استغل هجوم طلب الفدية واسع النطاق الذي ظهر يوم الجمعة الماضي ثغرة اكتشفت حديثا في نظام التشغيل ويندوز لينتشر بشكل أوسع وأسرع من أي هجوم سابق، الأمر الذي دفع مايكروسوفت المطورة لهذا النظام إلى كسر قواعدها المتعلقة بصيانة البرامج في محاولة للحفاظ على أمن المستخدمين.

وبرمجية طلب الفدية التي عرفت بعدة أسماء، منها "وناكريبتور" و"وناكراي" أو "ويكراي" أو "وناكربت" أو "ويكريبتور" استخدمت ثغرة في مكون خادم ويندوز للانتشار ضمن شبكات المؤسسة المستهدفة، واكتشفت هذه الثغرة أول الأمر وكالة الأمن القومي الأميركية ثم سرقها منها قراصنة إنترنت يطلقون على أنفسهم اسم "شادو بروكرز" ونشروها على الإنترنت.

وقد أطلقت مايكروسوفت تحديثا بعد وقت قصير من سرقة ونشر البيانات المتعلقة بالثغرة، مما أدى بالكثيرين للاستنتاج بأن وكالة الأمن القومي أخفت متعمدة وجود هذه الثغرة.

وبطبيعة الحال، فإنه نتيجة لسياسة الشركة فإن بعض نسخ ويندوز الشائعة الاستخدام لم تعد تتلقى تحديثات أمنية، بما في ذلك "ويندوز سيرفر "2003 و"ويندوز أكس بي"، وكذلك "ويندوز "8 الذي قد يفضله البعض على نسخة "ويندوز "8.1 المدعومة، لكن الشركة توفر "دعما خاصا" للمؤسسات التي تستخدم تلك الأنظمة مقابل رسوم باهظة.

لكن بمجرد انتشار فيروس "وناكراي" اتخذت مايكروسوفت خطوة غير معتادة إطلاقا، حيث أصدرت تحديثات أمنية مجانية لتلك الأنظمة التي لم تعد مدعومة، ويمكن تنزيل تلك التحديثات من موقع الشركة.

كيف تحمي حاسوبك من برمجية طلب الفدية

- الثغرة غير موجودة في ويندوز 10 أحدث أنظمة تشغيل ويندوز، لكنها موجودة في كل ما سبقه رجوعا إلى ويندوز أكس بي، لذا فإن الترقية إلى ويندوز 10 قد تكون خيارا مهما.

- بعد طرح مايكروسوفت التحديث الأمني في مارس/آذار الماضي فإن مستخدمي أنظمة ويندوز فيستا وويندوز 7 وويندوز 8.1 يمكنهم بسهولة حماية أجهزتهم بتشغيل أداة "تحديث ويندوز" (Windows update).

وفي الواقع إن الأجهزة المحدثة كانت محمية بالكامل من فيروس وناكراي حتى قبل يوم الجمعة الماضي، وأصيبت الأجهزة التي أخطأ أصحابها بتأجيل تحديثها.

- مستخدمو ويندوز أكس بي وويندوز سيرفر 2003 وويندوز 8 بإمكانهم حماية أنفسهم ضد هذه البرمجية بتحميل الترفيع الجديد من موقع مايكروسوفت.

- ويمكن لجميع المستخدمين حماية حواسيبهم أكثر بعدم فتح مرفقات البريد الإلكتروني المشبوه الذي يعد أبرز وسائل انتشار برمجيات طلب الفدية، وكذلك تحديث كافة تطبيقات "أوفيس".

- إن برامج مكافحة الفيروسات - بما في ذلك أداة مايكروسوفت ويندوز دفيندر- تستطيع الآن تمييز البرمجية الخبيثة، لكن الاعتماد على هذه الأدوات وحدها للدفاع عن نظام التشغيل ليس كافيا، وذلك أن نسخا جديدة متشعبة من الفيروس قد تتجاوز هذه الدفاعات، وقد وجدت بالفعل تشعبات من هذا الفيروس لكن تأثيرها كان محدودا جدا بسبب عدم قدرتها على نشر نفسها.

- بالنسبة إلى الذين أصيبت أجهزتهم بالفيروس فإن الخبراء ينصحون بعدم الاستجابة لمطالب القراصنة بدفع مبلغ الفدية، فعدا عن أن دفع المال لا يضمن استعادة الملفات فإنه يعمل أيضا على تمويل الجرائم الإلكترونية مستقبلا، ويبدو أن ضحايا وناكراي يوافقون على ذلك، حيث تبين أن أقل من مئة فقط دفعوا مبلغ الفدية البالغة قيمته ثلاثمئة دولار.

كاتب المقالة :
تاريخ النشر : 17/05/2017
من موقع : موقع الشيخ محمد فرج الأصفر
رابط الموقع : www.mohammdfarag.com