هک بیت کوین چگونه است و آیا باید نگران باشیم؟

نویسنده: امید فدوی

آیا هک کردن بیت کوین امکان پذیر است؟!

هک بیت کوین به دلیل فناوری بلاک چین و بررسی مداوم کاربران از اکوسیستم بیت کوین بسیار دشوار شده است. ولی هکرها می توانند با دستیابی به کیف پول های دیجیتالی صاحبان بیت کوین، دارایی های بیت کوین آنها را سرقت کنند. سرمایه گذاران در سراسر جهان به خرید بیت کوین هجوم آورده اند و برخی دولت ها را وادار می کنند تا مقرراتی را برای معاملات آن وضع نمایند. موفقیت بیت کوین باعث افزایش طرفداران ارز دیجیتال شده و درصدد راه اندازی رمزارزهای جدید بر روی فناوری بلاک چین شده اند. پس از پیدایش بیت کوین در سال ۲۰۰۹ رشد قیمت آن بسیار سریع بوده است. در حالی که در حال حاضر بیش از ۲۰۰ نوع ارز دیجیتال دیگر منتشر شده است، همواره بهای بیت کوین با فاصله بسیار زیاد از رمزارزهای دیگر در رتبه نخست قرار داشته است.

رشد سریع بهای بیت کوین باعث شده که سرمایه‌گذاران و تریدرهای ارز دیجیتال رغبت زیادی به خریداری و ذخیره بیت کوین از خود نشان دهند. هر چه اکوسیستم بیت کوین گسترده تر می شود حفظ امنیت این شبکه بیشتر مورد توجه قرار می گیرد. بازار پر رونق بیت کوین باعث شده توجه هکرها یا همان افرادی که به دنبال نفوذ در سیستم ها، و سرقت اطلاعات و یا دارایی های اشخاص هستند، برای هک بیت کوین بیشتر می شود. به همین دلیل بیشتر کاربران این شبکه همواره در اندیشه مسئله ایمنی و سپس مقابله با هک بیت کوین هستند. با توجه به علاقمندی روز افزون کاربران تازه‌کار برای ورود به عرصه معاملات بیت کوین، برای آشنایی هر چه بیشتر مبتدیان با ریسک های این معاملات پرسود، در این مقاله ارز دیجیتال به تشریح شیوه های مختلف حملات احتمالی جهت هک بیت کوین می پردازیم.

هک شدن بیت کوین چطور اتفاق می افتد؟

لینک دانلود ویدیو با کیفیتHD

فهرست مطالب

منظور از هک بیت کوین چیست؟

از زمان توسعه بیت کوین، مسئله برخورداری از ایمنی تاکنون یک موضوع اساسی برای این اکوسیستم بوده است. از یک طرف، هک بیت کوین بسیار دشوار است و این بیشتر به دلیل فناوری بلاک چین blockchain است که پشتیبانی بیت کوین را برعهده دارد. از طرف دیگر به دلیل بررسی مداوم بلاک چین توسط کاربران بیت کوین احتمال هک بیت کوین بعید است

منظور از هک بیت کوین یا hacking bitcoin نفوذ یا رخنه به سیستم های کامپیوتری بیت کوین برای سرقت ذخیره های بیت کوین کاربران شبکه آن می باشد. در واقع عمل هک کردن به معنای رخنه به سیستم کامپیوتر و به کاربردن روش سریع، ماهرانه و هوشمندانه برای حل مشکلی در کامپیوتر بوده است، اما در مباحث امروزی، اصطلاح نفوذ به یک کامپیوتر و سرقت اطلاعات و داده های مالی کاربر کامپیوتر، هک کردن نام گرفته است.

به طور معمول هکرها جهت نفوذ یا رخنه در یک سیستم، از طریق شبکه اقدام می کنند. مدیریت هر شبکه کامپیوتری متمرکز بوده و برعهده کامپیوتر قدرتمند مرکزی یا همان سرور server می باشد. هکرها به این سرور مرکزی حمله کرده و توسط نفوذ به آن به دستکاری اطلاعات آن پرداخته و با تغییر سیستم دیتا، سعی در بهره بردن از آن داده‌ها به نفع شخصی و یا جهت اهداف خاص دارند.

اکوسیستم بیت کوین به دلیل آنکه تحت حمایت بلاک چین می باشد از یک شبکه غیرمتمرکز بهره مند است. بیش از میلیون ها ماینر در سراسر جهان به استخراج بیت کوین مشغول هستند، به همین دلیل هکرها برای نفوذ به شبکه بیت کوین، به جای آنکه یک سرور متمرکز را هک کنند، لازم است به یک شبکه غیرمتمرکز نفوذ نمایند.

امکان هک کردن یک شبکه گسترده با حجم عظیمی از ماینرها کار را برای هکرها بسیار مشکل و شاید غیر ممکن ساخته است.

این مطلب هم میتونه کمک تون کنه: آیا سایت های کلود ماینینگ برای سرمایه گذاری مناسب هستند؟

حمله به شبکه بیت کوین چگونه انجام پذیر است؟

تولید کوین های بیت کوین بر اساس تکنولوژی بلاک چین و به روش غیرمتمرکز انجام می گردد. به آن معنی که در شبکه تولید بیت کوین هیچ کامپیوتر متمرکز یا server وجود ندارد که هکرها بتوانند از آن برای نفوذ به شبکه دسترسی داشته باشند

با این شرایط یکی از مزایای بیت کوین و دیگر آلتکوین ها در قیاس با ارزهای سنتی یا فیات، ایمنی در مقابل حمله هکرها می باشد

درست است که شبکه بلاک چین محافظ بر بیت کوین از نوع گسترده و غیرمتمرکز است و باعث می گردد تا حد زیادی از حملات هکرها در امان باشد، ولی این کار امنیت کامل و ۱۰۰درصدی را برای این اکوسیستم فراهم نمی کند. حتی از نظر تئوری هم حمله هکرها به بیت کوین امکان پذیر است، چنانکه در عمل نیز تاکنون شاهد حملاتی به شبکه بیت کوین بوده ایم

بعضی از این حمله ها را می توان در گروه حمله های رسانه ها به این بازار مالی دسته بندی کرد و بعضی دیگر به صورت محدودیت ها و ممانعت هایی بوده که قانون‌گذاران بر سر راه شبکه بیت کوین گذاشته اند.

ولی آیا هک بیت کوین از نظر سایبری و حمله به زیرساخت ها و ساختار شبکه بیت کوین نیز انجام پذیر بوده است؟

در ادامه به برخی از حمله های سایبری که علیه شبکه بیت کوین انجام گرفته اشاره می شود.

آیا حمله روز صفر علیه شبکه بیت کوین انجام گرفته است؟

حمله روز صفر یا Zero-day attack، یک نوع آسیب پذیری است که به صورت بالقوه در یک نرم افزار وجود دارد. ممکن است تولید کننده و توسعه دهنده نرم افزار از وجود آن مطلع نباشد ولی از طریق یک نقطه ضعف بالای امنیتی راه نفوذی را برای آن به وجود آورده است. هکر از این نقطه ضعف سوء استفاده کرده و حمله خود به نرم افزار را به انجام می رساند

مرسوم ترین حمله روز صفر، مربوط به اینترنت اشیاء یاIoT می باشد. منظور از اینترنت اشیا شبکه ای از اشیا و دستگاه هایی است که به شبکه جهانی اینترنت وصل می شوند و از طریق اپلیکیشن های موجود در گوشی های هوشمند نظارت و کنترل می گردند

احتمال دارد که هکرها بتوانند حمله سایبری روز صفر را به منظور خراب کردن یا ضعیف نمودن شبکه بیت کوین انجام دهند. البته حمله روز صفر، علیه بیت کوین فقط یک تهدید نبوده و در واقعیت نیز در تاریخ ۱۵ آگوست ۲۰۱۰ رخ داده است. این حمله را حادثه سرریز ارزش یا Value Overflow Incident نامیده اند.

این مطلب هم میتونه کمک تون کنه: آموزش کار با نوبیتکس به صورت قدم به قدم

ادثه سرریز ارزش در مورد شبکه بیت کوین چگونه اتفاق افتاد؟

از آنجا که نرم افزار بلاک چین منبع باز یا اپن سورس است، کاربران امکان وارسی آن را دارند. در ۱۵ آگوست ۲۰۱۰ حدود ده سال پیش یکی از معامله گران بیت کوین در انجمن گفتگوی بیت کوین اعلام کرد که بلوک ۷۴۶۳۸ شامل معامله ای است که تعدادی بیت کوین را برای سه آدرس مختلف ایجاد کرده است که ارزش آن بیشتر از ۹۲ میلیارد بیت کوین بوده است.

این به عنوان یک حادثه سرریز ارزش قلمداد می شود زیرا پس از وارسی‌های زیاد تشخیص داده شد یک هکر توانسته در طی چند لحظه کوتاه، بیشتر از ۱۸۴ میلیارد بیت کوین منتشر کند. در کد اصلی فقط تولید ۲۱ میلیون بیت کوین پیش بینی شده، لذا این هکر توانسته بیش از ۸۷۰۰ برابر تمامی بیت کوین ها، کوین تقلبی وارد اکوسیستم بیت کوین نماید

در آن زمان واکنش سریع ساتوشی ناکاموتو، بنیان گذار اولیه و ناشناس بیت کوین با همکاری گوین آندرسن توانست شبکه را پس از سه ساعت درگیری با این عارضه،اشکال زدایی کند. آنها به سرعت بروزرسانی گسترده ای در شبکه انجام داده و تمامی بیت کوین های استخراج شده را از بین بردند.

جالب است که طی چند ساعت بعد از انجام بروزرسانی توسط ناکاموتو، دو شبکه بیت کوین با هم در حال کار بودند و عده زیادی از ماینرها در حال استخراج کوین برای زنجیره مشکل دار بودند. ولی آنچنانکه ناکاموتو ادعا کرد، تنها نوزده ساعت پس از این حادثه، همه ماینرها توانستند شبکه معیوب را رها کنند و وارد چرخه تولید شبکه جدید گردند.

دست اندرکاران بر این باورند که این حمله در همان روزهای ابتدایی خلق بیت کوین، بهترین موهبتی بود که برای این ارز دیجیتال اتفاق افتاد. زیرا در همان روزهای اولیه متوجه این ایراد نرم‌افزاری شدند و حمله را متوقف کردند. تصور کنید این ماجرا چندین سال بعد آشکار می شد، در آن زمان که ارزش بیت کوین برابر با چند هزار دلار شده، و بهای بازار بیت کوین به چند میلیارد دلار میرسید، امکان داشت که به یکباره قیمت بیت کوین در مدتی کوتاه به نزدیک صفر برسد.

نحوه حملات اسپم به شبکه بیت کوین چگونه است؟

جهت آسیب رساندن به شبکه زنجیره ای بیت کوین روش های مختلفی وجود دارد. اینها از انواع حمله هایی هستند که می توانند سرعت شبکه را کم کنند و یا باعث کم شدن اعتبار بیت کوین گردند.

این نوع آسیب ها از نوع هک بیت کوین نیستند ولی انواع مختلفی دارند که در ادامه توضیح داده می شود. حملات اسپم بیشتر به نرم افزارهای ارتباط جمعی بر می گردد که در آن تعداد بسیار زیادی از پیام های ناخواسته به کاربران ایمیل، سوشیال مدیا و دیگر پیام رسانها ارسال می گردد. در مورد شبکه مرتبط با بیت کوین این پیام های ناخواسته باعث کند شدن سیستم های استخراج بیت کوین می گردد.

هدف از این کار دلسردی کاربران از بیت کوین و متمایل کردن ایشان به استخراج دیگر آلتکوین ها می باشد. در کد منبعِ بیت کوین، راه حلی که جهت رفع این مشکل عرضه شده این است که تراکنش های با کارمزد صفر در این شبکه قابل قبول نیستند و رد می‌شوند.

حال اگر بخواهند از طریق انتشار اسپم به بیت کوین حمله کنند، باید برای این حجم زیاد از تراکنش ها، کارمزدهای مناسبی ثبت گردد که این کار برای توزیع کنندگان اسپم، توجیه اقتصادی نخواهد داشت. یک راه حل که توزیع کنندگان اسپم از آن میتوانند برای بالا بردن هزینه اسپم استفاده کنند، این است که روشی را اتخاذ کنند که ماینرهای زیادی برای اسپمرها spammers کار کنند، در اینصورت سود به دست آمده از طریق استخراج، اسپم ها را به عنوان کارمزد در نظر می گیرند.

ولی در عمل چنین اتفاقی نیفتاده است، به دلیل آنکه در پروسه حمله اسپم ها، سرعت شبکه به شدت کم می شود و در مقابل آن کارمزد تایید تراکنش افزایش می یابد. این دو عامل یعنی سرعت کم و کارمزد زیاد می‌تواند باعث سقوط شدید بهای بیت کوین شود.

با کم شدن قیمت بیت کوین، پاداش استخراج آنقدر کم می شود که دیگر انجام ماینینگ صرفه اقتصادی نخواهد داشت. در این راستا اگر ماینری که برای توزیع اسپم مشارکت می‌کند، قادر به تامین هزینه‌های مالی اسپم نباشد، حمله اسپمر به شکست می انجامد.

این مطلب هم میتونه کمک تون کنه: BEP2 چیست و چه تفاوتی با ERC20 دارد؟

منظور از حمله ۵۱ درصدی چیست؟

زمانی که گروهی از ماینرها برای کسب بیشترین نرخ هش در اکوسیستم بیت کوین شروع به استخراج یا ماینینگ بیت کوین می کنند، لازم است میزان انرژی بالایی را فراهم کنند تا بتوانند توان پردازش تمامی سیستم ها را فراهم کنند. انرژی تامین شده بایستی از مجموع انرژی مصرفی برای همه دستگاه های استخراج بیت کوین بیشتر باشد. این شرایط حمله پنجاه و یک درصد یا ۵۱٪ attack نامیده می شود.

بنابراین، فردی که بخواهد حمله ۵۱ درصدی را انجام دهد، بایستی نرخ هشی برابر با نرخ هش فعلی زنجیره انتشار بیت کوین را دارا باشد. هم اکنون تعداد ماینرهای بیت کوین در سراسر جهان خیلی زیاد شده و ماینرهای تولید بیت کوین هر روز قدرتمندتر می گردند. بنابراین نرخ هش شبکه به وضوح بالا رفته است.

گرچه از لحاظ تئوری حمله ۵۱ درصدی به بیت کوین امکان پذیر است، ولی در حال حاضر با این توان شبکه، حمله ای در این ابعاد امکان نخواهد داشت. زیرا برای انجام چنین حمله ای میزان انرژی و پولِ بسیار زیادی لازم است. اگر فردی بتواند بر پنجاه و یک درصد شبکه بیت کوین مسلط باشد، احتمال اینکه یک کوین را دو بار به کار گیرد و یا از انجام تراکنش‌ها ممانعت به عمل آورد، وجود خواهد داشت.

به هر حال اگر حمله ۵۱ درصدی صورت گیرد، باز هم نخواهد توانست هک بیت کوین را انجام داده و شبکه را به نابودی کامل برساند. زیرا این فرد قادر نیست تراکنش هایی که در گذشته تایید شده اند را کنسل کند، تراکنش های جعلی ایجاد نماید، کوین هایی را از یک آدرس خاصی سرقت کند و یا کوین‌های جدیدی را استخراج نماید.

آیا هک بیت کوین از طریق کیف پول امکان پذیر است؟

از مطالب فوق دریافتیم که هک بیت کوین از طریق شبکه بلاک چینِ پشتیبان این ارز دیجیتال، در عمل امکان پذیر نمی باشد. ولی اپلیکیشن هایی که کاربران روی گوشی هوشمند خود نصب می نمایند، از جمله کیف پول بیت کوین و صرافی ارز دیجیتال امکان هک شدن را دارد.

چند صرافی بزرگ از جمله بایننس تا کنون از سوی هکرها مورد حمله واقع شده اند. به جز حمله به صرافی ها، هکرها همچنین روش هایی مانند فیشینگ را برای سرقت از ولت های بیت کوین به کار می برند.

اگر فردی بتواند همزمان به کلید خصوصی private key و کلید عمومی Public Key وَلت شما دستیابی پیدا کند، قادر خواهد بود که به تمام دارایی های آن کیف پول دست درازی کند. تاکنون مواردی از سرقت دارایی های ولت های آنلاین بر روی گوشی هوشمند و به خصوص ولت های تحت وب مشاهده شده است.

البته ولت های سخت افزاری دارای امنیت بسیار بالایی بوده و مسئله هک بیت کوین از طریق آنها امکان پذیر نیست.

تا کنون مواردی از هک شدن ولت و یا صرافی گزارش شده و اخباری در رابطه با این حملات و سرقت ارزهای دیجیتال در رسانه ها دیده شده است. ولی نکته مهم آن است که هک شدن صرافی و یا ولت به معنای هک بیت کوین و نفوذ به شبکه بلاک چین نمی باشد، همانگونه که بارها وبسایت هایی هک شده اند ولی شبکه جهانی اینترنت قابل هک شدن نیست.

این مطلب هم میتونه کمک تون کنه: کاربرد رمزنگاری cryptography در ارزهای دیجیتال چیست؟

جمع بندی مطالب ارائه شده:

حفظ ایمنی شبکه بیت کوین از مسائل اصلی میان کاربران شبکه بلاک چین است. این شبکه با وجود آنکه از امنیت زیادی بهره مند است ولی حملاتی جهت هک بیت کوین مشاهده شده است.

اولین و به احتمال زیاد آخرین حمله موفقیت آمیز در این رابطه که در سال ۲۰۱۰ اتفاق افتاد به حادثه سرریز ارزش مشهور است. ولی در طول یک دهه سابقه انتشار بیت کوین، به جز این مورد خاص، زنجیره بلاک چین بیت کوین توانسته ایمنی خود را در مقابل هجوم هکرهای سایبری به خوبی حفظ نماید.

تاکنون حملات موفقی از سوی هکرها به وَلت ها و صرافی های بیت کوین انجام شده ولی هیچ آسیبی به اکوسیستم بیت کوین و شبکه بلاک چینِ آن وارد نشده است. اگر ضعف امنیتی نیز وجود داشته در پلتفرم ها و اپلیکیشن هایی بوده که با بیت کوین در ارتباط بوده اند.

همیشه امکان دارد حملات گوناگونی از قبیل حمله پنجاه و یک درصدی و یا حمله اسپم در مقابل اکوسیستم بیت کوین اتفاق بیفتند. درست است که این حملات از نظر تکنیکی هک بیت کوین حساب نمی‌گردد ولی با کاهش سرعت در مبادلات می‌تواند اعتبار شبکه را خدشه دار نماید.

سوالات متداول:

آیا هک بیت کوین امکان پذیر است؟

در ده سال گذشته ارز دیجیتال به دنبال آن است که جایگاه خود را در بازارهای مالی گسترش دهد ولی دو گروه در پی هک بیت کوین هستند. یکی گروه های مخالف با تمرکززدایی از بازار ارز که در پی بی اعتبار نشان دادن بیت کوین و سایر آلتکوین ها هستند و گروهی دیگر که در این بازار مالی به دنبال کسب سود بیشتر از طریق هک کردن ارزهای دیجیتال می باشند

تاکنون به غیر از یک مورد از هک بیت کوین در مفهوم نفوذ به شبکه بلاک چین، مورد دیگری دیده نشده است. البته آن مورد نیز مر بوط به حمله روز صفر بوده که به سرعت اشکال زدایی گردید.

این مطلب هم میتونه کمک تون کنه: آیا بیت کوین در ایران قانونی است یا غیرقانونی؟

آیا امنیت کامل در اکوسیستم بیت کوین برقرار است؟

شبکه بلاک چین بیت کوین از امنیت زیادی برخوردار می باشد ولی مواردی از هک شدن پلتفرم ها و اپلیکیشن های مرتبط با شبکه بیت کوین مشاهده گردیده است. جهت مقابله با این مشکل، به کاربران بیت کوین امکاناتی داده شده که بتوانند امینت کیف پول خود را برقرار نمایند.

البته حملات سایبری به بیت کوین رو به فزونی است و مقدار زیادی از توکن ها در مبادلات ارزی به سرقت می روند. دلیل این امر هم آن است که هر روز به تعداد کاربران بیت کوین افزوده می گردد.

جان کانتر، یکی از توسعه دهندگان پروژه بیت کوین و لایتنینگ شبکه ، در توییتی در ۱۹ ژوئن ۲۰۲۰ اعلام کرد که با وجود موفقیت در هک کردن کیف پول بیت کوین، اطمینان داد که شبکه بیت کوین هنوز ایمن و قابل اطمینان است.

روش های حفاظت از ایمنی اپلیکیشن های بیت کوین کدامند؟

حفظ ایمنی ولت بیت کوین دارای اهمیت بسیار زیادی می باشد، به دلیل آنکه اگر کیف پول مورد هجوم هکرها قرار گیرد، ممکن است تمامی سرمایه ای را که ذخیره کرده از دست بدهد.

یکی از ساده ترین روش ها برای تامین امنیت کیف پول حفظ رمزهای ورودی کیف پول، در محلی امن است. البته سایت هایی نیز وجود دارند که نگهداری این امنیت را برای صاحبان کیف پول فراهم می کنند.

هنگامی که می خواهید با اکانت کاربری خود کار کنید، فقط باید با رمزعبور وارد شوید و سوال امنیتی دیگری پرسیده نمی شود. بنابراین اگر احیانا هکری به کیف پول صاحب آن وارد شود ممکن است کاربر متوجه ورود هکر نشود.

البته برخی از اپلیکیشن ها تایید دو فاکتوری را برای ورود به کیف پول الزامی نموده اند که سطح ایمنی را بالاتر می برد.

نحوه کار هکرها جهت هک بیت کوین چگونه است؟

هنگام حمله هکرها به حساب کیف پول کاربر، ارزهای کیف پول را با سرعت زیاد سرقت کرده و آنها را برای مبادله به صرافی یا کیف پول های دیگر منتقل می کنند.

بنابراین در صورت وقوع حمله اگر صاحب ولت مورد هجوم سایبری قرار گیرد، امکان دستیابی دوباره به دارایی های خود نخواهد داشت. زیرا معادلات مربوط به خریداری یا به فروش رساندن کوین ها و توکن های به سرقت رفته، از طریق بلاک چین ها یا صرافی ها انجام می گردد.

بنابراین نمی توان به تراکنش های انجام شده از طریق بلاک چین های قابل اعتماد دسترسی پیدا کرد، زیرا تمامی آدرس ها از سیستم های ایمنی خارجی پنهان می گردند.

صاحبان کیف پول می دانند که بیت کوین های دزدیده شده امکان بازگشت به ولت آنها را ندارند و لازم است تا آخرین حد امکان امنیت کیف پول بیت کوین خود را برقرار کنند.

منابع:

https://www.investopedia.com/
https://cointelegraph.com/news/