إسيت: مجموعة قراصنة كبيرة تستخدم موقع إنستاجرام للتجسس على أهدافها

الاثنين 12 يونيو 2017 07:06 م

أشارت شركة "إسيت" ESET إلى أن أحدث تكتيكات الهجمات الإلكترونية المستندة إلى الثغرة الأمنية watering hole تتضمن إساءة استخدام ترقية إحدى إضافات متصفح فايرفوكس على موقع التواصل الاجتماعي إنستاجرام

وقالت الشركة المتخصصة في أمن المعلومات إن مجموعة "تورلا إسبيوناج"، ذات السمعة السيئة في استهداف المواقع الحكومية ومسؤوليها الدبلوماسيين منذ عام 2007 على الأقل، نجحت في إضافة أسلوب جديد في هجماتها الإلكترونية إلى ترسانتها من البرمجيات الخبيثة

وأضافت "إسيت" أن "تورلا"، وكعادتها، تستهدف في هجماتها الإلكترونية الثغرات الأمنية من نمط watering hole في المواقع التي يزورها المستخدمون المستهدفون بهدف إعادة توجيههم نحو البنى التحتية لأنظمة القيادة والتحكم الخاصة بهم

وخلال الهجمات الإلكترونية الأخيرة، رصد الباحثون في "إسيت" انهيارًا في إحدى إضافات فايرفوكس المثبتة سابقًا وعلى نحو يغاير نسخها السابقة، تقوم الإضافة باستخدام خدمة bit.ly الخاصة بعنوان URL للوصول إلى أنظمة القيادة والتحكم

وبالرغم من ذلك، فلا يتم العثور على عنوان URL ضمن إضافات فايرفوكس، وإنما يتم الحصول عليها باستخدام التعليقات التي يتم إدراجها على منشورات محددة في موقع إنستاجرام ويشكل حساب المغنية الشهيرة بريتني سبيرز على موقع إنستاجرام أحد الأمثلة التحليلية على ذلك

وللحصول على خدمة bit.ly الخاصة بعنوان URL، تستعرض الإضافة التعليقات المنشورة على كل صورة، وتقوم باحتساب قيمة التجزئة المخصصة لبيانات كل تعليق وفي حال تطابق قيمة التجزئة مع رقم محدد، تقوم الإضافة بتشغيل رموز "التعبير النمطي" على التعليق بهدف الحصول على عنوان URL.

وفي معرض توضيحه لهذه الفكرة، قال جان إيان بوتين، كبير باحثي البرمجيات الخبيثة في شركة "إسيت": "لا شك أن استخدام تورلا لوسائل التواصل الاجتماعي من أجل الحصول على عناوين أنظمة القيادة والتحكم يسهم في تعقيد الأمور بالنسبة لمزودي خدمات الأمن الإلكتروني، إذ يسهم اتباع هذه التكتيكات في زيادة صعوبة عملية تمييز حركة البيانات الخبيثة من التدفق المشروع للبيانات على وسائل التواصل الاجتماعي ولذلك يمكن للمهاجم إجراء تعديلات أو محو أنظمة القيادة والسيطرة بكل سهولة، لأن المعلومات اللازمة للحصول على عنوان URL لأنظمة القيادة والتحكم هي عبارة عن تعليق يتم نشره على وسائل التواصل الاجتماعي".

وبهدف الوقاية من الوقوع كضحية للثغرة الأمنية watering hole، يوصي باحثو "إسيت" باتباع ممارسة فاعلة تتمثل في الاستمرار بترقية وتحديث المتصفحات وإضافاتها على نحو دائم وثمة إجراء آخر يمكن اعتماده وهو تجنب تحميل أو تثبيت أي إضافات/ملحقات من مصادر أو مواقع غير مشروعة