

كيف تنقذ هاتفك إن استغل للتنقيب عن العملة الرقمية؟



الأربعاء 14 فبراير 2018 01:02 م

بعدما تبين أن الهواتف الذكية معرضة أيضا لتسخيرها دون علم أصحابها في التنقيب عن العملات الرقمية مثلها مثل الحواسيب الشخصية، فقد أصبح لزاما اتخاذ إجراءات الحيلة والحذر ومعرفة كيف تكون هجمات "التنقيب" هذه وكيف يحتاط منها، خاصة أنها قد تتسبب بتلف دائم للهاتف الضحية

فقد كشفت شركة أمنية أميركية أن بعض مواقع الويب -حتى الآمنة منها- تتضمن إعلانات خبيثة تنبثق عند زيارة الصفحة فتستغل معالج الهاتف للتنقيب عن عملة مونيرو الرقمية، وأن نحو ستين مليون شخص يستخدمون أجهزة أندرويد زاروا مثل هذه المواقع بمتوسط زيارة يبلغ أربع دقائق، وهذا يعني بضعة آلاف من الدولارات من العملة الرقمية في كل مرة

وعملية التنقيب عن العملة الرقمية تؤدي إلى تشغيل معالج الهاتف بكامل طاقته بشكل مستمر مما يؤدي إلى سخونة مفرطة قد تتسبب، إذا طالت المدة ولم ينتبه صاحب الجهاز، بتلف دائم للهاتف نتيجة ذوبان بعض أجزائه

كيف يكون الهجوم؟

أولا، يصادف المستخدم إعلانا خبيثا في موقع ويب ربما كان آمنا قبل ذلك، فيحدد الإعلان نوعية متصفح الإنترنت الذي يستخدمه الشخص، وكذلك نوعية نظام التشغيل، فإذا اكتشف نظام أندرويد فإنه يعمل على توجيه المستخدم إلى صفحة خبيثة تدّعي أن الهاتف "يظهر سلوك تصفح مشبوها"، وعلى المستخدم إدخال عبارة التحقق (captcha) "للتيقن من أنه إنسان" وليس روبوتا

ولربما شاهد المستخدمون أمثال تلك المواقع المشبوهة إذا أمضوا بعض الوقت باستخدام متصفح في أجهزة أندرويد، لكن لدى هذا الموقع الخبيث ممسك، فهو يقول إنه حتى يكمل المستخدم إدخال عبارة التحقق، فإنه سيظل "ينقب لنا عن العملة الرقمية مونيرو كي نسترجع تكاليف الخادم التي كبدها حركة المرور الروبوتية (المؤتمتة)".

وهذا الجزء الأخير المتعلق باسترداد تكاليف الخادم، هو بطبيعة الحال مجرد هراء لا معنى له، لكن التنقيب عن العملة الرقمية ليس كذلك، فطالما بقي المستخدم على الصفحة، فإن صفحة الويب ستستغل معالج الهاتف للتنقيب عن مونيرو لكن المثير للاهتمام أنه بمجرد أن يدخل المستخدم عبارة التحقق وينقر على استمرار، فسيجري توجيهه إلى غوغل، وتتوقف عمليات التنقيب ولا يبدو أن هذا يؤدي إلى سرقة أية معلومات شخصية

والخطورة هنا إن دخلت إلى أحد هذه المواقع ونيست إغلاق الصفحة الخبيثة أو ابتعدت عن هاتفك وهو مفتوح على إحدى هذه الصفحات، فعندها قد يصيب الجهاز تلف دائم نتيجة السخونة المفرطة أثناء التنقيب عن العملة الرقمية

كيف تنقذ هاتفك من الموت؟

إن أفضل طريقة لمنع هذه الصفحة من التلاعب بهاتفك هو تشغيل حزمة تطبيقات مكافحة فيروسات لنظام أندرويد، وسيفيد هنا أي برنامج ما دام قادرا على حجب انبثاق الإعلانات غير المرغوبة في صفحات الويب

أما إذا لم ترغب في تثبيت أي برنامج لمكافحة الفيروسات، فلربما لن تتمكن من تفادي الهجوم، وذلك لأن بإمكان هذه الإعلانات الخبيثة الظهور في صفحات الويب الآمنة عادة التي ربما تستخدمها يوميا، لكن يمكن التخفيف من حدة الضرر الناتج بإغلاق متصفح الإنترنت فور ظهور الإعلان وإخبار الموقع الذي تستخدمه عن هذا الإعلان الخطير