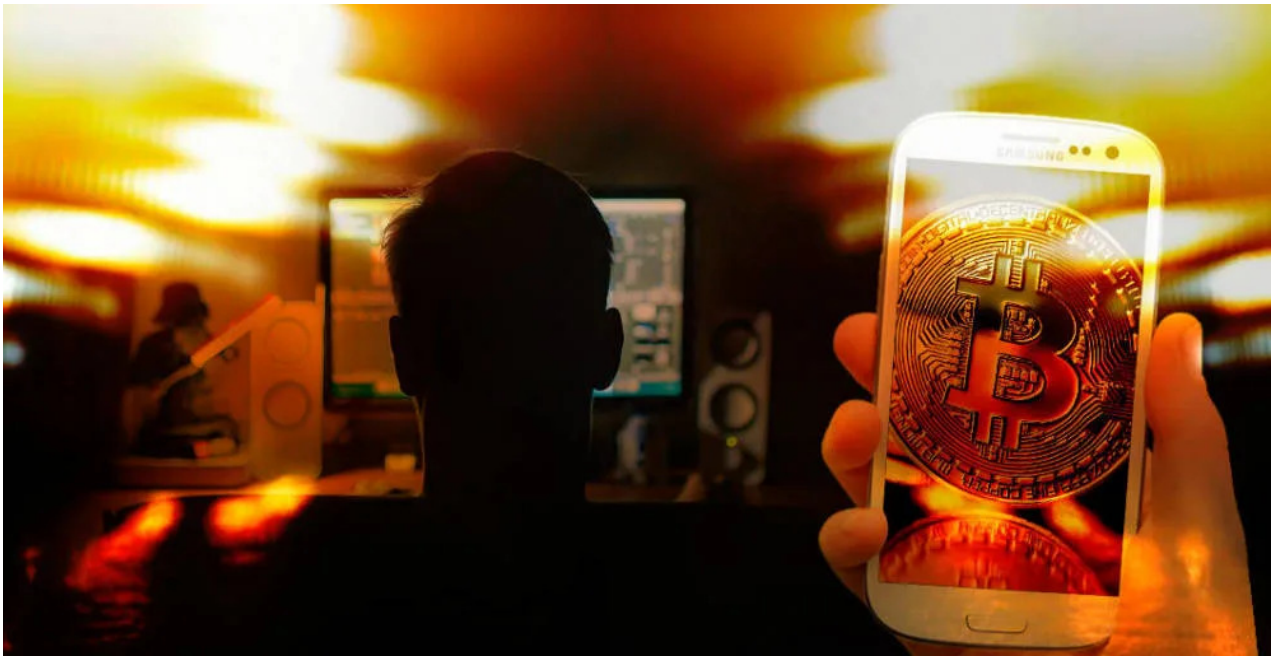
مايكل مكلوغلين | نشر في ٢٣ نوفمبر ٢٠١٧,

احذروا منها.. مواقع "تورنت" و"الواي فاي" المجاني أراضي خصبة لتعدين البيتكوين



ترجمة وتحرير: نون بوست

يشهد عصرنا الحالي نسخة مشابهة "لحمى الذهب" التي اعترت العالم في وقت سابق. وفي السنوات الأخيرة، أصبح ملايين الأشخاص يتهافتون لكسب العملة الرقمية، خاصة في ظل رواج عملة البيتكوين التي لم تفتأ تفجر حواجز لا يمكن تخطيها. ويتمثل آخر حاجز تخطته هذه العملة الرقمية، في وصول قيمتها إلى حدود ثمانية آلاف يورو. في الأثناء، تبقى عملية تعدينها غير سهلة. في الواقع، تتطلب عملية تعدين العملة الرقمية، البيتكوين، في المقام الأول "شلالا" من الطاقة الكهربائية. تحديدا، يحتاج الشخص الذي يرغب في المنافسة في سوق تعدين البيتكوين إلى 24 تيراواط ساعة في السنة. ونظرا لمعدل الطاقة الذي يحتاجه المنزل الإسباني على سبيل المثال في الأسبوع، يمكن فقط القيام بصفقة صغيرة في سوق هذه العملة الرقمية.

من جانب آخر، يتمثل العنصر الثاني في المعادلة، في المعدات التي يجب تخصيصها من أجل انتاج الطاقة اللازمة لإتمام عملية تعدين العملة الرقمية. وفي وقت ما، شهد العالم مشكلة خطيرة بسبب تزايد الطلب على بطاقات العرض المرئي عالية الجودة، التي يمكن أن تصل تكلفتها إلى حدود ألف يورو. وكان السبب الذي يقف وراء تزايد الطلب على هذه المعدات، تنامي عدد العاملين في "مناجم العملة الرقمية". في مرحلة موالية، يتم ربط الحاسوب المجهز بشكل جيد، بشبكة عالمية (أي شبكة التعدين). وتعمل بطاقات العرض المرئي بشكل جماعي وتجني نسبة من الأرباح بفضل مساهمتها في عملية تعدين العملة الرقمية.

ما هي الموارد الأخرى التي يتم تفعيلها؟

دفع هذا المزيج من استهلاك الطاقة والحاجة إلى العديد من الموارد، وأيضا التدفقات المالية العالية، القراصنة إلى البحث عن جملة من الحيل التي تساعدهم على تعدين البيتكوين دون متاعب. وترتكز هذه الخطة بالأساس على قرصنة العديد من الأجهزة (حواسيب وهواتف ذكية أساسا)، ليتحول بذلك

أصحابهم إلى مساعدين لهؤلاء القراصنة في عملية التعدين، دون أن يكون على علم بذلك. وفرضت هذه الخطة على القراصنة إنشاء شبكات "زومبي" ضخمة تتكون أساسا من أجهزة تتسم بقدرات عالية فيما يتعلق بعملية المعالجة لخدمة مصالح هذه المنظمات في حين تظل مستقلة لهذا الغرض، مع العلم أن هذه العملية تقع بطريقة غير مرئية وغير محسوسة من قبل المستخدمين العاديين.

في الآونة الأخيرة، حذرت العديد من الشركات المختصة في الأمن السيبراني من العديد من الممارسات التي تحدث على شبكة الإنترنت مشيرة إلى كيفية تطورها. وقد ورد آخر تنبيه خلال الأسبوع الماضي، حيث أطلقت السلطات الأسترالية تحذيرا مفاده أن "أحد القراصنة يجند العديد من الهواتف لصالح خدمته. وتتم هذه العملية من خلال الروابط التي ترسل عبر شبكات التواصل الاجتماعي أو البريد الإلكتروني".

"بكل بساطة، سيحترق الهاتف"

في هذه الحالة، تتم عملية "التصيّد" عن طريق رسالة قصيرة. وبعد فتح الرابط الوارد في الرسالة النصية، وتسجيله، يبدأ الهاتف الذكي بالعمل بشكل "بطيء للغاية". وفي هذا الصدد، أشار أوسيبيو نييفا، المختص في مراقبة أمن المعلومات، إلى أن "فقدان الهاتف لاستقلاليته وتردي أدائه، من الدلائل الجلية على تعرض الهاتف للقرصنة. وبشكل تدريجي، سينتهي أمر الهاتف بالاحتراق". وأضاف الخبير أن "مثل هذه الممارسات تمثل تهديدا جديا لمختلف المستخدمين، وفي أي مكان في العالم". وقد تمكنت الشركة التي يعمل لصالحها نييفا من الكشف عن "العديد من الحالات" التي تعرض خلالها المستخدمون العاديون لمثل هذا الاختراق. علاوة على ذلك، تزايد عدد الشركات المتضررة من عمليات التصيّد".

أكد أليكس بريوكشات، مؤلف كتاب "البلوك تشين، الثورة الصناعية للإنترنت"، أن "هجمات القراصنة تتبع تمشيا منطقيا، تماما مثل الذي تعتمده رسائل البريد المزعج أو ما يعرف بالسبام (الإعلان بأقل الأسعار).

في هذا السياق، تطرق الخبير إلى أماكن تمركز هؤلاء المتصيدين، حيث أورد أنه "في بداية الأمر، كانت عمليات التصيّد مرتبطة بمناطق جغرافية معينة، ألا وهي أساسا روسيا والصين. أما الآن، فقد انتشرت عمليات التصيّد على نطاق عالمي، حيث يمكن أن تحدث مثل هذه العمليات في جميع أنحاء العالم".

"عندما يصبح الهاتف المحمول جزءا من شبكة "الزومبي"، يبدأ أدائه في التدهور، ويفقد استقلاليته"

إلى جانب الرسائل النصية، تم اكتشاف أساليب أخرى يلجأ لها القراصنة لتحقيق هذا الغرض، أي تعدين العملة من خلال عملية التصيّد، خلال الأسابيع الأخيرة. وضمن أكبر منتدى على شبكة الإنترنت، ريديت، استنكر أحد المستخدمين عبر سلسلة من الرسائل، أمرا غريبا حدث معه على شبكة الإنترنت. فعندما حاول هذا المستخدم الاتصال بشبكة الإنترنت المجانية لأحد الفنادق، ظهر له إشعار مفاجئ من متصفح الكروم أدى إلى حظر الاتصال بالشبكة، وذلك بعد تسجيله ترصد أحد هؤلاء القراصنة المختصين في تعدين العملات الرقمية بهاتفه.

في وقت لاحق، وفي غضون وقت قصير، تطرق العديد من المستخدمين وخبراء آخرون إلى جملة من التجارب المماثلة. وقد سلطت هذه التجارب الضوء على حقيقة أن الواي فاي "العمومي" يمثل بوابة تؤدي في جميع الحالات إلى مثل هذه المشاكل. علاوة على ذلك، تقع ثلاثة أرباع هذه الحوادث عن طريق تطبيقات غوغل بلاي، وامتدادات مجانية لمختلف المتصفحات وشبكات تحميل التورنت. وخير مثال على ذلك، موقع "تورنت فريك" الذي تم إغلاقه بسبب استخدامه لبرمجية خبيثة في هذا الغرض.

من جهته، أكد أليكس بريوكشات، مؤلف كتاب "البلوك تشين، الثورة الصناعية للإنترنت"، أن "هجمات

القراصنة تتبع تمشيا منطقيا، تماما مثل الذي تعتمده رسائل البريد المزعج أو ما يعرف بالسبام (الإعلان بأقل الأسعار). وعلى هذا النحو، يصبح عمل القراصنة سهلا للغاية. ومن خلال هذه الإستراتيجية، لا يشرف المستعمل على إيصال جهازه بشبكة "الزومبي"، لكنه يتولى دفع الفاتورة بعد تصيد جهازه". وأضاف الخبير أن "المستقبل يحيل إلى تزايد مثل هذه العمليات بشكل كبير على مستوى الجيل الجديد من الإنترنت أو ما يعرف بمصطلح "إنترنت الأشياء"، الذي سيتيح للآلات القدرة على الاتصال بالشبكة على نحو متزايد".

2017: سنة قياسية

يتفق جميع الخبراء حول واقع أنه من الصعب جدا تحديد عدد الحواسيب المتضررة من عمليات القرصنة في جميع أنحاء العالم في الوقت الحالي، خاصة بعد اكتشاف حقيقة أن هذه التهديدات لحقت أيضا بالأجهزة اللوحية والهواتف المحمولة. وفي هذا السياق، أكدت شركت كاسبرسكي لاب المختصة في أمن الحواسيب في تحليل لها نشرته مؤخرا، أن "هذه السنة ستسجل أرقاما قياسية لعدد الحواسيب المتضررة بسبب مثل هذه البرمجيات الخبيثة التي سبق الحديث عنها".

بحلول شهر أيلول/ سبتمبر الماضي، تبين أن عدد الأجهزة الجديدة المتضررة التي تمثل جزءا من شبكات التعدين، قد وصل إلى حدود 1.65 مليون جهاز. وفي الإجمال، لم يتوقف هذا العدد عن النمو بتقدم الوقت. أما سنة 2016، فقد سجلت رقما قياسيا لأول مرة خلال هذا العقد، حيث بلغ هذا الرقم حدود 8.1 مليون جهاز. وعلى الرغم من تجنب الكشف عن حجم الأرباح التي تم جنيها عبر هذه الأعمال، إلا أن شركة كاسبرسكي لاب الروسية أكدت أن أحد معدني البيتكوين "غير القانونيين" يملك عملات رقمية من مختلف الأنواع بقيمة 200 ألف دولار.

"بحلول شهر أيلول/ سبتمبر الماضي، تعرض حوالي مليون جهاز جديد للقرصنة من قبل برمجيات خبيثة"

من جهة أخرى، يقف وراء النجاح والصعود الذي حققه سعر البيتكوين، تنامي عدد "الجرائم الرقمية" في هذا المجال. من جهته، أكد الخبير في أمن الحاسوب، سانتياغو ماركيز سوليس، أنه "نظرا لمدى تعقيد عملية تعدين هذه العملة الرقمية، أصبح نجاح هذه العمليات معتمدا أساسا على تزايد عدد الأجهزة المتضررة". وفي الأثناء، ليس من المنطقي أن يحاول أحد المستخدمين أن يكون هدفا لشبكات التعدين، الأمر الذي تروج له بعض التطبيقات. ويفسر ذلك بأن هاتفا محمولا واحد غير قادر إلا على جني بعض السنتات في السنة الواحدة.

لا يعد تعدين العملات الرقمية على غرار البيتكوين أو الإثيريوم أو غيرها، غير قانوني، إلا أن القيام بهذه العملية من دون إذن، يعتبر جريمة

تهتم شبكات "الزومبي" بعملات أخرى، تحتاج إلى عمليات وموارد أقل لإنتاجها. ومن بين هذه العملات الرقمية الأكثر شيوعا، نذكر مونيرو أو زكاش. وتقدر قيمة العملة الأولى بحوالي 140 دولارا، بينما تبلغ قيمة الثانية حوالي 300 دولار. وعلى الرغم من انخفاض قيمة هذه العملات مقارنة بالبيتكوين، إلا أنه يمكن للمعدنين الحصول عليها بسرعة أكثر.

التعدين وتصفح الإنترنت في الوقت نفسه

مثلما تطورت مقاطع الفيديو من خاصية التنزيل إلى الستريمينغ، يعمل القراصنة أيضا على تحديث أساليبهم وأدواتهم. وفي هذا الصدد، قال الخبير أوسيبيو نييفا إنه "في الآونة الأخيرة، ظهرت وسيلة أخرى، يمكن أن تتولى مهمة عملية التعدين وذلك عن طريق جميع أنواع الأجهزة القادرة على الإبحار عبر الإنترنت. ولا تتطلب هذه العملية تنزيل أي أداة بهدف تنفيذ عملية التعدين، حيث يقوم القراصنة

بعملهم من خلال برمجية جافا سكريبت".

"تستخدم بعض صفحات الويب أوامر برمجيات جافا سكريبت من أجل تعدين العملات الرقمية والإبحار عبر الإنترنت في الوقت نفسه"

لا يعد تعدين العملات الرقمية على غرار البيتكوين أو الإثيريوم أو غيرها، غير قانوني، إلا أن القيام بهذه العملية من دون إذن، يعتبر جريمة. وفي هذا الصدد، تُعلم بعض المواقع الشعبية مثل موقع خليج القراصنة، "بيرات باي" روادها أنهم يقومون بعملية التعدين خلال زيارتها، الأمر الذي يمكن تشبيهه بالاتفاق الذي تفرضه سياسة "ملفات تعريف الارتباط" المعروفة باسم "الكوكيز". علاوة على ذلك، ليس من المستغرب أن تلجأ بعض المواقع أو المنصات الحرة إلى مثل هذه الوسائل والاتفاقيات واعتمادها لإدارة أعمالها التجارية. في هذا الإطار، أوضح أوسيبيو نييفا، أنه "بمجرد إغلاق المتصفح، تتوقف عملية التعدين. وبالتالي، من الضروري عدم ترك بعض الصفحات مفتوحة، خاصة على الهواتف الذكية".

كيف يمكن تجنب مثل هذه العمليات؟ في هذا الشأن، أكد ماركيز سوليس أن الحل يختلف حسب تنوع المنصة. وأضاف سوليس أن "الحل يختلف من نظام تشغيل إلى آخر. ففي حال تعرض نظام ويندوز للقرصنة، فذلك يتطلب حلا خاصا، والأمر سيان إذا استهدف أحد القراصنة نظام لينكس". وينطبق المبدأ ذاته فيما يتعلق بالحلول الممكنة لمشاكل قرصنة الهواتف. وعموما، ينصح الخبير بالوقاية لضمان عدم التعرض لمثل هذه الحالات.

في الأثناء، أورد الخبير سوليس أن "الوقاية أفضل سلاح لضمان عدم مواجهة مثل هذه المشاكل. فضلا عن ذلك، يعد المستخدم العنصر الأضعف في كامل هذه الحلقة، لكن بإمكانه تقليص المخاطر إلى الحد الأدنى في حال كان على وعي بما يقوم به". وعلى العموم، يتفق الخبراء حول جملة من النصائح التي تتكرر في كل مرة، التي تتلخص في ضرورة تجنب زيارة المواقع غير الآمنة، وتحديث مكافح الفيروسات، وتفادي تنزيل برامج من مصادر غير معروفة.

المصدر: الكونفدنسيال الإسبانية

رابط المقال: https://www.noonpost.com/20847/