كاسبرسكي: لصوص البتكوين يضعون أعينهم على المدخرات المشفرة للمستخدمين

الأحد 5 نوفمبر 2017 09:11 م

اكتشف باحثون لدى شركة كاسبرسكي لاب برمجية خبيثة تسرق العملات المشفرة من محفظة المستخدم عن طريق وضع عنوانها بدل عنوان المستخدم في حافظة الجهاز.

وقالت الشركة الروسية الرائدة في مجال أمن المعلومات إن بياناتها أظهرت أن المجرمين يستهدفون العملات المشفرة التي تحظى بالرواج، مثل بتكوين وإثيريوم وزيكاش وداش ومونيرو. ونجح المجرمون مع محافظ بتكوين، واستطاعوا سرقة ما يقرب من 140,000 دولار.

وعلاوة على ذلك، وجد الخبراء برمجية خبيثة جديدة، مصممة لسرقة مونيرو من خلال عملية تُعرف باسم "التعدين" Mining، وثمّة في الواقع عينات متاحة منها.

وأشارت كاسبرسكي لاب إلى أن سرعان ما أصبحت العملات المشفرة (أو الافتراضية)، مع ازدهارها المستمر، هدفًا جذابًا لمجرمي الإنترنت في جميع أنحاء العالم.

وشهد باحثون في كاسبرسكي لاب ارتفاعًا في عدد برمجيات التعدين، ما أثّر في آلاف الحواسيب وخلق عائدات إجرامية بمئات الآلاف من الدولارات. كذلك، لاحظ الخبراء أن المجرمين بدأوا في استخدام تقنيات أقلّ تقدمًا وأنهم يقضون وقتًا أقل وينفقون موارد أقل في هذا المجال. ووفقًا للبحث، فإن لصوص العملات المشفرة، الذين يتزايدون انتشارًا منذ العام 2014، عاودوا مجددًا وضع أعينهم على مدّخرات المستخدمين المشفرة بهدف سرقتها.

واكتشف الباحثون في كاسبرسكي لاب برمجية خبيثة من نوع CryptoShuffler، مصمّمة لتغيير عناوين محافظ عملات المستخدمين المشفرة في حافظة الجهاز المصاب، التي تُستخدم للتخزين المؤقت للبيانات. وقد عُرفت هجمات اختطاف الحافظات لسنوات، والتي توجّه المستخدمين إلى مواقع خبيثة وتستهدف أنظمة المدفوعات عبر الإنترنت. ومع ذلك، فإن الحالات التي تنطوي على عنوان مضيف لعملات مشفرة تبقى نادرة الحدوث.

وإذا رغب المستخدم في نقل عملة مشفرة إلى مستخدم آخر، فمن الضروري، في معظم العملات المشفرة، معرفة رقم الهوية الخاصة بمحفظة المتلقي، وهو رقم فريد يتألف من عدة خانات. ويوضح الخبراء الطريقة التي تعمل بها برمجية CryptoShuffler على استغلال حاجة النظام إلى هذه الأرقام كي يشتغل.

تبدأ برمجية CryptoShuffler، بعد تهيئتها، بمراقبة حافظة الجهاز، التي يلجأ إليها المستخدم عند إجراء عملية دفع عبر الإنترنت، وذلك بنسخ رقم هوية المحفظة ولصقها في سطر "عنوان الوجهة" في التطبيق المستخدم لتنفيذ معاملة الدفع. ويبدّل التروجان محفظة المستخدم بأخرى مملوكة من الجهة التي تقف وراء البرمجية الخبيثة، وبالتالي فإن المستخدم بلصقه رقم هوية المحفظة في سطر "عنوان الوجهة"، سيضع عنوانًا غير العنوان المقصود إرسال المال إليه في الأصل. ونتيجة لذلك، فإن الضحية ينقل المال مباشرة إلى المجرمين، إلا إذا اكتشف المستخدم بيقظته عملية التبديل المفاجئة، إلا أن ذلك لا يحدث عادة؛ فالأرقام متعددة الخانات وعناوين المحافظ في المنصات العاملة بتقنية "بلوك تشين" Blockchain يصعب تذكرها. ولذلك من الصعب تمييز حدوث أي تغيير في سطر المعاملة، حتى وإن وقع أمام عيني المستخدم.

وأوضح الخبراء أيضًا أن استبدال الوجهة في الحافظة يحدث على الفور، وذلك بفضل بساطة البحث عن عناوين المحفظة؛ فالغالبية

العظمى من محافظ العملات المشفرة يكون له موضع ثابت في سطر المعاملة ودائمًا ما يستخدم عددًا معينًا من الخانات، ما يتيح للدخلاء بسهولة إنشاء رموز منتظمة لتحل محلها. واستنادًا إلى البحث، تعمل برمجية CryptoShuffler مع مجموعة واسعة من أكثر العملات المشفرة رواجًا، مثل بتكوين إثيريوم وزيكاش وداش ومونيرو وغيرها.

وسُجّلت أكثر نجاحات المجرمين الذيم يقفون وراء البرمجية الخبيثة CryptoShuffler، حتى الآن، في الهجمات التي شُنّت على محافظ بتكوين، استنادًا على ملحوظات من الباحثين المعنيين في كاسبرسكي لاب؛ إذ نجح أولئك المجرمون بسرقة 23 محفظة بتكوين قيمتها تعادل نحو 140,000 دولار، فيما تراوحت المبالغ الإجمالية في المحافظ الأخرى بين بضعة دولارات وعدة آلاف من الدولارات.

وقال سيرغي ياناكوڤسكي، محلل برمجيات خبيثة لدى كاسبرسكي لاب، إن العملات المشفرة "لم تعد تقنية بعيدة المنال"، مشيرًا إلى أنها تدخل في حياتنا اليومية وتنتشر بنشاط في جميع أنحاء العالم، لتصبح أكثر رواجًا بين المستخدمين، وأكثر جاذبية للمجرمين في الوقت نفسه، وأضاف: "لاحظنا في الآونة الأخيرة زيادة في الهجمات الخبيثة التي تستهدف أنواعًا مختلفة من العملات المشفرة، ونحن نتوقع أن يستمر هذا التوجّه، لذلك، فإن على المستخدمين الذين يفكرون في الاستثمار بالعملات المشفرة التفكير في ضمان تحقيق الحماية المناسبة لها".

كذلك وجد الخبراء تروجانًا آخر يستهدف عملة مونيرو المشفرة يُدعى DiscordiaMiner، وتم تصميمه لتحميل الملفات وتشغيلها من خادم بعيد. ووفقًا للأبحاث، ثمّة بعض أوجه التشابه في الأداء بين هذه البرمجية الخبيثة وبرمجية NukeBot، التي اكتُشفت في وقت سابق من هذا العام. وكما في حالة NukeBot، تم تشارك الشفرات المصدرية للبرمجية الخبيثة عبر منتديات القرصنة السرية.

ويوصي خبراء كاسبرسكي لاب المستخدمين بتثبيت حلول أمنية قوية تتيح وظائف مخصصة لحماية المعاملات المالية، مثل ميزة Safe Money المتاحة في حلول كاسبرسكي لاب. وتعمل هذه الميزة على فحص نقاط الضعف التي عُرفت باستغلال مجرمي الإنترنت لها، والتحقق باستمرار من البرمجيات الخبيثة المتخصصة، وحماية المعاملات من الاختراق بمساعدة من تقنية حماية برامج التصفح Protected Browser، وحماية الحافظة التي تخزّن البيانات الحساسة أثناء عمليات النسخ واللصق، على وجه التحديد.

وتقول الشركة إن منتجاتها تنجح في الكشف عن تلك البرمجيات الخبيثة ومنعها من العمل، وذلك بالأسماء التالية: Trojan-Banker.Win32.CryptoShuffler.gen، Trojan.Win32.DiscordiaMiner.