بدافزار استخراج رمز ارز

کوین هایو (CoinHive)

مرکزماهر
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

رمز ارز «Cryptocurrency»

رمز ارز یک ارز دیجیتالی است که توسط رایانه تولید می‌شود.

به صورت غیرمتمرکز و بدون نظارت می‌باشد.

تولیدشده از طریق حل مسائل پیچیده ریاضی به نام «**Mining**»

استخراج‌کنندگان در قالب رمز ارز «**Coin**» ایجاد شده پاداش خود را دریافت می‌کنند.

نرم‌افزارهای «**Mining**» از قدرت پردازشگر استفاده می‌کنند. در انتها تمامی مراحل به صورت پشت زمینه و بدون اطلاع کاربر صورت می‌گیرد.

- حملات و بدافزارها در سال 2017 متمرکز بر باج افزارها بوده است.
- گسترش روز افزون رمز ارزها و افزایش قیمت آنها منبع جدید تهدیدات امنیتی و غیره منتظره می‌باشد.
- سال ۲۰۱۷ بدافزارهای شناسایی شده استخراج رمز ارز رشدی معادل **۸۵۰۰** درصد داشته است.
- پیش بینی می شود یکی از چالش های امنیتی در سال های پیش رو، گسترش صعودی بدافزار های استخراج رمز ارز باشد.

کوین هایو «Coin Hive»

- کوین هایو، یک نرم افزار استخراج رمز ارز برپایه جاوا اسکریپت، مبتنی بر مرورگر ارائه می‌دهد.
- استفاده آسان از کتابخانه های جاوا اسکریپت به صاحبان وب سایت این اجازه را می دهد تا با سوء استفاده از بازدیدکنندگان بتوانند از این روش به کسب درآمد بپردازند.

- **عملکرد کوین هایو:**
  - قرار دادن کتابخانه جاوا اسکریپتی کوین هایو در کد HTML وب سایت
  - فراخوانی تابع قرار داده شده و شروع به استخراج، به ازای هر بازدید بدون اجازه کاربر

اثرات مخرب کوین هایو «CoinHive»

- عمل استخراج به شدت منابع کاربر را مصرف می‌کند و می‌تواند عملکرد مرورگر و سیستم عامل را دچار مشکل سازد.
- مرورگر وب بیش از ۵۰% قدرت پردازنده را استفاده می‌کند.
- با وجود اینکه سیستم عامل بیش از حد متعارف کار می‌کند، روند اجرای برنامه ها کند می‌شود.

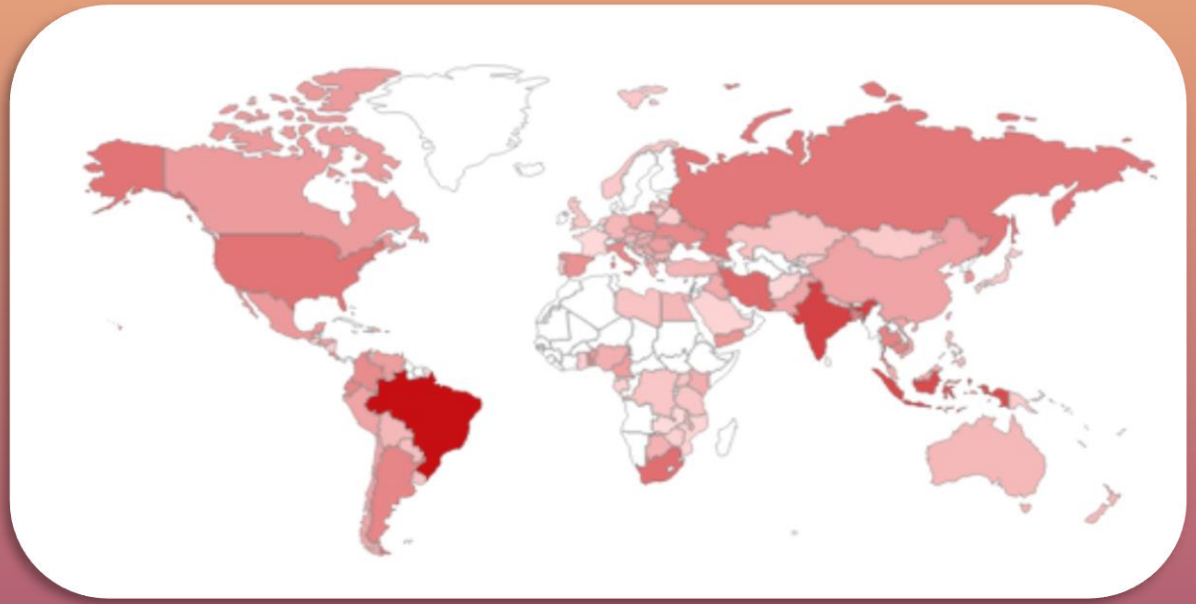
راه های جلوگیری از نفوذ کوین هایو «CoinHive»

- استفاده از آنتی ویروس معتبر
- استفاده از افزونه های مسدود کننده استخراج رمز ارز در مرورگر
- مسدود کردن دستی دامنه های آلوده
- استفاده از AdBlocker

سواستفاده از روترهای میکروتیک با بهره‌گیری از کوین هایو «CoinHive»

- پس از عمومی شدن آسیب پذیری تجهیزات میکروتیک، تعدادی از هکرها شروع به استخراج رمز ارز از دستگاههایی که وصله امنیتی را دریافت نکرده اند نموده اند.
- بیشترین میزان سوء استفاده از ضعف امنیتی روترهای میکروتیک، استخراج رمز ارز با استفاده از تکنولوژی کوین هایو « CoinHive » می‌باشد.
- تعداد روترهای میکروتیک آلوده به کوین هایو « CoinHive » در ایران در زمان تدوین این گزارش ۱۱۳۶۰ دستگاه بوده است.
- این حمله باعث استفاده بیش از حد از پردازنده میکروتیک شده لذا دستگاه قادر به عملکرد صحیح نمی‌باشد.

آلودگی روترهای میکروتیک به کوین هایو «CoinHive»



کشورهای دارای بیشترین آلودگی	تعداد دستگاه
برزیل	81,848
هند	29,265
اندونزی	23,143
ایران	11,360
آفریقای جنوبی	9,170

پنج شهر کشور دارای بیشترین تعداد آلودگی

تهران	۶۰۶
اصفهان	۲۴۴
تبریز	۱۴۴
بوشهر	۸۸
خوی	۴۰

بیشترین سرویس های آلوده

HTTP (8080)	7,736
HTTP	3,624

پنج سرویس دهنده دارای بیشترین تعداد آلودگی در کشور

- پیشگامان توسعه ارتباطات
- مخابرات فارس
- پیشگامان هرمزگان
- آسمان فراز سپاهان