

۲ حمله سایبری به «اتریوم کلاسیک» طی یک هفته؛ میلیون‌ها دلار به یغما رفت - دیجیاتو

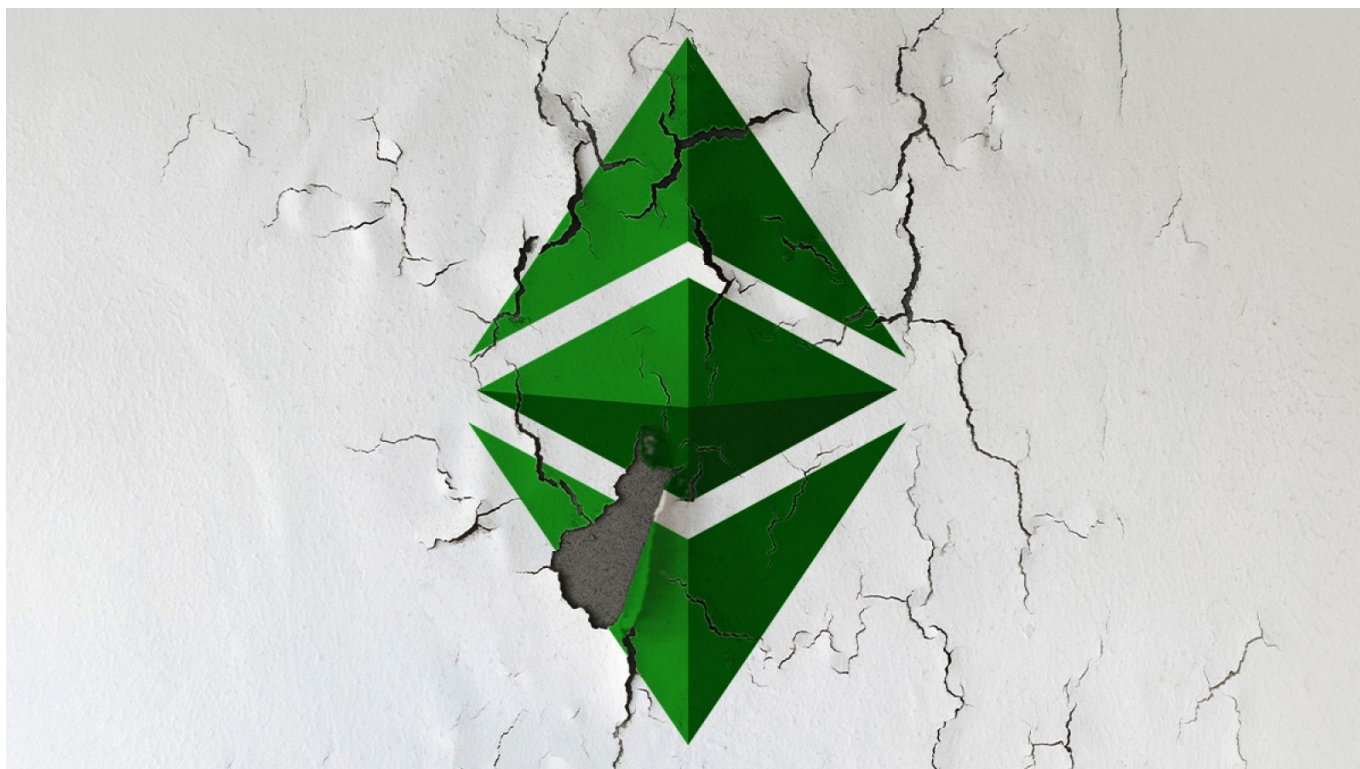
محمد قریشی | یکشنبه، ۱۹ مرداد ۱۳۹۹

هفته گذشته اتریوم کلاسیک با حمله ۵۱ درصد مواجه شد و حالا برای دومین بار، این شبکه مورد حمله مشابه قرار گرفته و حداقل ۴۰۰۰ بلاک بازنویسی شده‌اند.

بر اساس گزارشی که توسط «الکسی استودنوف» از شرکت «Bitquery» [منتشر شده](#)، فرد مهاجم در حمله اول توانسته به ۸۰۷,۲۶۰ اتریوم دست پیدا کند. طبق تخمین این گزارش، هکر ۲۸۰۰ درصد بیشتر از هزینه‌های خود سود بدست آورده است. این فرد با پرداخت ۱۷.۵ بیت کوین به ارزش ۱۹۲ هزار دلار، قدرت هش موردنیاز خود را از «NiceHash» اجاره کرده و توانسته چنین حمله‌ای را انجام دهد. هکر توانسته با استفاده از دو بار خرج کردن، اتریوم سرقت کند یعنی پول پرداخت شده برای کالا یا خدمات دوباره به کیف پول هکر بازگشته است.

حمله ۵۱ درصد یکی از خطرناکترین چالش‌های بلاکچین محسوب می‌شود که طی آن، فرد مهاجم می‌تواند حداقل ۵۱ درصد از قدرت هش را تصاحب کند که نتیجه آن، کنترل شبکه خواهد بود. در حمله دوم مبلغ هنوز مشخص نشده و تنها به بازنویسی بیش از ۴۰۰۰ بلاک اشاره شده است.

گزارش درباره حمله اول با تئوری‌های اولیه که سازماندهی مجدد بلاکچین را غیرعمدی اعلام کرده بودند، مخالف است. این حمله در روزهای دهم و یازدهم مرداد ماه صورت گرفته اما به علت پیچیدگی و همچنین دانش بالا درباره پروتکل اتریوم کلاسیک، تا چندین روز شناسایی نشد. هکر حمله خود را با انتقال اتریوم از کیف پول تحت کنترل خود شروع کرد.



پس از اجاره قدرت هش از NiceHash برای دستیابی به کنترل روی اکثر قدرت هش اتریوم کلاسیک، مهاجم توانست در طی چهار روز ۴۲۸۰ بلاک استخراج کند. هکر پیش از اینکه بلاک‌های شامل تراکنش‌ها را برای سازماندهی مجدد بلاکچین پخش کند، تراکنش‌های خصوصی ایجاد کرد که توسط آن‌ها، اتریوم‌ها را به چندین کیف پول تحت کنترل خود فرستاد.

هکر بیش از ۱۲ ساعت زمان برای انجام معاملات میان صرافی‌ها و چندین کیف پول تحت کنترل خود از طریق زنجیره غیرسازمان یافته صرف کرده است. این فرد توانسته توسط چندین عملیات کوچک در صرافی‌ها، ارزهای دیجیتال سرقتی را تبدیل کند و شناسایی نیز نشود.

این حمله شاهد ۱۱ تراکنش مخرب از یک آدرس درون بلاکچین اتریوم بوده که نتیجه آن‌ها، هکر توانسته ۸۰۷ هزار اتریوم به سرقت ببرد. به اعتقاد Bitquery، کیف پول اصلی احتمالاً توسط OKEx یا یکی از کمپانی‌های وابسته به آن یعنی «Anchain» میزبانی شده است.

[دیجیاتو](#)