اختراق الهواتف.. جيل جديد من حروب ال سعود

عملية اختراق الهاتف المحمول لمالك موقع "أمازون" وصحيفة "واشنطن بوست"، "جيف بيزوس"، إثر تلقيه رسالة على "واتساب" من الحساب الشخصي لمحمد بن سلمان، تسلط الضوء على تطور برمجيات التجسس عبر اختراق الهواتف.

ويشارك مكتب التحقيقات الفيدرالي الأمريكي في التحقيقات المتعلقة بعملية الاختراق، التي أثارت جدلا صاخبا في أوساط الرأي العام الأمريكي والعالمي.

وتشهد الساحة التقنية، تطورات متسارعة بشكل جنوني، يتجاوز القوانين والتشريعات القائمة في هذا الإطار، بما يجعل الهواتف المحمولة تتحول إلى أداة تجسس خطيرة، مع ظهور تطبيقات أحدث وأكثر تعقيدا.

وفق التحقيقات الجارية، في اختراق هاتف مؤسس "أمازون" ومالك صحيفة "واشنطن بوست"، فإن اختراق الهاتف تم من خلال برنامج "واتساب" المثبت على هاتف "بيزوس" من نوع "أيفون إكس".

وتقول شركة "إف تي آي" للاستشارات الأمنية، إنه جرى تسريب كم هائل من المعلومات من هاتف "بيزوس" بعد تلقيه ملف فيديو من "بن سلمان" عبر "واتساب".

وتقوم البرمجيات الخبيثة المتقدمة عادة بتثبيت نفسها على نظام الملف الأصلي للجهاز، حتى لا تتم إزالتها وتجنب كشف أنظمة الأمان لها.

وربما تكشف قضية "بيزوس" عن جانب خفي من البرمجيات الخبيثة المعقدة، ذات القدرة على التحايل على تقنيات الرصد والأمان.

لعبة الإغراق

وتعمل الهواتف الذكية من خلال مجموعة تطبيقات يتم تنظيمها بواسطة نظام التشغيل الخاص بالهاتف، فضلا عن مستقبلات وعدسات وأجهزة استشعار.

ويمكن أن ينهار نظام التشغيل للهاتف، أو يتصرف على نحو غير متوقع عند استقبال رسالة خداعة، أو ملفات تحتوي على برامج خبيثة، لديها القدرة على التسلل والسيطرة الكاملة على الهاتف الذكي، وتحويله إلى جهاز مراقبة.

الخطير، أن تلك النوعية من الاختراقات، مع تطور برامجج التجسس، تتيح للجهة المنفذة لعملية الاختراق تتبع أماكن المستخدمين سرا، والحصول على نسخ من بريدهم الإلكتروني ورسائلهم الفورية وصورهم، ومكالماتهم الصوتية والمرئية.

يؤكد تلك المخاطر، نجاح شركة التجسس الإسرائيلية (NSO) خلال العام 2019، في اختراق هواتف مجموعة من الناشطين، والتسلل إلى هواتفهم ببساطة عن طريق إجراء مكالمة صوتية عن طريق "واتساب".

لكن التطور الجديد أن الاختراق صار يحدث حتى لو لم يستجب الهدف للمكالمة، بما يعني تثبيت البرامج الضارة على جهازه، وتنشيط كاميرات الأجهزة والميكروفونات لأخذ التسجيلات.

ويعمل هذا الهجوم من خلال طريقة تعرف باسم (الإغراق)، وتعني تجاوز سعة المخزن المؤقت للهاتف.

ولكل هاتف مخزن يحتوي على شفرات برمجية محفوظة بشكل آمن، لكن هذا المخزن في حالة امتلائه لا يقوم بالتوقف عن استقبال هذه الشفرات، بل يتم تخزينها في مكان آخر، وهي الثغرة التي توصلت إليها الشركة الإسرائيلية.

بيجاسوس

ويستخدم الهجوم، الذي طال موظفي منظمة العفو الدولية وغيرهم من ناشطي حقوق الإنسان، قطعة برمجية من أقدم برامج التجسس المعروفة، وهي برنامج "بيجاسوس" (Pegasus)، التي تسمح للمتسللين بجمع البيانات على المكالمات الهاتفية والرسائل والصور والفيديو.

ويتمتع برنامج "بيجاسوس" للتجسس، بقدرة على مراقبة أدق التفاصيل في حياة الهدف كإرسال تنبيهات إذا دخل الهدف منطقة معينة، على سبيل المثال، أو إذا ما التقى هدفان أو إذا اتصل الهدف برقم معين.

وتفيد وثيقة صادرة عام 2015 على صلة بدعوى قضائية رفعتها شركة "واتساب" ضد مجموعة (NSO) المالكة للبرنامج، بقدرة برنامج "بيجاسوس" على تسجيل الضغطات على لوحة المفاتيح والتنصت على الاتصالات الهاتفية.

ويمكن تحميل برنامج التجسس على هاتف الضحية من خلال حثه على الضغط على روابط خبيثة أو رسائل نصية مخادعة.

وتواجه الشركة الإسرائيلية اتهامات باستغلال خطأ تقني في تطبيق "واتساب" للاتصال عن طريق الفيديو وتوظيفه لاختراق هواتف 1400 مستخدم على مستوى العالم في الفترة ما بين 29 أبريل/نيسان حتى 10 مايو/أيار 2019.

ثغرة "جالاكسي"

وفي العام الماضي، أقرت أكبر شركة تصنيع هواتف ذكية في العالم، بوجود ظهور ثغرة أمنية كبيرة على بعض هواتفها.

وأعلنت "سامسونج" أنها ستصدر تحديثًا للبرامج لمعالجة ثغرة أمنية كبيرة ظهرت على هواتف "جالاكسي"، من خلال خداع الماسح الضوئي لبصمات الأصابع الموجود على شاشات هواتف "غلاكسي إس 10" و"نوت 10".

وتتيح تلك الثغرة الأمنية الحصول على بيانات مستخدمي جلاكسي الشخصية، واختراق محافظهم الإلكترونية.

ويقول الباحث في شركة "تشك بوينت" الإسرائيلية للأمن الإلكتروني، "عوديد فعنونو" إنه "لا يوجد برنامج خال من الأخطاء البرمجية".

وفي يوليو/تموز الماضي، اكتشف باحثون في "جوجل" 6 عيوب أمنية في "آيفون"، وعملت "أبل" (عدد عملائها ملياري مستخدم) على إصلاح 5 منها.

وقبل شهور، أعلنت "أبل" عن مكافأة قدرها مليون دولار مقابل اختراق هاتف "آيفون" في اختبار لأنظمة الأمان الخاصة بها.

وختاما، يبقى أن نؤكد أن أمن الهواتف الذكية بات مهددا بشكل متزايد، الأمر الذي يزيد المخاوف بشأن حياة المعارضين، والمدافعين عن حقوق الإنسان، لاسيما مع تنامي تجارة برمجيات التجسس واختراق الهواتف حول العالم.