ممارسات خاطئة تعرّض الجهاز الذكي للاختراق.. تعرّف عليها

الجمعة 11 أغسطس 2017 11:08 م

مع التنامي المتسارع لأعداد مستخدمي الأجهزة الذكية حول العالم، تزداد المخاوف من مخاطر اختراق الأنظمة المُشغِّلة لها، وفي مقدمتها "آندرويد"، الأمر الذي دعا الشركات العالمية إلى إطلاق تحديثات أمنيّة مستمرة لإغلاق الثغرات، التي خصصت لمراقبتها مجموعة من المتخصصين في مكافحة القرصنة.

خطر الاختراق أصبح حقيقة، إذ باتت الشركات المطوّرة للأنظمة نفسها تتحدث عنها، بعد أن كانت تتجنّب ذلك لغايات تجارية؛ حرصاً على عدم خسارة مستخدميها الذين دخلوا ضمن حسابات المنافسة.

فكلما زاد عدد المستخدمين الفاعلين زادت الشركة حذراً وتطويراً لأنظمتها لتحافظ على موقعها في ساحة المنافسة العالمية، التي باتت تتأثر بعوامل عدة؛ في مقدمتها أمن النظام الذي تحققه الشركات في أجهزتها الذكية.

ووفقاً لما أوضحه خبير أمن المعلومات الفرنسي، جوليان فليتش، لـ "الخليج أونلاين"، فإن القيود الصارمة التي فرضتها القوانين العالمية أجبرت صنّاع التكنولوجيا الحديثة حول العالم على الإفصاح عن كافة المخاطر التي تواجه مستخدمي الأجهزة الذكية والأنظمة التي يصنعونها.

وقال فليتش: "من المهم جداً الإشارة إلى الأخطاء الكبيرة للمستخدمين التي تعرّضهم لخطر الاختراق، أو فشل النظام في توفير الحماية الكافية لهم، وذلك من خلال استخدامهم برامج كسر الحماية في أنظمة الأجهزة الذكية؛ مثل تفعيل خاصية روت في نظام آندرويد، الذي تطوره جوجل، وتفعيل خاصية جلبريك في نظام (آي أو إس)، المستخدم في الأجهزة الذكية التي تصنعها آبل".

وتعمل خاصية "روت" في الأجهزة الذكية العاملة بنظام "آندرويد" على الدخول إلى جذر النظام، وكسر الحماية التي يوفرها النظام للأجهزة الذكية؛ من أجل تحميل برامج غير موافق عليها من الشركة، تلك التي يقوم عدد من المطوّرين بتصنعيها وعرضها على شبكة الإنترنت، ما يعرّض المستخدم في حال تحميلها لخطر الاختراق عبر فيروسات التجسّس المتضمّنة فيها.

أما خاصية "جلبريك" التي يتم تفعيلها في الأجهزة الذكية المصنّعة من قبل "آبل"، فهي لا تختلف كثيراً عن خاصية "روت" من حيث آلية العمل، فضلاً عن أنها تقدّم للمستخدمين متجر "سيديا"، الذي يوفر بعد تفعيله ما يعرف بأدوات "سيديا"، التي تتيح للمستخدمين تطبيقات عديدة لا يستطيع المستخدم الحصول عليها في الأحوال العادية، ومن بينها تطبيق تسجيل المكالمات، حتى مع تطبيقات الاتصال مثل "واتساب"، و"فايبر"، وفتح أكثر من حساب "واتساب"، وأكثر من حساب "فيسبوك"، في الجهاز الذكي الواحد.

خبير البرمجة الفرنسي، فرانسوا شواب، أكد لـ "الخليج أونلاين" ما سبق ذكره حول خطورة استخدام خاصيتي "روت" و"جلبريك"، مضيفاً إلى ذلك أن تفعيلهما "سيمنع أيضاً تحميل التحديثات التي تطلقها الشركات لأنظمتها، وخاصة الأمنية منها، بحسب ما يتم رصده من مخاطر على المستوى العالمي، هذا فضلاً عن الإرباك الذي سيسببه كسر حماية النظام في عدم توافقية البرنامج مع وحدة المعالجة المركزية في الجهاز الذكي".

وتشير آخر التقارير العالمية لمراكز الأمن الإلكتروني إلى وجود الملايين من التطبيقات الذكية في متجر "بلاي ستور" التي تحتوي على برمجيات خبيثة، إضافة إلى عدد كبير منها في نظام "آي أو إس"، ونظام "ويندوز فون".

من جهتها صرّحت "جوجل"، عبر مدوّنتها الرسمية، في وقتٍ سابق من شهر يوليو الماضي، أن أي تطبيقات يتم رصد برامج خبيثة في تكوينتها البرمجية يتم إيقافها مباشرة، وحظر مطوريها، في حين نفت الشركة المزاعم التي تشير إلى وجود الملايين من التطبيقات الخبيثة الفعالة داخل متجرها.

جدير بالذكر أن آخر الميزات التي أضافتها شركة "جوجل" إلى متجر "بلاي ستور" هي تبويب (اختيار المحررين)، الذي تم اعتماده في عدد من دول العالم، وسيصل إلى عموم المستخدمين خلال العام الحالي، بالإضافة إلى ميزة "Play Protect" الجديدة، والتي تقوم تلقائياً بفحص التطبيقات المتاحة في متجر "بلاي ستور" المثبتة على الجهاز الذكي، وفي حال العثور على ما يريب فسوف يتم حظر التطبيق فوراً، وتنبيه المستخدم إلى ذلك