کریپتوجکینگ چیست و چگونه انجام می‌شود؟

کریپتوجکینگ یکی از جرایم سایبری است. هکرها و کلاه برداران با این روش سعی می‌کنند تا از سیستم کاربران به عنوان استخراج کننده استفاده نمایند. به دلیل استفاده غیر قانونی از منابع سخت افزاری سیستم افراد دیگر، این کار یک جرم سایبری محسوب می‌شود.

به دلیل استفاده از ارز دیجیتال، کاربران نمی‌توانند چنین هکرهایی را ردیابی کنند. پس کریپتوجکینگ در دسته جرایم سایبری مربوط به دنیای ارزهای دیجیتال قرار می‌گیرد. کریپتوجکینگ را می‌توان به روش‌های مختلفی روی سیستم کاربران پیاده سازی کرد. برای این که از این خطرات در امان باشید، در این مطلب از کیف پول من به معرفی کامل کریپتوجکینگ و راه‌های آلوده شدن سیستم خواهیم پرداخت.

آشنایی مختصر با مکانیک‌های دنیای بلاک چین

قبل از این که به بحث کریپتوجکینگ و نحوه انجام آن بپردازیم، بهتر است با مکانیزم‌های دنیای بلاک چین آشنا شوید؛ چرا که بدون دانستن برخی مفاهیم اولیه شاید به طور کامل مفهوم کریپتوجکینگ را درک نکنید. در دنیای بلاک چین، تراکنش‌ها از دو روش کلی اعتبارسنجی و تایید می‌شود. تنها پس از تایید تراکنش است که ارزهای مورد نظر انتقال می‌یابند. وظیفه اعتبارسنجی و تایید تراکنش‌ها به عهده ماینرها خواهد بود.

برای اعتبارسنجی و تایید یک تراکنش در محیط بلاک چین، ماینرها باید محاسبات ریاضی پیچیده‌ای را انجام دهند و سپس آن را در پایگاه داده بلاک چین ثبت نمایند. انجام چنین فرایندی دشوار بوده و به سخت افزارهای قدرتمند نیاز دارد.

به کاری که ماینرها در هنگام اعتبارسنجی و تایید تراکنش‌ها انجام می‌دهند، استخراج ارز دیجیتال نیز گفته می‌شود. چرا که در هنگام اعتبارسنجی تراکنش‌ها، بلوک جدیدی به لیست بلاک‌های قبلی بلاک چین اضافه می‌شود. به این ترتیب می‌توان گفت اعتبارسنجی روشی برای استخراج ارز دیجیتال است.

در فرایند استخراج بلوک‌های جدید، ماینرها به عنوان پاداش از **بلاک چین**، ارز دیجیتال جدید دریافت می‌کنند. ناگفته نماند که کارمزد تراکنش که توسط کاربران پرداخت می‌شود نیز به ماینرها تعلق می‌گیرد. به همین ترتیب ماینرها می‌توانند از اعتبارسنجی تراکنش‌ها کسب درآمد کنند.

به دلیل ارزش بالای ارزهای دیجیتال، استخراج ارز دیجیتال را می‌توان راه مناسبی برای کسب درآمد دانست. قابل ذکر است که استخراج رمزارز با استفاده از قدرت سخت افزاری تنها برای ارزهایی امکان پذیر است که از روش اثبات کار استفاده می‌کنند. اثبات کار باعث شده تا برای تایید تراکنش‌ها کاربران از قدرت سخت افزاری سیستم خود استفاده نمایند.

کریپتوجکینگ چیست؟

کریپتوجکینگ، همان طور که گفتیم، یک روش کلاه برداری ارز دیجیتال بوده و در دسته جرایم سایبری قرار می‌گیرد. این جرم در دنیای ارزهای دیجیتال انجام می‌شود چرا که این روش کاربرد دیگری ندارد.

کریپتوجکینگ می‌تواند به روش‌های مختلفی انجام شود. در کریپتوجکینگ هکرها ابتدا سیستم کاربران را با روش‌های متفاوت آلوده می‌کنند. در مرحله بعدی، سیستم‌های آلوده شده به سخت افزاری برای استخراج ارز دیجیتال تبدیل می‌شوند. بدین ترتیب اگر سیستمی آلوده شود، به عنوان نود شبکه شناخته شده و ارز دیجیتال را برای هکر استخراج می‌کند.

به خاطر این که استخراج ارزهای دیجیتال کار نسبتا سختی است، برای این که استخراج به درستی انجام گیرد، باید قدرت پردازشی زیادی استفاده شود. به همین خاطر در اکثر مواقعی، سیستم‌هایی که تحت کریپتوجکینگ قرار گرفته‌اند، از لحاظ سخت افزاری دچار مشکل می‌شوند. در کریپتوجکینگ هکرها سیستم کامپیوتری و سخت افزار شما را مورد هدف قرار می‌دهند و از این طریق می‌توانند به **استخراج رمزارز** بپردازند.

دنیای ارزهای دیجیتال که با هدف امنیت به وجود آمده، بعضا شاهد برخی بدافزارها است که می‌تواند امنیت این حوزه را زیر سوال ببرد. البته این نوع از جرم و دزدی در دنیای بلاک چین، چندان رواج ندارد. چرا که استفاده از آن به تایید کاربر و نصب برخی بدافزارها نیاز دارد.

پس تا زمانی که روی هر لینکی کلیک نکرده و هر برنامه‌ای را نصب نکنید، از شر کریپتوجکینگ در امان خواهید بود. البته برای این که سیستم شما تحت کریپتوجکینگ قرار بگیرد، راه‌های مختلفی وجود دارد که در ادامه به آنها می‌پردازیم.

روش‌های مختلف کریپتوجکینگ

برای این که هکرها موفق به کریپتوجکینگ شوند، راه‌های مختلفی وجود دارد. این امر می‌تواند امنیت شما در دنیای مجازی و بلاک چین را به خطر بیاندازد. ابتدایی‌ترین روشی که هکرها برای آلوده کردن سیستم کاربران در نظر می‌گیرند، استفاده از ایمیل است.

مانند روش‌های سنتی، هکرها لینک‌های آلوده یا لینک دانلود برخی بدافزارها را به کاربران زیادی ارسال می‌کنند. زمانی که شما چنین ایمیل‌هایی را باز کرده و روی لینک آنها کلیک کنید، سیستم شما آلوده خواهد شد. در صورتی که روی لینک کنید، یک کد به صورت مخفی در بک گراند سیستم کامپیوتری شما اجرا می‌شود.

پس از این که بدافزار اجرا شد، شروع به **استخراج ارز دیجیتال** می‌کند. بدین ترتیب شاید در عملکرد سیستم کامپیوتری خود تغییراتی را مشاهده کنید. در نظر داشته باشید که شناسایی این که به سادگی انجام نمی‌شود چرا که این کد به صورت مداوم در بک گراند شما اجرا می‌شود.

در روش دوم کریپتوجکینگ، هکرها کدهای مخرب را درون تبلیغات قرار می‌گیرند. تبلیغات بنری بهترین روش برای مخفی کردن کدهای مخرب هستند. در این حالت، به طور معمول از کدهای جاوا اسکریپت استفاده می‌شود. هنگامی که روی یک بنر با کد مخرب کلیک کنید، این کد در مرورگر شما اجرا می‌شود. ذخیره شدن این کد در مرورگر باعث می‌شود تا هر زمانی که مرورگر شما باز شد، کد شروع به کار کند.

به همین دلیل مرورگر تبدیل به دستگاه استخراج کننده هکرها می‌شود. اگر مشاهده کردید که مرورگر شما بدون دلیل منابع سخت افزاری زیادی استفاده می‌کند، امکان دارد کریپتوجکینگ در آن اجرا شده باشد. روش بعدی شاید کمی نامحسوس‌تر باشد اما همیشه در دنیای مجازی کلاه برداری و دزدی از این روش متداول بوده و هکرها از آن استفاده می‌کنند.

مطلب پیشنهادی : بهترین نرم افزار های استخراج ارز دیجیتال

در این حالت، کدهای مخرب درون بازی‌ها و برنامه‌های آنلاین قرار می‌گیرند. این یک راه تبادلی دو طرفه است. هنگامی که از یک بازی یا برنامه رایگان در سایت‌های مختلف استفاده می‌کنید، در قبال دریافت خدمت، قدرت سخت افزاری خود را باید در اختیار نرم افزار قرار دهید.

در این حالت دانسته یا نادانسته قدرت سخت افزار شما برای **استخراج ارز دیجیتال** استفاده می‌شود. البته زمانی که استفاده از سایت را متوقف کنید، استخراج ارز دیجیتال نیز متوقف می‌شود و نمی‌تواند به صورت مداوم از منابع سیستم شما استفاده کند.

برخی سایت ها برای این که مخارج خود را تامین کنند، در هنگام ورود کاربران استفاده از منابع برای استخراج ارز دیجیتال را به کاربران اعلام می‌کنند. آخرین روشی که برای کریپتوجکینگ در دنیای بلاک چین مشاهده شده است، استفاده از کیف پول‌های سخت افزاری و نرم افزارهای رابط است.

در حقیقت، این نرم افزارها تا چندی پیش در فروشگاه هایی مانند گوگل پلی و اپ استور نیز وجود داشتند. با نصب این برنامه، زمانی که شما کیف پول ترزور خود را به سیستم متصل می‌کردید، نرم افزار شروع به دزدیدن ارزهای دیجیتال شما می‌کرد. یا در حالت دیگر، خود برنامه مشغول کریپتوجکینگ می‌شد.

چرا باید با کریپتوجکینگ مقابله کرد؟

جدا از این که کریپتوجکینگ یک جرم سایبری محسوب می‌شود، ضررهای مختلفی نیز برای کاربران در بر دارد. به همین خاطر بهتر است با علم بیشتری در دنیای دیجیتال فعالیت کنید تا دچار این نوع بدافزارها نشوید. در وهله این بدافزارها ناخواسته وارد سیستم کامپیوتری یا حتی گوشی کاربران می‌شود.

در روش بعدی این برنامه ها به صورت مخفی و در پشت پرده یک برنامه ساده از سخت افزار شما استفاده می‌کنند. به همین دلیل هکرها می‌توانند به راحتی به استخراج ارز دیجیتال بپردازند بدون این که کاربران متوجه شوند.

خطر دیگر کریپتوجکینگ، به دستگاه های شما مربوط می‌شود. علاوه بر این که برخی از برنامه های کریپتوجکینگ می‌توانند اطلاعات مهم شما را به سرقت ببرند، در اکثر مواقع به دستگاه شما ضربه می‌زنند. همان‌طور که گفتیم استخراج ارز دیجیتال کار راحتی نیست و به قدرت پردازشی زیادی نیاز دارد.

استخراج ارز دیجیتال با دستگاه های کامپیوتر ساده و گوشی موبایل کار هوشمندانه‌ای نیست و می‌تواند به سخت افزار شما ضربه بزند. به همین دلیلی زمانی که دستگاه های شما مدام مورد سو استفاده قرار بگیرند، احتمال خرابی آنها افزایش پیدا می‌کند.

چگونه می‌توان کریپتوجکینگ را تشخیص داد؟

کریپتوجکینگ یکی از راه‌های پیچیده برای دزدی از کاربران است و نمی‌توان روش مشخصی برای شناسایی آن معرفی کرد. اما کریپتوجکینگ نیز مانند هر روش دیگری نشانه‌هایی دارد. به دلیل استفاده از منابع سخت افزاری دستگاه، می‌توان کریپتوجکینگ را تشخیص داد.

اگر مشاهده کردید که بدون هیچ دلیل منابع سخت افزاری زیادی را مصرف می‌کنید. به طور مثال، پردازنده مرکزی و گرافیکی شما بدون هیچ دلیلی در بیشترین حد خود در حال پردازش است، به احتمال زیاد به کریپتوجکینگ آلوده شده‌اید.

زمانی که سیستم شما پردازش‌های قدرتمندی انجام می‌دهد، به منابع انرژی زیادی نیز نیاز خواهد داشت. به همین دلیل دستگاه‌هایی که دچار کریپتوجکینگ شده باشند، به سرعت باتری خالی می‌کنند یا در برخی مواقع احتمال خاموشی سیستم کامپیوتری به دلیل نیاز به منبع برق قدرتمندتر نیز وجود دارد.

چگونه از کریپتوجکینگ جلوگیری کنیم؟

توصیه می‌کنیم برای **مقابله با کریپتوجکینگ** جلوگیری به جای درمان را انتخاب کنید. به همین خاطر از نصب هر گونه نرم افزار و افزونه مرورگری به شدت خودداری کنید. چرا که این گونه برنامه‌های به احتمال قوی می‌توانند بدافزار باشند. تنها برنامه‌ها و افزونه‌هایی را نصب کنید که تحت تایید تعداد کاربران زیادی باشند. از طرف دیگر برای بررسی کریپتوجکینگ شدن کامپیوتر، بهتر است همیشه استفاده منابع سیستم خود را بررسی کنید.

در حال حاضر برخی افزونه‌های مرورگری به وجود آمده‌اند تا از ورود کدهای مخرب کریپتوجکینگ به سیستم شما جلوگیری کنند. به همین ترتیب می‌توانید چنین افزونه‌هایی را برای در امان ماندن از کریپتوجکینگ نصب کنید. در وهله بعدی بهتر است روی هر تبلیغی کلیک نکرده و در صورت امکان از افزونه‌های مسدود کننده تبلیغات استفاده کنید.