كيف تستخدم الحكومات تقنيات اختراق الهواتف لزرع برامج التجسس؟

ترجمة وتحرير: نون بوست

يقول عدد من الباحثين أنه فيما تعمل شركات التكنولوجيا والخبراء على تعزيز حماية الهواتف ضد برامج التجسس الحكومية، تستخدم الحكومات القمعية منتجًا يتم تسويقه على نطاق واسع داخل وكالات إنفاذ القانون الأمريكية، ويضمن الوصول إلى الأجهزة وزرع برامج المراقبة.

كشفت تقارير حديثة عن ممارسات من هذا القبيل في روسيا والصين. وتحدثت منظمة العفو الدولية عن سلسلة من الحوادث المماثلة في صربيا؛ حيث اكتشف نشطاء وصحفيون أنه تم اختراق هواتفهم بعد أن احتكوا بالشرطة، وغالبًا دون أن يتم اعتقالهم أو توجيه أي تهم.

في إحدى الحالات، أوقفت شرطة المرور الصحفي سلافيسا ميلانوف بالقرب من مدينة بَيروت جنوب شرق صربيا في وقت سابق من هذه السنة، وتم اقتياده إلى مركز شرطة بزعم إجراء اختبارات للكحول والمخدرات، وقد اجتازها. طُلب منه ترك متعلقاته، بما في ذلك هاتفه، خارج الغرفة التي تم استجوابه فيها، واستعادها بعد ساعتين ونصف عندما تم الإفراج عنه، وفقًا لمنظمة العفو الدولية. بعد أن لاحظ ميلانوف أن بعض الإعدادات في الهاتف قد تم تغييرها، استخدم تطبيقًا أمنيًا ليكتشف أنه تم تثبيت برامج جديدة.

وقال ميلانوف لصحيفة "واشنطن بوست" إن السلطات المحلية كانت منزعجة من مقالاته التي تناولت إنفاق الأموال العامة على السيارات الفاخرة ومنح مشاريع البناء للمقاولين المتنفذين، مضيفًا: "لقد أوقفنا المحتوى النقدي مؤقتًا" بسبب عملية الاختراق.

وجدت منظمة العفو الدولية من خلال تحقيقاتها ثلاثة أنواع من برامج التجسس تم تثبيتها على أجهزة ميلانوف وآخرين في صربيا ممن ساورتهم الشكوك بعد ظهور إشعارات غريبة على هواتفهم.

كما وجدت المنظمة أدلة على أن بعض الهواتف قد تم فتحها في البداية باستخدام برامج من شركة "سيلبرايت"، وهي شركة مقرها إسرائيل، تبيع برامجها لأقسام الشرطة والسلطات في الولايات المتحدة

والعديد من البلدان الأخرى.

في الولايات المتحدة، يمكن لسلطات إنفاذ القانون التي لديها مذكرات تفتيش أن تستخدم مثل هذه البرامج لاستخراج المعلومات من الأجهزة بشكل قانوني، بما في ذلك هواتف كبار المجرمين.

نددت منظمة العفو الدولية – وهي واحدة من بين قلة من المنظمات غير الربحية التي تقود حملات ضد صانعي برامج التجسس، بما في ذلك شركة "إن إس أو" التي تنتج برنامج بيغاسوس سيئ السمعة – بسوء استخدام ما يُعرف ببرامج التحقيق الجنائي، قائلةً إنها "قد تصبح عوامل تمكين للقمع الرقمي، ومن المحتمل أن يتم استخدامها في دول وسياقات أخرى، وهو ما قد يكون حدث بالفعل".

فرضت الولايات المتحدة في السنوات القليلة الماضية عقوبات على عدة شركات تصنع برامج التجسس، معلنةً أنها تهدد الأمن القومي، وذلك بعد استخدامها ضد بعض الدبلوماسيين الأمريكيين وشخصيات أخرى. يهدف تقرير منظمة العفو الدولية إلى توثيق القضية ذاتها لكن من منظور مختلف.

وقالت المنظمة: "بينما أعرب النشطاء منذ فترة طويلة عن مخاوفهم بشأن التعرض لبرامج التجسس أثناء الاستجوابات مع الشرطة، فإن منظمة العفو الدولية تعتقد أن هذا التقرير يوثق لأول مرة عمليات الاختراق ببرامج التجسس للهواتف المحمولة من خلال تقنية التحقيق الجنائي من شركة سيلبرايت".

وقال ديفيد جي، رئيس قسم التسويق في "سيلبرايت"، لصحيفة "واشنطن بوست" إنه سيكون "صادمًا ومخيبًا للآمال" إذا ما كشفت منظمة العفو الدولية عن الحالات بدقة، وأضاف أن الشركة تحقق فيما إذا كانت صربيا قد انتهكت البند الخاص في اتفاقية الترخيص الذي يدعو إلى الاستخدام القانوني لتلك البرامج. وأوضح جي أن الشركة قد تستخدم تحديثًا برمجيًا لجعل أدوات التثبيت واستخراج البيانات الخاصة بها غير قابلة للتشغيل في صربيا.

وأضاف أن استخدام البرنامج يتم عادةً بعد الاعتقال، "ونحن نحقق في الأمر حاليًا"، موضحا أن الشركة قد انسحبت من دول أخرى في الماضي، بما في ذلك الصين وروسيا.

وأصدرت الشركة بيانا أكدت فيه أنها تلتزم بلائحة العقوبات الأمريكية والأممية، وكذلك لوائح الرقابة على الصادرات الإسرائيلية. بالإضافة إلى ذلك، قالت الشركة إنها منذ سنة 2020، "توقفت طواعيةً عن بيع برامجها للعملاء في أكثر من 60 دولة".

وقال جون سكوت-رايلتون من "سيتيزن لاب"، والذي نشر مؤخرا تقريرًا عن قيام السلطات الروسية بزرع برامج تجسس في هواتف مواطنيها، إن تقرير منظمة العفو الدولية يعد "خطوة مهمة في المسار الذي شهدناه في السنوات الأخيرة للمساءلة عن برامج التجسس".

وأضاف: "حصلت الشركات التي تنتج هذا النوع من برامج التصوير الجنائي على ما يشبه الضوء الأخضر، ويرجع ذلك جزئيًا إلى ارتباطها بتقنيات المراقبة التي يسمح بها القانون. لكن لم يعد من الممكن للشركات التي تصنع هذه التكنولوجيا أن تتصرف كما لو أنها لا تعلم بالانتهاكات".

وقالت منظمة العفو الدولية إن اختراق الهواتف حدث أثناء استجواب المستهدفين من قبل الشرطة أو وكالة المعلومات الأمنية الصربية المعروفة اختصارًا باسم "بي آي إيه". ولم تستجب الوكالة لطلب صحيفة "واشنطن بوست" للتعليق على هذه الادعاءات.

كما كشفت منظمة العفو الدولية عن أدلة على وجود ثغرات أمنية غير معروفة سابقًا في برنامج تشغيل أجهزة أندرويد للهواتف التي تعمل بشرائح كوالكوم، مما سمح لشركة سيلبرايت بالوصول إلى المزيد من مكونات الهواتف الداخلية. وأقرّت شركة غوغل المصنعة لنظام أندرويد بهذه الثغرة في تدوينة نشرتها يوم الاثنين، وقالت إنها أخطرت كوالكوم بذلك قبل أكثر من ثلاثة أشهر، وأضافت أنه لم يتم إصلاح هذه

الثغرات.

وكتب سيث جينكينز من غوغل: "نحن واثقون من أن هذا البرنامج التشغيلي يستغله مخترقون في العالم الحقيقي على نطاق واسع، وأن جميع الثغرات التي تمت معالجتها كجزء من هذا البحث كان لها تأثير كبير في منع استغلال تلك الثغرات في العالم الحقيقي".

إلى حد ما، فإن هذه التحولات في أساليب اختراق الهواتف تعدّ نتيجة لجهود "أبل" و"غوغل" في تحصين الأجهزة من عمليات القرصنة عن بُعد. وبعد أن بدأ الباحثون من منظمة العفو الدولية و"سيتيزن لاب" وغيرها من المنظمات في العثور على هواتف مخترقة وتحليل أساليب الاختراق، تم إطلاع "أبل" و"غوغل" على النتائج، وقد اكتشفت الشركتان المزيد من المشاكل وأغلقتا بعض الثغرات المستخدمة في عمليات التجسس. وقال ديفيد جي إن تلك الجهود جعلت عمل شركات مثل سيلبرايت أكثر صعوبة.

وإدراكًا منها أن السلطات في عدة دول لا تتوانى عن قرصنة الأجهزة، واصلت "آبل" تعزيز حماية هواتفها ضد التهديدات المحتملة. فأحدث إصدار من برنامج "آي أو إس" الخاص بها يقوم بإعادة التشغيل تلقائيًا إذا لم يتم فتح الهاتف لعدة أيام، وهو الوقت الذي قد يكون فيه الهاتف في مختبرات الشرطة. هذا يجعل الهاتف في حالة أكثر أمانًا، ويُعرف باسم "قبل فتح القفل الأول".

وكتب إيفان كريستيك، رئيس قسم هندسة الأمان في شركة "أبل": "تعمل فرق الأمان لدينا حول العالم بلا كلل لتتبع هذه التهديدات المتطورة، وتعزيز ميزات الأمان بشكل مستمر".

وقال العديد من الخبراء التقنيين في مجال إنفاذ القانون، والذين تحدثوا شريطة عدم الكشف عن هوياتهم، إن الشرطة في مختلف أنحاء الولايات المتحدة ليس لديها الفرصة والقدرة التقنية والسلطة القانونية لإصدار مذكرة تفتيش وتثبيت برنامج تجسس على جهاز أحد الموقوفين. وأوضحوا أن مكتب التحقيقات الفيدرالي لديه القدرة على ذلك، ولكن من غير المرجح تطبيق هذا الأسلوب على نطاق واسع. ولم تستجب الوكالة لطلب الصحيفة للتعليق على هذه المسألة.

ورغم أن استخدام برنامج سيلبرايت أو برامج مشابهة لاختراق الهواتف بعد صدور مذكرات تفتيش لا يعتبر أمرًا غير مألوف في الولايات المتحدة، يقول مسؤول سابق في مكتب التحقيقات الفيدرالي إنه لم يسمع قط عن تثبيت برامج تجسس بهذه الطريقة. وأضاف شريطة عدم الكشف عن هويته، قائلا إن الاستماع إلى المكالمات يتم بموجب أمر قضائي منفصل وبالتعاون مع شركات الاتصالات.

المصدر: واشنطن بوست

رابط المقال: https://www.noonpost.com/278505/