كيف تحمي نفسك من الهجوم السري الذي يستهدف ملايين الهواتف في العالم؟

الأحد 9 يونيو 2024 11:35 م

ستهدف هجوم وُصف بـ"السرّي الخطير" ملايين أجهزة الهاتف في العالم، حيث استهدف المعلومات والمحتويات؛ فيما حذّرت وكالة الأمن القومي الأمريكية، جميع مستخدمي الهواتف الذكية في العالم، بكافة أنواعه، من هذا النوع من الهجوم، في إشارة إلى أن الضحية على الرغم من أنه قد يكون مُستهدفا، فإنه لا يشعر بالأمر.

وفي هذا السياق، كشف تقرير لجريدة "ديلي ميل" البريطانية، عن مسؤولين أمريكيين من وكالة الأمن القومي قولهم، إن أي شخص لديه هاتف "آيفون" أو هاتف بنظام "أندرويد" يجب عليه الحذر من هذا الهجوم الإلكتروني.

ومن أجل تفادي الوقوع، ضحية لهذه الهجمات، فقد كشفت الوكالة، أن الطريقة بسيطة، وهي أنه يجب مواظبة المستخدمين على إطفاء جهاز الهاتف وإعادة تشغيله مرة واحدة على الأقل في الأسبوع، حيث إن هذه الطريقة يمكن أن تحمي الشخص من المتسللين.

ويقول الخبراء إن "إطفاء الجهاز بشكل كامل ومن ثم إعادة تشغيله يُمكن أن يحمي من الهجمات التي يُطلق عليها اسم "Zero Click" أو ما يمكن تسميته بالعربية "صفر نقرات"، وهي التي تتضمن تنزيل برامج تجسس على هواتف المستخدمين دون النقر على أي رابط.

إلى ذلك، أيّدت وكالة الأمن القومي، هذه الطريقة، في إشارة إلى أنها تحذف بشكل مؤقت المخازن الضخمة من المعلومات التي تعمل باستمرار في الخلفية، مثل التطبيقات أو متصفح الإنترنت.

كذلك، طلبت وكالة الأمن القومي، من المستخدمين، توخّي الحذر بخصوص الاتصال بشبكات "WiFi" العامة، كما أنها نصحت في الوقت نفسه بـ"تحديث برامج وتطبيقات الهواتف بانتظام".

وأبلغت وثيقة الوكالة، المستخدمين، بأهمية تحديث البرامج والتطبيقات بشكل متكرر لضمان أمان جهازك. حيث إنه بمرور الوقت، يجد المتسللون طرقا جديدة لاقتحام النظام، لكن تحديث البرامج القديمة سيؤدي إلى إزالة أي عيوب أو ثغرات محتملة ربما استخدموها للوصول إلى بياناتك.

وأوصت وكالة الأمن القومي، الأشخاص بتعطيل تقنية البلوتوث الخاصة بهم عندما لا يستخدمونها، لأن ذلك يقلل من فرصة حصول الأشخاص على وصول غير مصرح به إلى أجهزتهم.

تجدر الإشارة إلى أنه عكس الأشكال الأخرى من البرامج الضارة، فإن هجمات "صفر نقرات" لا تتطلب أي تفاعل من طرف الضحية. حيث إن المتسللين يستغلّون ثغرة أمنية في البرنامج ويتمكنون من الوصول إلى الأجهزة، من دون الحاجة إلى خداعك للنقر على رابط ضار أو تنزيل ملف ضار.

وفي حال لم يلتزم مستخدم الهاتف، بإيقاف النظام وإعادة تشغيله، على الأقل مرة واحدة أسبوعيا، فإنه يمكن لمجرم الإنترنت التعامل مع عناوين "URL" المفتوحة من أجل تشغيل التعليمات البرمجية التي تبت ملفات ضارة على الأجهزة.

أيضا، سوف تضيف شاشة القفل القوية التي تحتوي على رقم تعريف شخصي مكون من ستة أرقام على الأقل الحماية المطلوبة بشدة عند دمجها مع الميزة التي تطالب الهاتف الذكي بمسح نفسه بعد 10 محاولات غير صحيحة.

وحذرت من أنه يجب على الأشخاص تجنب فتح مرفقات البريد الإلكتروني أو الروابط من مصدر غير معروف والتي قد تؤدي إلى تثبيت برامج ضارة دون علم الشخص.

وبحسب بيانات نشرتها شركة "ستاتيستا" فإنه تم اختراق بيانات 353 مليون شخص في الولايات المتحدة، العام الماضي، بما في ذلك الانتهاكات والتسريبات والكشف.

وكان آخر استغلال كبير لهجمات "صفر نقرات" قد حدث خلال عام 2021 والذي استهدف تطبيق "iMessage"، واستخدم ثغرة أمنية تتعلق بالطريقة التي يعالج بها التطبيق الصور.

وكانت شركة التكنولوجيا العملاقة، قد رفعت دعوى قضائية ضد مجموعة "NSO" وهي شركة استخبارات إلكترونية إسرائيلية، معروفة في المقام الأول ببرنامج التجسس الخاص بها "Pegasus" وهو القادر على استغلال النقرات الصفرية.