حمى تعدين العملات المشفرة

يستخدم المخترقون حيلًا قديمةً إضافةً إلى الشيفرات الجديدة لتحويل قوّة الحواسيب المسروقة إلى عملاتٍ رقميةٍ.

هل زرت موقع شوتايم **Showtime** مؤخرًا؟ إن فعلت ذلك، قد تكون معدِّن عملاتٍ مشفّرةٍ. حيث أطلق مستخدم تويتر **Twitter**، الشّهر الماضي، تحذيرًا بأنّ الرّماز المصدريّ لموقع شوتايم أني تايم **Showtime Anytime** يحوي أداةً تقوم بالاستيلاء على حواسيب الزّوار بغرض تعدين عملة مونيرو **Monero**، وهي عملةٌ شبيهةٌ بالعملة الرقمية البيتكوين **Bitcoin**، لكنّها ترتكز على السريّة وإخفاء الهويّة.

ليس معروفًا بعد كيفية وصول تلك الأداة إلى هناك، وقد قام موقع شوتايم بإزالتها عند اكتشافها. إن كان هذا عمل المخترقين، فهو جزءٌ من موجةٍ جديدةٍ، فقد شهد خبراء الأمن هذا العام ارتفاعًا كبيرًا في الهجمات الإلكترونيّة الهادفة إلى الاستيلاء على الحواسيب بغرض

عمليات التّعدين الرقميّة. التّعدين عمليةٌ مكثّفةٌ حسابيًّا، لدرجة أن جميع الحواسيب في الشبكة المشكّلة للعملة المشفّرة مطلوبةٌ للتحقّق من عملية نقل السّجل، الّتي تدعى سلسلة الكتل (**Blockchain**)، لتحصل بالمقابل على العملة الرقمية.

مؤخّرًا ظهرت تلك الأداة في كلّ مكانٍ على الإنترنت. هذه الأداة أطلقتها شركةٌ تُدعى كوينهايف **Coinhive**، وكان من المفترض أنّها تسمح لأصحاب المواقع الإلكترونيّة بكسب المال دون عرض الإعلانات. ولكن يبدو أنّ مؤلفيّ البرمجيات الخبيثة كانوا من أوائل مستثمريّ هذه الأداة. ففي الأسابيع القليلة الماضية، اكتشف الباحثون برنامجًا مخفيًّا في إضافات المتصفح غوغل كروم **Google Chrome**، ومواقع ووردبريس **Wordpress** المخترَقة، وحتى في أوساط قراصنة الإعلانات الخبيثة **malvertising** سيئي السّمعة.

أداة كوينهايف ليست الوحيدة، حيث يستخدم المخترقون العديد من الأساليب للاستيلاء على الحواسيب. مؤخّرًا أصدرت مختبرات كاسبرسكي **Kaspersky Lab** تقريرًا بيّنت فيه أنّها وجدت أدوات تعدين العملة المشفرة على 1.65 مليون جهاز حاسبٍ لعملائها هذا العام، وهو ما زاد كثيرًا عن معدّل العام الماضي.

وقد اكتشف الباحثون مؤخّرًا أعدادًا كبيرةً من روبوتات الشبكة (**botnets**) مجهّزةً للربح من عمليات تعدين العملة المشفّرة، وأشارت تقديراتٌ وسطيةٌ أن هذه العملية قد تولّد 30,000 دولارٍ بشكلٍ شهريٍّ. إضافةً إلى ذلك، فقد شهد الباحثون محاولاتٍ متزايدةً لتثبيت أدوات التعدين على مخدّمات عددٍ من المنظمات. وفقًا لفريق إكس فورس **X-Force**، وهو فريق آي بي إم **IBM** الأمني، فإنّ هجمات تعدين العملات الرقمية التي تستهدف شبكات الشركات، ازدادت ستّة أضعافٍ في الفترة بين يناير/كانون الثّاني وأغسطس/آب.

يقول الباحثون أنّ القراصنة منجذبون بشكلٍ خاصٍّ إلى البدائل الحديثة نسبيًا للبيتكوين **Bitcoin**، خاصةً مونيرو **Monero** وزي كاش **zCash**. أحد أهمّ الأسباب الّتي جعلت من القراصنة يفضّلون هذه العملات هو خصائصها التشفيريّة، والّتي تجعل من تعقّب القوى القانونيّة للتّعاملات الرقميّة أمرًا غير ممكنٍ. كما يمكن لهؤلاء القراصنة تحقيق أرباحٍ بتعدين العملات الجديدة أكثر ممّا يحقّقون من البيتكوين. كانت برمجيّة تعدين البيتكوين الخبيثة منتشرةً بكثرةٍ في السنتين أو الثلاث سنوات الماضية، لكنّ شعبيّة العملة جعلتها أكثر صعوبةً في التّعدين نتيجةً لتصميمها، ممّا يجنّبها هذا النوع من الهجمات. يقوم القراصنة حاليّاً بانتهاز العملات الجديدة، الأكثر سهولةً في التّعدين.

يقول جاستن فير **Justin Fier**، مدير الذّكاء الرقميّ في المختبر الأمني داركتريس **Darktrace**، إنه يمكن اكتشاف البرمجيات الخبيثة الّتي تحوي أدوات تعدين العملات المشفرة مباشرةً باستخدام برمجيّات مضادات الفيروسات. لكنّ عمليّات التعدين غير القانونية والّتي يقوم بها موظفون مصرّحٌ لهم تزداد، حتى أنه هناك موظّفون لديهم صلاحيّاتٌ عاليةٌ على الشّبكات، ومهاراتٌ تقنيةٌ كبيرةٌ تمكّنهم من تحويل بنية شركاتهم التحتيّة الحاسوبيّة إلى مراكزَ لإنتاج العملة.

في إحدى الحالات، تمكّن فريق فير (الّذي يعتمد على تعلّم الآلة **machine learning** في اكتشاف النشاطات الشاذّة داخل الشّبكات) من اكتشاف عاملٍ في شركة اتصالاتٍ كبيرةٍ، استخدم حاسب الشّركة بشكلٍ غير مصرّحٍ به للاتصال بحاسبٍ موجودٍ في منزله. وبعد تحقيقاتٍ موسّعةٍ اكتشفوا أنّ هذا الموظف كان يخطّط لتحويل غرفة الخوادم في شركته إلى منجم تعدين.

وإلى أن يأتي اليوم الّذي يُحاسب فيه المخترِقون، فإنّ هذه الأعمال داخل الشّركات ستبقى في قمّة تحديّات الأمن الرقميّ. وقد قامت بعض برامج منع الإعلانات بحظر كوينهايف لتُبقي المواقع المخترِقة بعيدةً عن حاسبك.

- التاريخ: 2018-01-27
- التصنيف: تكنولوجيا

#البتكوين #bitcoin #العملات المشفرة #العملات الرقمية

المصطلحات

- **تعليم الآلة (machine learning)**: تعلم الآلة هو أحد أنواع الذكاء الاصطناعي، يمكّن التطبيقات البرمجية من التنبؤ بنتائج أكثر دقة دون برمجتها بشكل صريح. ويتم ذلك عن طريق بناء خوارزميات تتلقى بيانات الإدخال وتستخدم التحليل الإحصائي للتنبؤ بقيمة المخرجات ضمن نطاق مقبول.
- **سلسلة الكتل (Blockchain)**: هي لائحة متنامية ومستمرة من الكتل Blocks، مرتبطة مع بعضها ومحمية بمستويات عالية من التشفير، وهي التقنية الأساسية التي تقوم عليها العملات الرقمية.

المصادر

- TechnologyReview

المساهمون

- ترجمة
  - المقداد علي
- مُراجعة
  - حنان مشقوق
- تحرير
  - حسن شوفان
  - رأفت فياض
- تصميم
  - أسامة أبو حجر
- صوت
  - ابتسام الخيال
- نشر
  - ريم فاخر