كيف يكسب قراصنة العملات المشفرة الأموال من وراء اختراق هواتفنا؟

كتبه بينيديكت فوست | 28 فبراير ,2018

ترجمة وتحرير: نون بوست

يمكن التنقيب عن بدائل البيتكوين، على غرار عملة مونيرو، على الهواتف الذكية والحواسيب اللوحية. ولعل هذا ما يجعل القراصنة يقدمون على قرصنة أجهزة الإلكترونية بهدف كسب الأموال، ما من شأنه أن ينعكس سلبا على أصحاب هذه الأجهزة.

في نهاية شهر كانون الثاني/ يناير الماضي، اكتشف الباحثون المختصون في مجال الأمن لدى شركة "كرودسترايك" للأمن السيبراني في كاليفورنيا، برنامجا ضارا جديدا أطلقوا عليه اسم "وانا ماين". ويخترق هذا البرنامج الخبيث الحواسيب لاستغلال قدراتها الحاسوبية بهدف التنقيب عن عملة المونيرو المشفرة، ويعرف هذا النوع من عمليات القرصنة باسم "كريبتو جاكينغ". في هذا السياق، أفاد المختصون في الأمن لدى مختلف شركات الأمن السيبراني بأن عملية الكريبتو جاكينغ تشكل أكبر خطر بالنسبة للمستخدمين خلال سنة 2018.

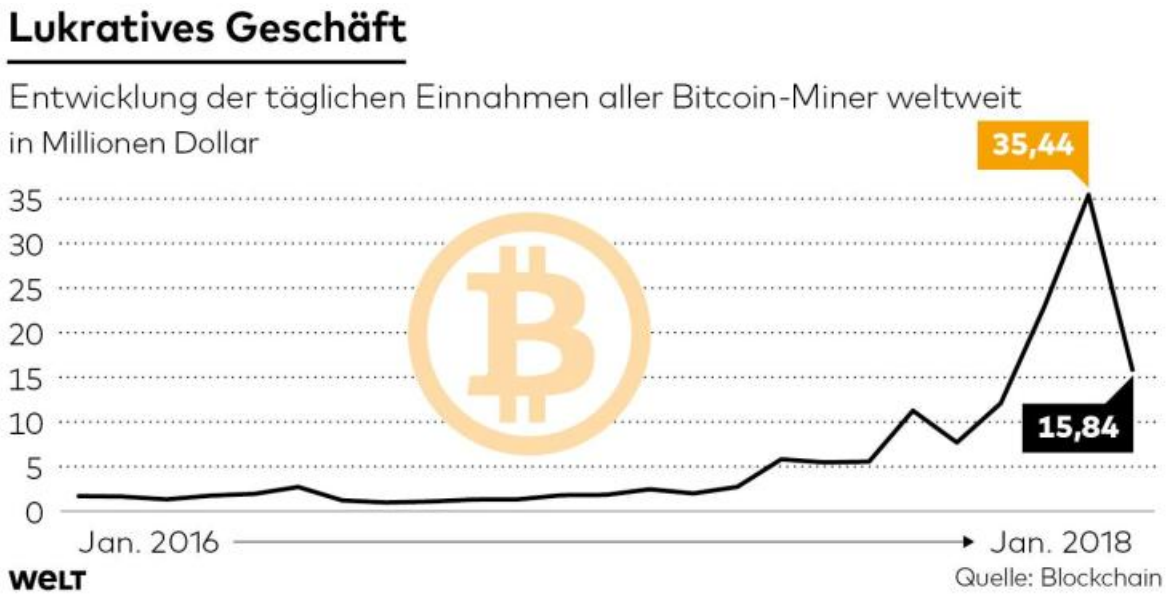
في الواقع، تعد المونيرو إحدى العملات الرقمية البديلة غير المنظمة، التي استفادت من الطفرة التي حققتها عملة البيتكوين خلال فصل الخريف الماضي. وتجدر الإشارة إلى أن عملة المونيرو تصدر باستخدام حاسوب مخصص للمعاملات الرقمية. ويتم مكافأة مستخدم الحاسوب ببعض العملات الرقمية. وخلافا للبيتكوين، يمكن احتساب قيمة المونيرو عن طريق الحواسيب العادية والهواتف الذكية، ما يجعل هذه العملة الرقمية عرضة للقرصنة من قبل جيل جديد من البرامج الضارة.

بالنظر إلى قدرته الحاسوبية المحدودة، لا يقدر الحاسوب إلا على التنقيب عن بعض السنتات من المونيرو. وفي حال اخترق البرنامج الضار آلاف الحواسيب، سيتمكن القراصنة من جني آلاف الدولارات في الشهر. ولعل الأجهزة الأكثر عرضة للقرصنة هي الأجهزة المحمولة؛ على غرار الهواتف الذكية والحواسيب اللوحية. ورغم قدرتها الحاسوبية المحدودة، إلا أن الهواتف الذكية أكثر انتشارا من الحواسيب، وتعتبر على الأغلب أقل تحصينا ضد هجمات البرامج الضارة مقارنة بالحواسيب، بالإضافة إلى أنها تبقى في وضع تشغيل لوقت طويل. وعلى هذا النحو، سيتمكن البرنامج الضار من استنزاف البطارية.

> يعتبر برنامج "الكريبتو جاكينغ" مزعجا جدا بالنسبة لمستخدمي الهواتف الذكية

مفتاح التعدين السري

في الوقت الراهن، يعمل القراصنة على ابتكار أساليب جديدة "للكريبتو جاكينغ". وعلى هذا الأساس، لن يخترق القراصنة الحواسيب فحسب، بل سيقومون بتحويل برامج التعدين على تطبيقات وهمية مثبتة على هواتف الأندرويد الذكية، أو سيحاولون خداع مقدمي الإعلانات الإلكترونية عن طريق إعلانات تتضمن مفاتيح تعدين سرية. ومن المتوقع أن يتعرض مستخدمو منصة الفيديو التابعة لشركة غوغل "يوتيوب" لهذا النوع من الهجمات.



رسم بياني يوضح تطور مداخيل المنقبين عن العملات الرقمية بملايين الدولارات في كافة أنحاء العالم

مما لا شك فيه، يعتبر برنامج "الكريبتو جاكينغ" مزعجا جدا بالنسبة لمستخدمي الهواتف الذكية. في هذا السياق، فسر الباحثون لدى الشركة المصممة للبرنامج المخصصة لمكافحة البرمجيات الخبيثة "مالوير بايتس" في مدونتهم، الأساليب التي يعتمدها القراصنة لجعل الملايين من هواتف الأندرويد الذكية تعمل على التنقيب عن العملات المشفرة. وقد تبين أن القراصنة المجهولين يبثون إعلانات

خاصة بأجهزة الأندرويد على مواقع الواب العادية أو على التطبيقات الهاتفية.

عندما يقوم متصفح الهاتف الذكي بتحميل هذا الإعلان، يتم توجيه المستخدم إلى موقع إلكتروني، بينما تبدأ عملية التنقيب بشكل سري. ومنذ ذلك الوقت إلى حدود إعادة تشغيل الهاتف على أقل تقدير، يطور المعالج قدرته الحاسوبية بشكل يصبح قادرا على التنقيب عن العملات الرقمية بالاشتراك مع الملايين من الأجهزة الأخرى. وفقا لتحليل برنامج "مالوير بايتس"، تم الولوج إلى المواقع الإلكترونية الخفية أكثر من 34 مليون مرة منذ شهر تشرين الثاني /نوفمبر. كما تعد أدوات "الكريبتو جاكينغ" والبرامج الخبيثة المخصصة لهذا الغرض الأكثر شيوعا بالنسبة لعملاء الأندرويد.

في المقابل، يعد مستخدمو "آي أو إس" الأكثر تحصينا ضد البرامج الخبيثة نظرا لأن متصفح "سفاري" غير قابل للاختراق بسهولة. بالإضافة إلى ذلك، تقوم آبل باختبار البرامج على الآب ستور بشكل أكثر دقة من غوغل.

شبكات حواسيب تعرضت بأكملها للاختراق

لم تُصمم الهواتف الذكية بشكل يجعلها تعمل لوقت طويل، حيث يمكن أن ترتفع درجة حرارتها، أو تتلف شاشة الصمام الثنائي العضوي الباعث للضوء بشكل سريع بمفعول الحرارة في البيت. فضلا عن ذلك، يمكن أن يفرغ شحن البطارية في غضون ساعة أو ساعتين أو يُستنزف تماما، خاصة أن التعدين يستهلك كامل حجم بيانات الهاتف.

> وصف الباحثون في مجال الأمن السيبراني في ريدلوك كيف كانت شركة تيسلا موتورز ضحية إحدى هجمات "كريبتو جاكينغ" التي اعتمدت على تطبيق مسروق من وكالة الأمن القومي الأمريكية

في الحقيقة، يعد "وانا ماين" البرنامج الأكثر تطورا في مجال الكريبتو جاكينغ إلى حد اليوم، نظرا لأنه يخترق شبكات حواسيب بأكملها داخل المؤسسات. وبالنسبة للقراصنة، تشترك خوادم الشركات والهواتف الذكية في ميزة واحدة، ألا وهي أنها نادرا ما تُغلق. ووفقا لتحليل شركة "كرودسترايك"، تم اقتباس شيفرة برنامج "وانا ماين" بشكل غير مباشرٍ من البرمجيات الخاصة بوكالة الأمن القومي الأمريكي.

خلال السنة الفارطة، تم الاستيلاء على برامج القرصنة الخاصة بوكالة الأمن القومي الأمريكي. وفي وقت لاحق، باعت مجموعة القراصنة وسطاء الظل شيفرات هذه البرامج. ومن جهتها، طورت وكالة الأمن القومي الأمريكي برنامجا أطلقت علية تسمية "إيترنال بلو"، المخصص لاختراق مختلف أنظمة الحواسيب. وقد تضمن برنامج " وانا ماين "أحد رموز البرنامج الخبيث الخاص بوكالة الأمن القومي الأمريكي.

تيسلا موتورز كانت من بين الضحايا

أما فيما يتعلق بالشركات التي تمتلك شبكة متكاملة من محطات العمل المزودة بمراوح ذات صوت مدوٍ، تعمل بكامل طاقتها لتعدين العملات المشفرة، فمن الممكن أن تقوم برمجية "وانا ماين" أو برمجيات خبيثة مشابهة لها بتعطيل مسارات العمل في هذه الشركات أو شلّ النظام بأكمله من خلال الحمل الزائد. وتتمثل الإشارة الوحيدة على التعرض لمثل هذا النوع من الهجمات من قبل تطبيقات الاستخبارات، في الارتفاع المفاجئ في قدرة عمل المعالج حتى تصل إلى 100 بالمائة. وفي حال كان الفاعلون أكثر حنكة، فلن يستغلوا أنظمة ضحاياهم بكامل طاقتها حتى لا يفتضح أمرهم.

في تحليل جديد نشر الأسبوع الماضي، وصف الباحثون في مجال الأمن السيبراني في ريدلوك كيف كانت شركة تيسلا موتورز ضحية إحدى هجمات "كريبتو جاكينغ" التي اعتمدت على تطبيق مسروق من وكالة الأمن القومي الأمريكية. فقد تبين أن القراصنة قد نجحوا في تحليل بيانات التتبع عن بُعد للسيارات الكهربائية بهدف استخدامها للتعدين.

> من خلال عملية "الكريبتو جاكينغ"، يستطيع قراصنة الإنترنت التنقيب عن العملات المشفرة مباشرة، دون الحاجة إلى ابتزاز الضحية للحصول على هذه العملات

لقد استطاعت برمجية "وانا ماين" الخبيثة أن توضح المجهود الذي بذله هؤلاء القراصنة من أجل الحصول على العملات المشفرة. وفي هذا الصدد، ذكر الباحث في شركة كراودسترايك، ريان ماكومبس، في تحليله لهذه الهجمات، "أنه لم يعد هناك فرق واضح بين الهجمات التي تشنها سلطات الأمن على مستوى الدولة والهجمات الإلكترونية العادية التي يشنها هؤلاء".

في سياق مغاير، أكد المحللون في كراودسترايك أن ذلك التطور يعد في صالح المستخدمين من الأفراد. فخلال السنوات الماضية، دأبت هذه المجموعات على قرصنة الحاسوب الشخصي للضحية أولا، ومن ثم تشفير القرص الصلب للحاسوب، وبعد ذلك يطلبون من ضحيتهم مبلغا من المال يدفع بواسطة العملة المشفرة مقابل إعطائه كلمة المرور التي وضعوها على حاسوبه.

من خلال عملية "الكريبتو جاكينغ"، يستطيع قراصنة الإنترنت التنقيب عن العملات المشفرة مباشرة، دون الحاجة إلى ابتزاز الضحية للحصول على هذه العملات. وبناء على ذلك، تعتبر تكلفة الطريقة الجديدة بالنسبة للمستخدمين الأفراد أقل بكثير من الطريقة السابقة، نظرا لأن المستخدم يستطيع الولوج إلى حاسوبه وبياناته الشخصية.

المصدر: فيلت

رابط المقال : https://www.noonpost.com/22261/