وب‌سایت‌ها از پردازنده سیستم شما برای درآمدزایی استفاده می‌کنند

آیا از پردازنده شما برای استخراج غیرقانونی بیت‌کوین استفاده می‌شود؟ + 5 راه جلوگیری از آن

استخراج کریپتوکارنسی (ارز رمزنگاری شده) یکی از اتفاقات روبه‌رشد دنیای امروز در اینترنت است و برخی از وبسایت‌ها با به‌کارگیری پردازنده سیستم‌های بازدیدکنندگان خود روش جدیدی برای درآمدزایی پیدا کرده‌اند. آن‌ها از این راه ارزهای دیجیتالی استخراج می‌کنند و ظاهرا درآمد خوبی هم دارند.

کریپتوکارنسی‌ها (cryptocurrency) یا به‌اصطلاح ارزهای رمزنگاری شده، پول‌های دیجتالی یا مجازی هستند که به‌منظور حفظ امنیت رمزگذاری می‌شوند (**بیت‌کوین**، **اتریوم** و ...). از آن‌جایی که این ارزها ذاتا ناشناس و غیرمتمرکز هستند، می‌توان از آن‌ها برای پرداخت‌ها استفاده کرد در حالی‌که دولت‌ها قادر به‌ردگیری آن‌ها نیستند. از طرف دیگر، محبوبیت کریپتو-ماینینگ رو به‌افزایش است به‌همین دلیل صاحبان سایت‌ها رو به استفاده از اسکریپت‌های استخراج کریپتوکارنسی آورده‌اند تا با استفاده از توان پردازنده سیستم‌های بازدیدکنندگان از وبسایت‌شان درآمدزایی کنند. حتی، برخی از توسعه‌دهندگان ترغیب شده‌اند تا با به‌کارگیری روش‌های مختلف مانع از استخراج کریپتوکارنسی در مرورگر وب شوند.

اخیرا مشخص شد که سایت Pirate Bay، در حال تست استخراج کریپتوکارنسی Monero روی سایت‌اش بوده است. گردانندگان این سایت اعتراف کردند که ممکن است برای ادامه حیات این سایت مجبور به‌استخراج کوین در آینده‌ای نزدیک شوند.

مطلب پیشنهادی

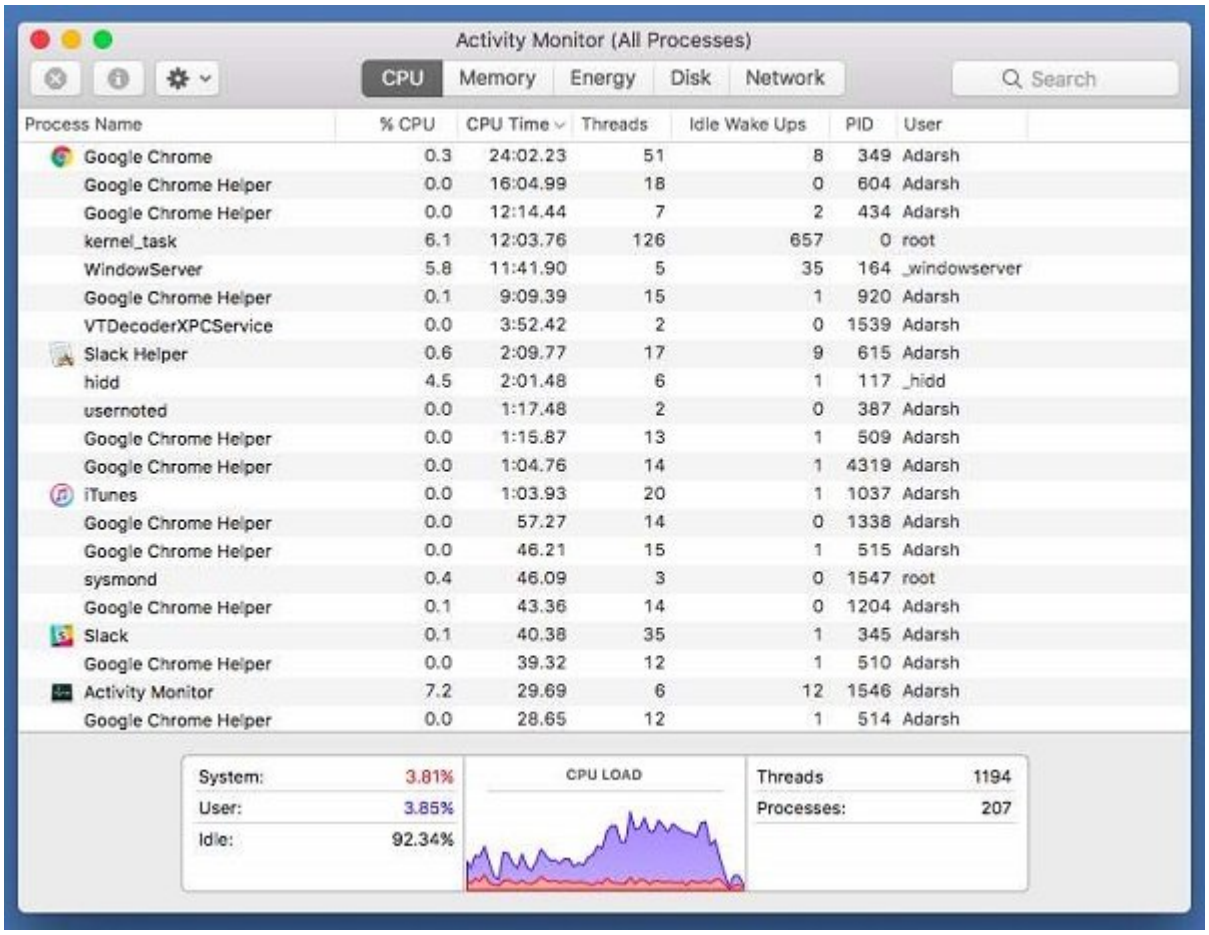
پرونده ویژه بیت‌کوین
دو روی سکه بیت‌کوین (بخش اول)

البته این کارها چندان هم جدید نیستند. اما Pirate Bay نخستین سایت مشهور دنیاست که از روش استخراج کریپتوکارنسی استفاده می‌کند. در پی انتشار این خبر، نگرانی‌هایی در بین کاربران این سایت به‌وجود آمده است. برخی از آن‌ها می‌گویند ممکن است که صاحبان این وبسایت خیلی از بازدیدکنندگان خود را در خفا نگه دارند.

اما نکته جالب آن است که خیلی از این افراد اهمیت چندانی به استفاده وبسایت‌ها از توان مصرفی پردازنده سیستم خود نمی‌دهند. قبل از این‌که به‌نحوه جلوگیری از استخراج کریپتوکارنسی در مرورگر وب بپردازیم بهتر است ببینیم که آیا هدف یکی از این فعالیت‌های استخراج قرار گرفته‌ایم یا نه.

از کجا بفهمیم که پی‌سی ما به‌طور مخفیانه در حال استخراج کریپتوکارنسی است؟

به‌غیر از باج‌افزارها، محبوبیت بدافزارهای استخراج بیت‌کوین با سرعت غیرقابل تصوری در حال افزایش است. اما، فهمیدن این‌که کدام وبسایت از مرورگر وب سیستم شما برای استخراج کوین‌های کریپتو استفاده می‌کند کار ساده‌ای است.



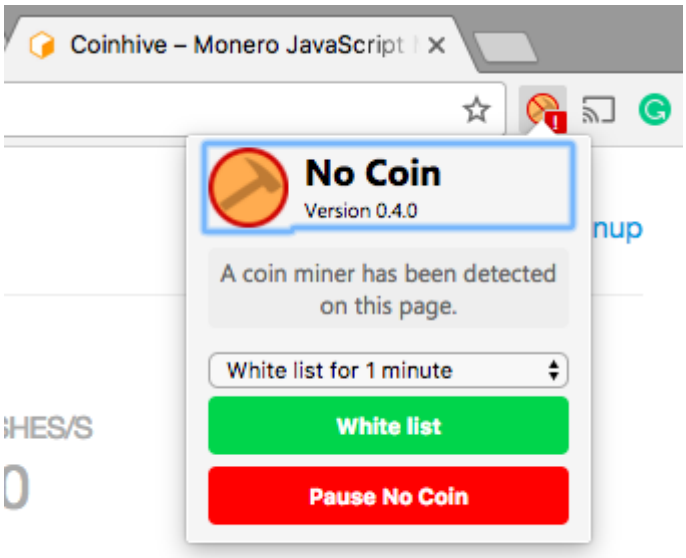
کاربران Pirate Bay زمانی متوجه سوءاستفاده این وبسایت از توان پردازنده سیستم‌های خود شدند که در هر بار بازدید از این وبسایت میزان استفاده از پردازنده به‌شدت افزایش پیدا می‌کرد. شما هم با همین روش می‌توانید بفهمید که آیا یک وبسایت خاص با استفاده از پردازنده سیستم شما در حال درآمدزایی است یا خیر. اگر بیشتر تب‌های مرورگر بسته است و هیچ اپلیکیشنی هم در حال اجرا ندارید به‌احتمال زیاد هدف این وبسایت‌ها قرار گرفته‌اید. اگر اطلاعات فنی زیادی ندارید کافی است به‌وبسایت‌های مختلف مراجعه کنید تا ببینید کدام یک از آن‌ها بار زیاد از پردازنده می‌کشد. اما، افراد فنی با استفاده از ابزارهای مخصوص مانیتورینگ این فرآیند می‌توانند وبسایت‌های خراب‌کار را پیدا کنند.

مطلب پیشنهادی

نگاهی به پول‌های دیجیتالی رمزگذاری‌شده و سرویس BaaS
آیا Ether جایگزین بیت‌کوین می‌شود؟

1 - استفاده از افزونه No Coin برای کروم

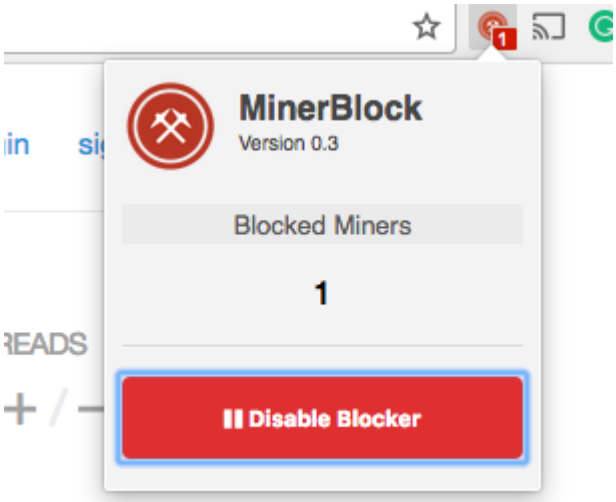
نصب افزونه‌های کروم ساده‌ترین و آسان‌ترین راه برای جلوگیری از استخراج کوین در مرورگر وب است. یکی از این راه‌کارهای رایگان No Coin نام دارد. این افزونه متن باز یک راه امن و قابل اطمینان برای کنترل تعاملات وبسایت‌ها با مرورگر وب سیستم شماست.



وقتی از یک سایت بازدید می‌کنید، No Coin در صورت شناسایی فعالیت‌های مشکوک به‌شما اخطار می‌دهد و یک علامت قرمز رنگ روی صفحه ظاهر می‌شود. این افزونه علاوه بر جلوگیری از این فعالیت، به‌شما این امکان را می‌دهد تا برای مدت کوتاهی با خیال آسوده از آن سایت بازدید کنید.

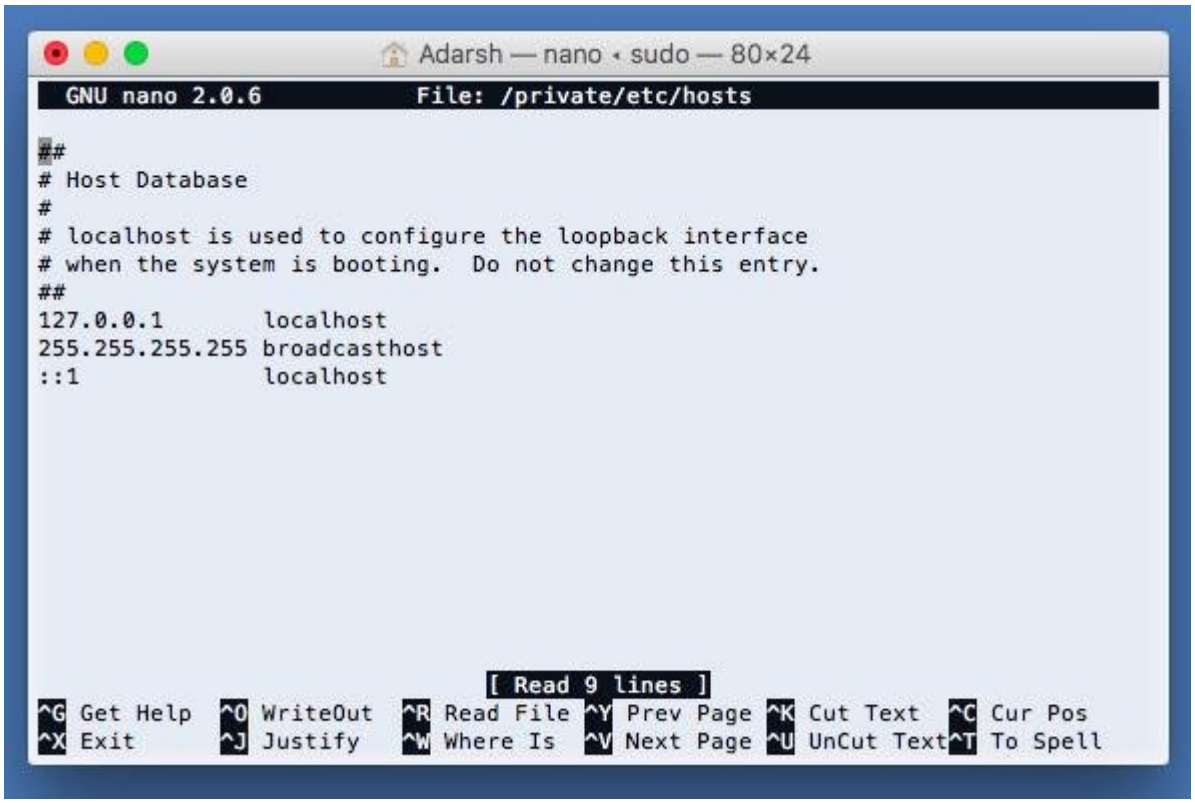
2 - استفاده از افزونه minerBlock برای کروم

افزونه minerBlock هم مانند No Coin یکی دیگر از ابزارهای متن باز است که برای این منظور استفاده می‌شود. این افزونه‌ها لیستی از چند دامین مشهور در این زمینه را به‌کاربر ارائه می‌دهند. این لیست دائما در حال افزایش است.



3 - بلاک دامین‌های ماینینگ کوین در فایل hosts

برای جلوگیری از ماینینگ کوین می‌توانید به‌صورت دستی هم عمل کنید. با این کار، مرورگر نمی‌تواند به‌این دامین‌ها وصل شود. می‌توان فایل hosts را ویرایش و آدرس آن‌را به 0.0.0.0 دایرکت کرد.



اگر از لینوکس استفاده می‌کنید با استفاده از دستور زیر فایل hosts را باز کنید و به‌آخر فایل ،coin-hive.com 0.0.0.0 را اضافه کنید:

sudo nano /etc/hosts

در لینوکس این دستور را اجرا کنید:

sudo nano /private/etc/hosts

در سیستم‌عامل ویندوز، به‌مسیر C:\Windows\System32\drivers\etc بروید تا 0.0.0.0 ،coin-hive.com به‌آخر فایل hosts اضافه کنید.

4 - دامین‌ها را در ad Blocker بلاک کنید

افزونه‌های بلاک تبلیغات مانند AdBlock هم می‌توانند جلوی ماینینگ کرپیتوکارنسی را بگیرند. با توجه به‌نوع مرورگری که استفاده می‌کنید می‌توانید با دست‌کاری در تنظیمات آن، جلوی اتصال به این وبسایت‌ها را بگیرید. به‌عنوان مثال، برای پیدا کردن AdBlock در کروم وارد لیست افزونه‌ها شوید و AdBlock را پیدا کنید. بعد به‌دنبال Customize > Block an ad by its URL بگردید. سپس، این متن را در جعبه متن وارد کنید:

https:\\coine-hive.com\lib\coinhive.min.js

مطلب پیشنهادی

پرونده ویژه بیت‌کوین
مراحل اجرای تراکنش‌های بیت‌کوین

5 - برای فایرفاکس از NoScripts استفاده کنید

برای فایرفاکس از افزونه‌های بلاک جاوااسکریپت مانند NoScript استفاده کنید. قبل از استفاده از آن، بهتر است بدانید که با یک افزونه خیلی قدرت‌مند و تهاجمی روبر هستید و هر سایتی که این اسکریپت‌ها را اجرا کند از لیست شما خارج می‌شود.

آیا بهتر است جلوی کریپتوکارنسی ماینینگ را بگیریم؟

پاسخ این سئوال به‌وبسایتی بستگی دارد که از استخراج کننده کریپتو استفاده می‌کند. زمانی‌که وبسایت در همان پنجره شروع به‌اخطار کرد خودتان تصمیم بگیرید که به‌بازدید از سایت ادامه دهید یا خیر. هم‌چنین به‌میزان توانی که پردازنده استفاده می‌کند توجه داشته باشید.

منبع:
فوس‌بایتس
تاریخ انتشار:
17 مهر 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/world/10059/%D8%A2%DB%8C%D8%A7-%D8%A7%D8%B2-%D9%BE%D8%B1%D8%AF%D8%A7%D8%B2%D9%86%D8%AF%D9%87-%D8%B4%D9%85%D8%A7-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D8%B3%D8%AA%D8%AE%D8%B1%D8%A7%D8%AC-%D8%BA%DB%8C%D8%B1%D9%82%D8%A7%D9%86%D9%88%D9%86%DB%8C-%D8%A8%DB%8C%D8%AA%E2%80%8C%DA%A9%D9%88%DB%8C%D9%86-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D8%AF%D8%9F-5-%D8%B1%D8%A7%D9%87-

%D8%AC%D9%84%D9%88%DA%AF%DB%8C%D8%B1%DB%8C