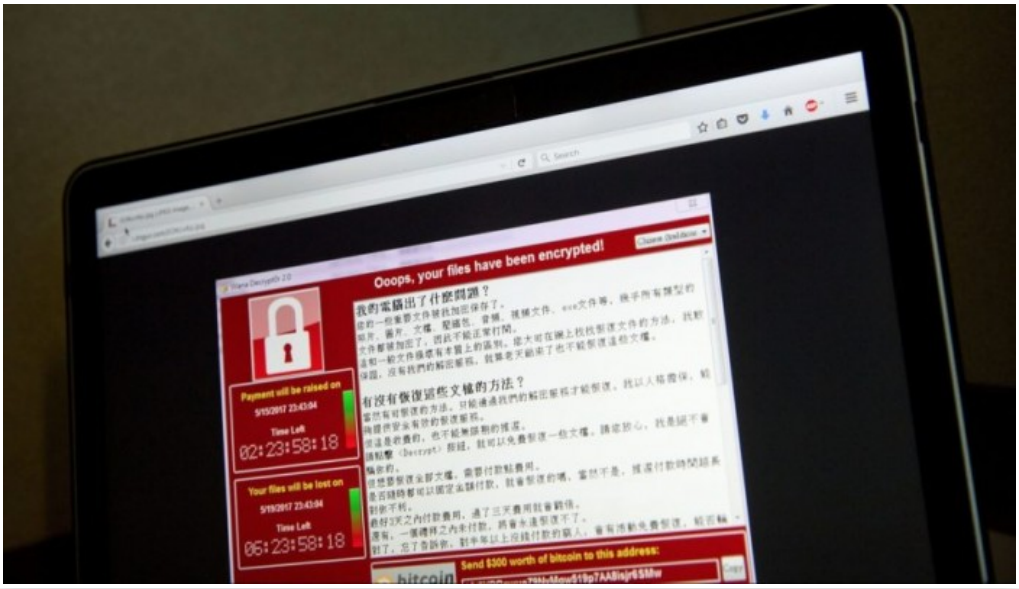
باحثون أمنيون يتوصلون لطريقة لمواجهة برمجية "وانا كراي" دون دفع الفدية



السبت 20 مايو 2017 06:05 م

باحثون أمنيون يتوصلون لطريقة لمواجهة برمجية "وانا كراي" دون دفع الفدية

وقد هددت برمجية "وانا كراي"، التي بدأت اكتساح العالم يوم الجمعة الماضي، وأصابت أكثر من 300,000 جهاز حاسب في نحو 150 دولة، بحذف بيانات الضحايا الذين لم يدفعوا فدية تراوحت قيمتها بين 300 و 600 دولار أمريكي في غضون أسبوع من الإصابة.

وقال فريق من الباحثين الأمنيين المنتشرين في جميع أنحاء العالم إنهم تعاونوا على تطوير حل لإلغاء قفل مفتاح التشفير للملفات التي أُصيبت في الهجوم العالمي الذي أكده العديد من الباحثين الأمنيين المستقلين.

وحذر الباحثون من أن حلهم لا يعمل إلا في ظروف معينة، يُذكر منها: إذا لم يحدث أن أُعيد تشغيل أجهزة الحاسب منذ إصابتها بالبرمجية الخبيثة، بالإضافة إلى وجوب أن تستعجل الضحية تطبيق الإصلاح قبل أن تقوم "وانا كراي" بتنفيذ تهديدها بقفل ملفاتها بصورة دائمة.

وقالت الشرطة الأوروبية "يوروبول" على موقع التدوين المصغر تويتر إن مركز الجريمة الإلكترونية الأوروبي قد اختبر أداة الفريق الجديدة وأكد نجاح الحل في "استرداد البيانات في بعض الظروف".

وأطلق الباحثون على أداتهم المجانية التي سوف تساعد على فك تشفير الأجهزة المصابة دون الحاجة لدفع الفدية اسم "وانا كيوي" WannaKiwi.

وقد تم اختبار "واناكيوي" بسرعة وأظهرت فعاليتها على نظام ويندوز 7 والإصدارات الأقدم مثل ويندوز إكس بي وويندوز سيرفس 2003، وفق ما أكد أحد الباحثين، وأضاف أن الأداة التي طُورت على عجل قد تعمل أيضًا على أنظمة ويندوز سيرفس 2008 وويندوز فيستا، ما يعني أنه تصلح للعمل على جميع الحواسب الشخصية المتأثرة بالبرمجية الخبيثة.

وذكر فريق الباحثين أنه حتى الآن تواصلت معهم مصارف مالية، وشركات طاقة، وبعض وكالة الاستخبارات الحكومية من العديد من الدول الأوروبية والهند، فيما يتعلق بالإصلاح.

وحتى يوم الأربعاء، كانت نصف عناوين الإنترنت التي أُتلفت عالميًا بسبب "وانا كراي" تقع في الصين وروسيا، مع نسبة بلغت 30% في الأولى، و 20% في الأخرى، وذلك بحسب البيانات التي قدمتها شركة كريبتوس لوجيك لتحليل التهديدات.

وعلى النقيض من ذلك، تمثل الولايات المتحدة 7% فقط من إصابات "وانا كراي"، أما بالنسبة لبريطانيا وفرنسا وألمانيا فتمثل كل منها نحو 2% فقط من الهجمات فى جميع أنحاء العالم، حسبما ذكرت كريبتوس لوجيك.

وكانت شركات وباحثون أمنيون قد توصلوا إلى أن كوريا الشمالية قد تكون وراء برمجية "وانا كراي"، الأمر الذي رد عليه نائب سفير كوريا الشمالية لدى الأمم المتحدة يوم الجمعة بالقول إن ربط بيونجيانج بهجوم "وانا كراي" الذي استخدم برمجيات الفدية الخبيثة أمر "سخيف".