاتف الهذلول، تركه برنامج التجسس عن طريق الخطأ، أثار انتباه باحثي الأمن الإلكتروني.

واشتهرت الهذلول بدعمها حملة لإنهاء الحظر المفروض على قيادة النساء للسيارات في السعودية. وأطلق سراحها من السجن بعد إدانتها بتهمة الإضرار بالأمن القومي، في فبراير 2021.

وبعد فترة وجيزة من إطلاق سراحها من السجن، تلقت الهذلول بريدا إلكترونيا من "غوغل" يحذرها من أن المتسللين المدعومين من الدولة حاولوا اختراق حساب البريد الإلكتروني الخاص بها "Gmail".

وقال ثلاثة أشخاص مقربين من الهذلول إنها وخوفا من اختراق هاتفها، اتصلت بمجموعة "سيتيزن لاب" الكندية الناشطة في حقوق الخصوصية وطلبت منهم التحقق من جهازها للحصول على أدلة.

وبعد ستة أشهر من البحث في سجلات هاتفها، قام الباحث في "سيتيزن لاب"، زبيل ماركزاك، بما وصفه بـ "اكتشاف غير مسبوق"، تمثل بالعثور على خلل في برنامج المراقبة المزروع على هاتف الهذلول ترك نسخة من ملف الصورة الخبيثة، بدلاً من حذف نفسه تلقائيا، بعد سرقة رسائل الناشطة المستهدفة.

وأكد الباحث أنهم كشفوا عن الشيفرة التي خلفها الهجوم، والتي تضمنت دليلا مباشرا على أن "أن إس أو" أنشأت أداة التجسس.

ويقول ماركزاك: "لقد غيرت قواعد اللعبة، اكتشفنا شيئا اعتقدت الشركة أنه لا يمكن الوصول إليه".

وكان الاكتشاف بمثابة مخطط كامل لعملية القرصنة، ما دفع شركة "آبل" لإخطار الآلاف من ضحايا القرصنة في جميع أنحاء العالم، وفقا لأربعة أشخاص على دراية مباشرة بالحادث.

قدمت النتائج التي كشفها "سيتيزن لاب" والهذلول الأساس للدعوى القضائية، التي رفعتها "آبل" في نوفمبر 2021 ضد "إن إس أو"، كما تردد صداها في واشنطن، حيث علم المسؤولون الأميركيون أن سلاح

الشركة الإسرائيلية الإلكتروني استُخدم في التجسس على الدبلوماسيين الأميركيين أيضا.

وفي السنوات الأخيرة، تمتعت صناعة برامج التجسس بنمو هائل، حيث تشتري الحكومات في جميع أنحاء العالم برامج قرصنة الهاتف التي تسمح بهذا النوع من المراقبة الرقمية والتي كانت في السابق من اختصاص عدد قليل من وكالات الاستخبارات النخبوية.

وخلال العام الماضي، ربطت سلسلة من المعلومات، التي كشف عنها عدد من الصحفيين والنشطاء، بما في ذلك مشروع "بيغاسوس" للتعاون الصحفي الدولي، صناعة برامج التجسس بانتهاكات حقوق الإنسان، مما أدى إلى مزيد من التدقيق في "إن إس أو" ونظرائها.

لكن باحثين أمنيين يقولون إن اكتشاف الهذلول كان أول من قدم مخططا لشكل جديد قوي من التجسس الإلكتروني، تمثل بأداة اختراق تتسلل إلى الأجهزة دون أي تفاعل من المستخدم (أي دون الحاجة إلى الضغط على رابط لتحميل برنامج خبيث مثلا)، وأنه يعد أكثر الأدلة الملموسة حتى الآن على قدرات السلاح الإلكتروني.

وقد كان لدى الهذلول سبب وجيه للشك، فتلك لم تكن هذه هي المرة الأولى التي تتم فيها مراقبتها.

إذ كشف تحقيق أجرته رويترز، في عام 2019، أنه تم استهدافها، في عام 2017، من قبل فريق من المرتزقة الأميركيين الذين قاموا بمراقبة المعارضين نيابة عن الإمارات العربية المتحدة في إطار برنامج سري يسمى "مشروع الغراب الأسود" (Raven Project)، والذي صنفها على أنها "تهديد للأمن القومي" واخترق هاتفها "الآيفون".

واعتقلت الهذلول في السعودية وسجنت لمدة ثلاث سنوات تقريبا، حيث تقول عائلتها إنها تعرضت للتعذيب والاستجواب باستخدام المعلومات المسروقة من جهازها.

وأطلق سراح الهذلول في فبراير 2021 وهي ممنوعة حاليا من مغادرة البلاد.

وقالت شقيقتها، لينا الهذلول، إن تجربة الناشطة في المراقبة والسجن جعلتها مصممة على جمع الأدلة التي يمكن استخدامها ضد من يستخدم هذه الأدوات، مضيفة "إنها تشعر أنها تتحمل مسؤولية مواصلة هذا القتال، لأنها تعلم أنها تستطيع تغيير مجريات الأمور".

ويُعرف نوع برنامج التجسس"سيتيزن لاب" الذي تم اكتشافه على هاتف "آيفون" الخاص بالهذلول باسم (zero click) ، مما يعني أنه يمكن إصابة المستخدم دون النقر فوق أي رابط ضار.

وعادة ما تحذف البرامج الضارة التي تعمل بنقرة صفرية نفسها تلقائيا عند اختراق المستخدم، تاركة الباحثين وشركات التكنولوجيا دون عينة من السلاح الإلكتروني لدراسته.

ويقول باحثون أمنيون إن ذلك يمكن أن يجعل جمع أدلة دامغة على عمليات اختراق "آيفون" عملية شبه مستحيلة.

ولكن هذه المرة كان الأمر مختلفا. فخلل في برنامج التشغيل ترك نسخة من برنامج التجسس مخبأة على هاتف الهذلول ، مما سمح لماركزاك وفريقه بالحصول على مخطط افتراضي للهجوم ودليل على من قام ببنائه.

قال: "لدينا هنا غلاف الرصاصة من مسرح الجريمة".

اكتشف ماركزاك وفريقه أن برنامج التجسس يعمل، بشكل جزئي، عن طريق إرسال ملفات صور إلى الهذلول عبر رسالة نصية غير مرئية.

وخدعت ملفات الصور جهاز "الآيفون" لإتاحة الوصول إلى ذاكرته بالكامل، وتجاوز الحواجز الأمنية والسماح بتثبيت برامج التجسس التي من شأنها سرقة رسائل المستخدم.

وقال ماركزاك، الذي أكد تحليله باحثون من منظمة العفو الدولية وشركة آبل، إن اكتشاف "سيتيزن لاب" قدم دليلاً قوياً على أن "إن إس أو" صنعت السلاح الإلكتروني.

وأشار ماركزاك إلى أن برنامج التجسس الذي تم العثور عليه على جهاز الهذلول يحتوي على رمز يظهر علاقته بخوادم كان "سيتيزن لاب" قد ربطها سابقا بشركة "إن إس أو".

وأطلق "سيتيزن لاب" تسمية "الاختراق القسري" (ForcedEntry) على عملية الاختراق الجديدة. ثم قدم الباحثون العينة لشركة "آبل" في سبتمبر الماضي.

وساعد وجود مخطط للهجوم في متناول اليد شركة "آبل" على إصلاح الثغرة الأمنية الحرجة وقادها إلى إخطار الآلاف من مستخدمي "آيفون" الآخرين الذين استهدفهم برنامج "إن إس أو" ، محذرينهم من أنهم استهدفوا من قبل "المهاجمين الذين ترعاهم الدولة".

وكانت هذه هي المرة الأولى التي تتخذ فيها "آبل" هذه الخطوة.

وبينما قررت شركة "آبل" أن الغالبية العظمى كانت مستهدفة من خلال أداة "إن إس أو"، إلا أن باحثي الأمن اكتشفوا أيضا برنامج تجسس من شركة إسرائيلية ثانية مصنّعة لبرامج التجسس "QuaDream"، والتي استغلت برامجها ثغرة "آيفون" ذاتها، حسبما ذكرت رويترز في وقت سابق من هذا الشهر.