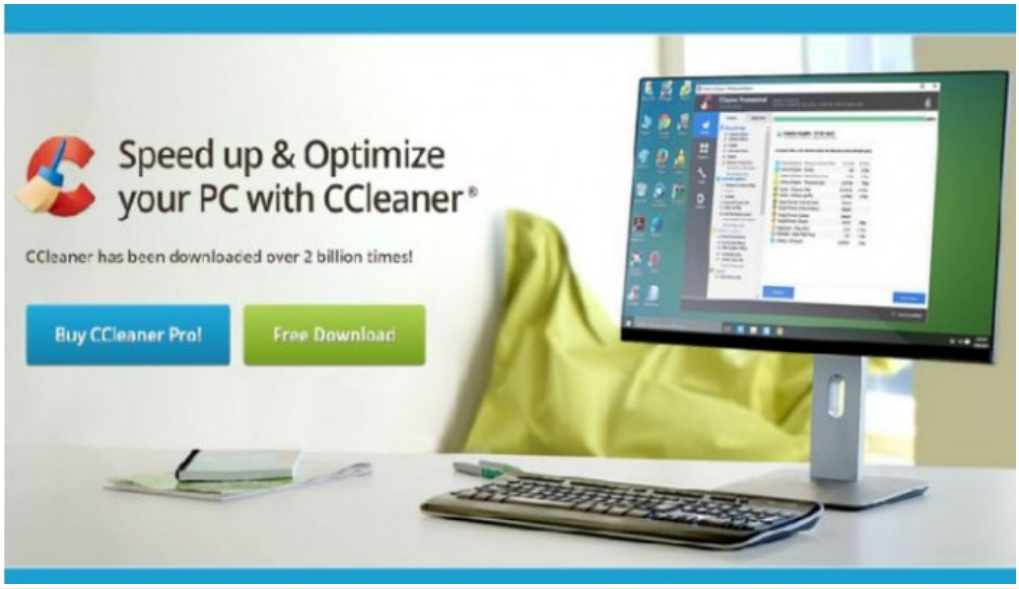
قراصنة يخترقون برنامج CCleaner الشهير ويعرضون أكثر من مليوني مستخدم للخطر



الاثنين 18 سبتمبر 2017 05:09 م

اخترق قراصنة إلكترونيون في الشهر الماضي برنامج تحسين أداء الحواسيب الشخصية المجاني من شركة "بيريفورم" Piriform البريطانية، الأمر الذي أتاح لهم التحكم بأجهزة أكثر من مليوني مستخدم، وفق ما أعلنت الشركة وباحثون مستقلون اليوم الاثنين.

وقالت الشركة إن البرنامج الخبيث أُخفي في برنامجها الشهير "سي كلينر" CCleaner، الذي يشهد أكثر من 5 ملايين تنزيل للحواسيب الشخصية وهواتف أندرويد أسبوعيًا. والذي يُستخدم لتنظيف "فضلات" البرامج وملفات تعريف الارتباط "كوكيز" الخاصة بالإعلانات بغية تسريع الأجهزة.

ويعد "سي كلينر" المنتج الرئيسي لشركة "بيريفورم"، التي تم شراؤها في شهر تموز/يوليو الماضي من قبل شركة أمن المعلومات التشيكية أفاست Avast. وحين الاستحواذ، أعلنت الشركة عن أكثر من 130 مليون مستخدم لبرنامج "سي كلينر".

وقال باحثون أمنيون في وحدة "تالوس" Talos التابعة لشركة سيسكو إن نسخة من برنامج "سي كلينر" جرى تنزيلها في شهر آب/أغسطس الماضي تضمنت أدوات إدارة عن بُعد حاولت الاتصال بالعديد من صفحات الويب غير المسجلة، التي يُحتمل أن تقوم بتنزيل برامج إضافية غير مصرح بها.

وقال الباحث لدى تالوس، كريج ويليامز، إنه كان هجومًا متطورًا لأنه اختراق موردًا موثوقًا به على غرار هجوم "نوت بيتيا" NotPetya الذي هاجم في شهر حزيران/يونيو الماضي الشركات التي قامت بتحميل برامج المحاسبة الأوكرانية المصابة.

وذكر ويليامز "لا يوجد شيء يمكن للمستخدم أن يلاحظه"، مشيرًا إلى أن برنامج تحسين أداء الحواسيب والهواتف يتمتع بشهادة رقمية أصلية، ما يعني أن أجهزة الحاسب الأخرى تثق تلقائيًا في البرنامج.

ومن جانبها، أكدت شركة "بيريفورم" في منشور على مدونتها أن اثنين من برامجها صدرا في شهر/أغسطس الماضي قد اخترقا. ونصحت مستخدمي الإصدار 5.33.6162 من برنامج "سي كلينر" والإصدار 1.07.3191 "سي كلينر كلاود" بتنزيل إصدارات جديدة.

وقالت متحدثة باسم الشركة إن 2.27 مليون مستخدم قد قاموا بتنزيل الإصدار المخترق من برنامج "سي كلينر" في شهر آب/أغسطس، فيما لم يقم سوى 5,000 مستخدم بتنزيل الإصدار المخترق من برنامج "سي كلينر كلاود".

وقالت بيريفورم إن شركتها الأم، أفاست، قد كشفت عن الهجمات يوم 12 أيلول/سبتمبر الجاري. وقد تم إطلاق إصدار جديد سليم من "سي كلينر" في نفس اليوم، وتم إطلاق إصدار سليم "سي كلينر كلاود" فى 15 أيلول/سبتمبر.

يُشار إلى أن برنامج "سي كلينر" لا يمكن تحديثه تلقائيًا، لذا يتعين على كل مستخدم قام بتنزيل الإصدار المخترق حذفه وتنزيل إصدار جديد، وفق ما قال ويليامز، الذي أشار إلى أن تالوس اكتشفت المشكلة في مراحلها الأولى، حينما ظهر أن القراصنة بدأوا يجمعون معلومات عن الأجهزة المصابة، بدلًا من إجبارهم على تنزيل برامج جديدة.