الخليج

اقتصاد, تقنية وسيارات

10 مايو 2023 16:57 مساء

كاسبرسكي» تحذر من إضافات متصفح الويب التي تسرق العملات المشفرة

أشارت «كاسبرسكي» إلى أن «إضافات المتصفح تُعد جزءاً من البرنامج يُمكن للمستخدمين تثبيتها لتخصيص وظائف متصفح الويب، ومع أنها سهلة الاستخدام، قد تشكل أيضاً تهديدات خطيرة للخصوصية والأمان»، لافتة إلى أنه «مع وجود عدد متزايد من الأشخاص الذين بدؤوا في الاعتماد على العملات المشفرة في المعاملات عبر الإنترنت طوّر مجرمو الإنترنت طرقهم بالتوازي مع ذلك، حيث أصبحت إضافات المتصفح هدفاً جذاباً للمتسللين الذين يتطلعون إلى استغلال مستخدمي العملات المشفرة المطمئنين».

وفي بداية 2023، لاحظت «كاسبرسكي» زيادة مضاعفة في عدد الإضافات الخبيثة، خاصة تلك المصممة لأداء عمليات تثبيت على الويب وسرقة العملات المشفرة. وتم أيضاً تسجيل ارتفاع في عدد برمجيات التي تثبت الإضافات الخبيثة على أجهزة الضحايا.

وأوضحت «كاسبرسكي» أن الإضافة الخبيثة تتدخل في وظائف المتصفح نفسه، كما أنها تحاكي البرامج الشرعية. وربما يكون من الصعب اكتشافها بواسطة برامج مكافحة الفيروسات. ويمكن للإضافات الخبيثة أن تغير ما يراه

المستخدم على متصفحه، على عكس ما يرسله الخادم بالفعل؛ على سبيل المثال: يمكن لهذه الإضافات إضافة أو إزالة نصوص، وتصنيفات، وحقول نصيّة، وعناصر موقع الويب الأخرى. وتستطيع أيضاً تتبع معرفات الشركات التابعة، والانخراط في أنشطة التصيد الاحتيالي، وسرقة بيانات الاعتماد، إضافة إلى سرقة العملة المشفرة.

• سرقة المعلومات الحساسة

وبحسب «كاسبرسكي»، يمكن لإحدى الإضافات الخبيثة إدراج حقل إضافي في نموذج أرسله خادم محفظة التشفير. ويتمثل الهدف من هذه الحقول الإضافية (المقترنة بملصقات وإرشادات داعمة) في خداع المستخدم، وحفزه على إدخال معلومات سرية معينة (مثل بيانات اعتماد تسجيل الدخول، وأرقام بطاقات الائتمان، وقيم التحقق من البطاقة وأرقام التعريف الشخصية، والرموز المميزة.. وما إلى ذلك)، حتى لو لم يتم طلب هذه المعلومات من (CVVs) محفظة العملات الرقمية بشكلها الأصلي.

وفي الغالب، تحاكي هذه الإضافات الخبيثة الإضافات الشرعية، ما يجعل من الصعب على المستخدمين التمييز بين الوظائف الإضافية الآمنة والخبيثة. وحال الانتهاء من تثبيتها تتمكن الإضافات من إدخال رمز خبيث في متصفحات المستخدمين، ليتمكن مجرمو الإنترنت بعد ذلك من سرقة المعلومات الحساسة، مثل المفاتيح الخاصة والعبارات الأولية لمحافظ العملات المشفرة، وبيانات اعتماد تسجيل الدخول، ومعلومات المصادقة الثنائية.

• الحذر من إضافات المتصفح

وقال سيرجي لوزكين، الباحث الأمني الرئيسي في فريق البحث والتحليل العالمي التابع لشركة «كاسبرسكي»: «يمكن تثبيت إضافات المتصفح من المتاجر الرسمية (مثل كروم وفايرفوكس)، أو مباشرة من أحد الملفات المتوفرة حالياً على أجهزة «ويندوز» في المتصفح الأكثر شيوعاً (كروم). وعند التثبيت من خارج المتاجر الرسمية يزداد خطر الإضافات الخبيثة. وفي هذه الحالة، يجب على المستخدمين وخاصة أولئك الذين يتعاملون مع عمليات العملات المشفرة على أجهزة «ويندوز» الخاصة بهم، وأن يكونوا حذرين من إضافات المتصفح التي يقومون بتثبيتها».

• نصائح للحماية

ولتوفير الحماية اللازمة، توصي «كاسبرسكي» بعدم تثبيت الكثير من الإضافات؛ لأنها لا تؤثر فقط على أداء الكمبيوتر، ولكنها تمثل أيضاً ناقلاً محتملاً للهجوم؛ لذا قم بتثبيت أقل عدد ممكن من العناصر الأكثر فائدة، وتثبيت الإضافات من متاجر الويب الرسمية فقط؛ لأنها تخضع لبعض التدقيق على الأقل، حيث يصفّي المتخصصون الأمنيون العناصر الضارة بطريقة شاملة.

كما دعت إلى ضرورة الانتباه إلى طلبات الأذونات التي قد تطلبها الإضافات. وإذا طلبت إحدى الإضافات المثبتة بالفعل على جهاز الكمبيوتر الخاص بك إذناً جديداً يجب أن يثير ذلك الحذر حول احتمال حدوث شيء ما. وربما تم الاستيلاء على هذه الإضافة أو بيعها. وقبل تثبيت أي إضافة، يفضل دائماً إلقاء نظرة على الأذونات التي تتطلبها والتفكير فيما إذا كانت تتطابق مع وظائف التطبيق. وإذا لم تتمكن من العثور على تفسير منطقي للأذونات يفضل عدم تثبيتها على الأرجح.