ملايين الحواسب في خطر ولن تسعفها برامج مكافحة الفيروسات

الأحد 30 أكتوبر 2016 02:10 م

الكثير من مستخدمي الحواسب والأجهزة الذكية تعتمد على برامج مكافحة الفيروسات، حتى تقيهم شر البرامج الخبيثة التي تستهدف أجهزتهم وقد تفسد البيانات الخاصة بهم، ولكن بعض تلك الفيروسات لن توقفها أي أنظمة أمان

اكتشفت مجموعة من الباحثين في مجال الأمن والحماية وسيلة جديدة تسمح للبرمجيات الخبيثة بحقن تعليماتها ضمن عمليات أخرى دون أن يتم اكتشافها من قبل برامج مكافحة الفيروسات وأنظمة الأمن

وبحسب "بوابة التقنية"، تعمل الطريقة الجديدة مع كل النسخ الخاصة بنظام التشغيل ويندوز، بما في ذلك الإصدار الأحدث ويندوز 10، بحيث لا يمكن كشف هذه الطريقة عن طريق أدوات مكافحة البرمجيات الخبيثة الموجودة، الأمر الذي قد يشكل تهديدًا للملايين من أجهزة الحاسب في جميع أنحاء العالم

وقد ابتكر الطريقة الجديدة باحثون من شركة Ensilo الأمنية، وأطلقوا على الطريقة اسم AtomBombing، وذلك لأنها تعتمد على آلية جداول atom الموجودة في أنظمة ويندوز، ويوفر نظام التشغيل هذه الجداول الخاصة، بحيث يمكن استخدامها لتبادل البيانات بين التطبيقات

وقال الباحث الأمني تال ليبرمان من شركة Ensilo "ما وجدناه هو أن هناك إمكانية لدى المهاجمين لكتابة التعليمات البرمجية الخبيثة في جدول atom وإجبار برنامج شرعي على استرداد تلك التعليمات البرمجية الخبيثة من الجدول"، وأضاف "وقد وجدنا أيضاً إمكانية التلاعب بالبرامج الشرعية، والتي تحتوي الآن على التعليمات البرمجية الخبيثة، من أجل تنفيذ التعليمات البرمجية".

ولا يمكن لبرامج مكافحة الفيروسات والبرامج الأمنية الأخرى اكتشاف هذه التقنية الجديدة في حقن التعليمات البرمجية، وذلك لانها تستند على وظيفة شرعية ضمن نظام التشغيل، وتتواجد آلية جداول atom في جميع إصدارت ويندوز، ولا يمكن تصحيحها لانها ليست نقطة ضعف

وتستخدم البرمجيات الخبيثة تقنيات حقن التعليمات البرمجية لمجموعة متنوعة من الأسباب، على سبيل المثال تعمل أحصنة طروادة المصرفية على حقن التعليمات البرمجية الخبيثة في عمليات المتصفح من أجل مراقبة وتعديل المواقع المصرفية المعروضة محلياً، الأمر الذي يتيح للمهاجمين سرقة بيانات الدخول وتفاصيل بطاقات الدفع أو إعادة توجيه المعاملات سراً إلى حساباتهم

ويمكن استخدام تقنيات حقن التعليمات البرمجية من أجل تجاوز القيود التي تسمح بالوصل إلى بعض البيانات، والتي لا يتم الوصول إليها إلا عن طريق عمليات محددة، بحيث يمكن استخدامها على سبيل المثال لسرقة كلمات السر المشفرة من التطبيقات الأخرى أو لأخذ لقطات من سطح مكتب المستخدم عند عدم امتلاك البرمجيات الخبيثة لمثل تلك الإمتيازات المطلوبة

وقال ممثل شركة مايكروسوفت في بيان "تشجع شركة مايكروسوفت عملائها على ممارسة عادات حوسبة جيدة على الإنترنت، بما في ذلك الحذر عند النقر على وصلات تنقل المستخدم إلى صفحات الويب، أو فتح ملفات غير معروفة، أو قبول نقل الملفات، وذلك من أجل المساعدة على تجنب العدوى الخبيثة".

وقد لا تتمكن شركة مايكروسوفت من تصحيح هذه المشكلة دون قيامها بتغيير الطريقة التي تعمل بها أنظمة تشغيلها بشكل كامل، وذلك لأن تقنية AtomBombing تستغل وظائف شرعية ضمن نظام التشغيل لتنفيذ الهجوم