شن هاكرز هجوما عطل عمل عشرات آلاف الحواسيب في 74 دولة على نطاق العالم باستخدام خلل برمجي كان جزءا من أدوات مراقبة تستخدمها وكالة الأمن القومي الأميركي، وطلبوا دفع فدى بعملة إلكترونية.

وأوضحت صحيفة واشنطن بوست في تقرير لها أن الفوضى الإلكترونية ضربت عشرات الآلاف من الحواسيب بالعالم وعطلت أنشطة وزارة الداخلية الروسية، والاتصالات الإسبانية والخدمات الصحية البريطانية التي عاد العاملون فيها إلى استخدام القلم والورق.

وقال التقرير إن الهجمة -التي طالت أوروبا وأميركا اللاتينية وأجزاء من آسيا والولايات المتحدة- هي أحدث هجوم في عمليات "انتزاع الفدية" متنامية التهديدات، حيث يرسل الهاكرز ملفات إلى الحواسيب فتقوم بعد ذلك بتشفير بياناتها تلقائيا وتعرض مذكرة بطلب فدية على ملف نصي، الأمر الذي يعطل الحاسوب تماما إلا بعد دفع فدية.

الفدية بعملة إلكترونية

وتقول المذكرة بالملف النصي "عليك أن تدفع رسوم الخدمة إذا أردت فتح حاسبوك -إلغاء التشفير"، وحددت المذكرة مبلغ ثلاثمئة دولار لرسوم الخدمة المذكورة مدفوعة بعملة بتكوين -وهي عملة رقمية يصعب تعقبها- لترسل إلكترونيا إلى عنوان محدد، ولا تعرف الجهة المرسل إليها.

وقال التقرير إن حجم الفدية -وهو ثلاثمئة دولار- يعتبر قليلا مقارنة بفديات في هجمات سابقة مثل تلك التي أجريت في يونيو/حزيران الماضي بجامعة كالغاري الكندية التي وافقت على دفع 16 ألف دولار بعملة بتكوين لمجموعة قراصنة مجهولة.

وعلقت واشنطن بوست بأن هذه القرصنة أعادت من جديد جدلا قديما بشأن مخاطر وكالات الاستخبارات مثل وكالة الأمن القومي الأميركي التي تقوم بجمع واستخدام أخطاء البرمجة لأغراض التجسس بدلا من إبلاغ الشركات المنتجة للبرمجيات بهذه الأخطاء فورا لإصلاحها.

سبب نجاح الهجوم

وشرحت الصحيفة أن ما حدث هو أن وكالة الأمن القومي اكتشفت خللا في أحد برامج مايكروسوفت والذي أتاح للقراصنة أن يشنوا هجومهم.

وكانت الوكالة قد أبلغت مايكروسوفت بعد اكتشاف انتهاك لأمن أجهزتها في أغسطس/آب الماضي، وقامت مايكروسوفت بإصلاح الخلل في مارس/آذار الماضي قبل أن تنشره مجموعة تسمي نفسها "شيدو بروكرز" على الإنترنت علنا في أبريل/نيسان الماضي.

ولم يعمم إداريو مايكروسوفت إصلاح الخلل على كل الحواسيب التي تستخدم البرنامج، الأمر الذي ترك كثيرا منها عرضة للهجمات.

ولم تتضح بعد الجهة التي تقف وراء الهجوم واسع النطاق الذي قال عنه خبراء إنها المرة الأولى المعروفة التي يستخدم فيها هاكرز أدوات وكالة الأمن القومي الأميركي التي نشرتها "شيدو بروكرز".

أسرع وأوسع الهجمات

وقد أدهشت سرعة ونطاق انتشار الخلل كثيرا من الخبراء، وقال كبير الإستراتيجيين لشركة فلاشبوينت الأميركية كريس كاماشيو -وهي شركة لاستخبارات الإنترنت- إنها واحدة من أوسع الحملات العالمية التي تتم، وإنها المرة الأولى التي تستخدم فيها "دودة انتزاع الفدية".

ويسمى البرنامج الذي يستخدمه الهاكرز "وانادیکریبت أو آر "2.0 ويبدو أنه يدعم 28 لغة، الأمر الذي يؤكد طموحات المهاجمين.

ولم ترد وكالة الأمن القومي على أسئلة الصحيفة، لكن بعض الخبراء عبروا عن تعاطفهم مع الوكالة نظرا إلى أنها أبلغت مايكروسوفت بالمشكلة بالفعل قبل نشرها من قبل القراصنة.

كاتب المقالة :
تاريخ النشر : 13/05/2017
من موقع : موقع الشيخ محمد فرج الأصفر
رابط الموقع : www.mohammdfarag.com