



منتشر شده توسط

نویسنده: پویا علیخانی

کوین ایران



ایمیل نویسنده: pouya_8283@yahoo.com

کوین ایران بزرگترین پایگاه خبری فارسی زبان در حوزه فناوری بلاکچین، ارزهای رمزنگاری شده و پلتفرم های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیوند و آرش محبوب، با هدف اطلاع رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه مند به رمز ارزها راه اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید. هدف کوین ایران از معرفی این فناوری ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com



- بیت کوین چگونه هک می شود؟
- دزدی های تاریخی بیت کوین و آلتکوین ها کدام اند؟
- چطور رمز ارز های خود را در امنیت بالا نگه داریم؟

مقدمه

شاید وقتی که Satoshi در سال 2009 و برای اولین بار، بیت کوین را در مقاله خود معرفی می کرد، فکرش را هم نمی کرد که رشد و توسعه این پول مجازی بعد از هشت سال، تا این اندازه باشد. بیت کوین، بازار نابی ایجاد کرد که سلطه دولت ها و دلالان را به چالش کشید و سیستم نظارت مرکزی را زیر سوال برد. با وجود ویژگی های مثبت زیادی که برای بیت کوین و سایر ارز های محبوب دیجیتالی وجود دارد، نگرانی های امنیتی از نخستین سوالات سرمایه گذاران تازه کار و یا حتی کهنه کار است. در این مقاله نگاهی به شیوه های هک بیت کوین خواهیم داشت؛ سپس، برخی از معروف ترین هک های بیت کوین را مرور می کنیم و در آخر، توصیه های امنیتی برای داشتن کیف پول امن را بررسی خواهیم کرد.



و اما، هک بیت کوین چگونه اتفاق می افتد؟

پرسود ترین دزدی هایی که از بیت کوین اتفاق می افتد، مربوط به سرویس های آنلاین است که کد های مخفی مربوط به تعداد زیادی کاربر در آن ها، ذخیره شده است (مثل کاری که Sheep Marketplace انجام داد). به نظر



می رسد که حملات هکری، بیشتر توسط افراد خودی در این شرکت ها، اتفاق افتاده است؛ کسانی که چندان هم هکر های ماهری نبوده اند، اما به کد های مخفی کاربران، دسترسی داشته اند. با کپی کردن این کد ها می توان کنترل مبادله بیت کوین ها را در دست گرفت و به هر آدرس مورد نظری، انتقال داد.



اکنون، فرد مورد نظر دارای مقدار زیادی بیت کوین است. البته فرآیند دزدی هنوز کامل نیست و مرحله بعد، اعمال پول شویی است؛ به این صورت که باید با استفاده از یک mixer یا tumbler، این حجم زیاد از بیت کوین را به مقادیر کوچک، خرد کرد و آن را به طور رندوم، وارد مبادله با سایر کاربران کرد. در نهایت، حساب پاکي وجود دارد که مقادیر زیادی بیت کوین دارد. در صورتیکه فرد هکر اقدام به مبادله مقدار زیادی بیت کوین کند، گردانندگان بلاکچین آن را رصد و بر ملا خواهند کرد.

با اینکه بیت کوین ویژگی هایی دارد که آن را برای دزدی، ایده آل می سازد، ویژگی هایی نیز دارد که برای هکر ها، اصلا خوب نیست. در اصل، بلاکچین یک ابزار عمومی است که هر کسی می تواند ببیند که کوین ها به کدام کیف پول، منتقل می شوند. بنابراین، با رد پایی که یک هکر از خود به جا می گذارد، حتی اگر در لحظه امکان آشکار سازی مسیر انتقال بیت کوین مشخص نباشد، در آینده، قابل ردیابی است.

راه دیگر برای هک بیت کوین، داشتن نام و شماره تلفن فردی با کیف پول پر از بیت کوین است. محققان به تازگی نشان داده اند که می توان با استفاده از نام و شماره موبایل یک فرد، حساب کاربری گوگل وی را هک کرد و برای دسترسی به حساب های بانکی یا بیت کوین شخص، مورد سو استفاده قرار داد. برای این کار، نخست با استفاده از یک شماره تلفن و Gmail برای یافتن حساب کاربری شخص قربانی استفاده کردند.

سپس رمز عبور مربوط به حساب مربوطه را reset کردند و با رخنه ایجاد شده در سیستم سیگنالینگ SS7 و دسترسی به پیام های SMS، به کد فرستاده شده به تلفن همراه آن فرد، دسترسی پیدا کردند. سپس، همین کار را برای بازیابی حساب Coinbase مورد نظر، انجام دادند که در نهایت توانستند به حساب آنلاین فرد قربانی، دسترسی پیدا کنند. [برای مشاهده کامل این خبر، اینجا را کلیک کنید.](#)



در نهایت، راه سومی برای هک بیت کوین وجود دارد که فیشینگ نیزه ای یا (spear phishing) نامیده می شود. در این روش، هکر ها خود را به جای افراد دیگری جا می زنند و سعی در فریب قربانی و دریافت اطلاعات ورود به حساب کاربری دارند. به طور مثال، اخیرا هکر های کره شمالی با چنین روشی تلاش کردند تا خود را به عنوان متخصصان امنیت شبکه جا بزنند و از طریق ایمیل های حاوی بدافزار، به اطلاعات کاربری کارمندان چند صرافی در کره جنوبی،

دست یابند. هکر ها در تلاش برای رخنه در سیستم تایید دو مرحله ای در تلفن های هوشمند کارمندان هدف حمله بودند؛ با این حال به گفته پلیس، شکست خوردند. [برای مشاهده این خبر به صورت کامل، اینجا را کلیک کنید.](#)

نگاهی به دزدی های تاریخی بیت کوین و آلتکوین ها

محل مورد حمله	تاریخ	مبلغ سرقت شده	نحوه سرقت
1- صرافی Mt Gox	ژانویه 2014	850000 بیت کوین	هک اطلاعات یک حسابرس، دسترسی به سیستم خرید و فروش بیت کوین، فروش بیت کوین ها به ارزش میلیون ها دلار
2- صرافی Bitfinex	آگوست 2016	119756 بیت کوین	ایجاد رخنه امنیتی، دزدی از حساب کاربران، تایید غیر قانونی تراکنش ها توسط بخش تامین امنیت Bitfinex
3- هاست Linode	مارس 2012	46703 بیت کوین	رنه به اطلاعات ادمین و دسترسی به درگاه های تبادل بیت کوین مثل Bitcoinica، Slush و غیره. بیت کوین در این زمان، حدود 5 دلار ارزش داشت. هکر ها با بهره بردن از یک ضعف امنیتی در هاست Linode، موفق به سرقت 46700 بیت کوین شدند که 43000 واحد آن، در اکسچنج Bitcoinica نگهداری می شد. این اکسچنج پیش تر نیز هک شده بود و در ماه می همین سال، 18000 بیت کوین از دست داد.
4- صرافی Bitstamp	ژانویه 2015	19000 بیت کوین	دزدی از کیف پول آنلاین اتفاق افتاد. با این حال مسئولان گفتند که این مقدار، تنها کسری از مقدار کل بیت کوین صرافی است و بخش بزرگی از پول به صورت ذخیره سرد (آفلاین) و در امنیت کامل، نگهداری می شود.
5- صرافی Bter	فوریه 2015	7000 بیت کوین	سرویس ارائه میزبانی وب Bter مغلوب حملات هکری شد.



هک های تاریخی بیت کوین و آلتکوین ها

6-	صرافی Picostocks	نوامبر 2013	6000 بیت کوین	دزدی از کیف پول سخت افزاری و آنلاین اتفاق افتاد و پس از آن، مبادلات از این صرافی، متوقف شد.
7-	کیف پول Inputs.io	نوامبر 2013	4100 بیت کوین	هکر توانست به کد API دسترسی یافته و تعادل بین کیف های پول را مخدوش سازد.
8-	صرافی Mintpal	دسامبر 2014	3894 بیت کوین	با تغییر مدیریت این صرافی، مقدار بیت کوین مذکور دزدیده شد و هرگز بازگردانده نشد. به زعم افراد بسیاری، مظنون این دزدی که Green Alex بود، هرگز به این اتهام محاکمه نشد و تنها به اتهام تجاوز به عنف، دادگاهی شد.
9-	صرافی Kipcoin	فوریه 2015	3000 بیت کوین	به دلیل ضعف امنیتی، هکر در ماه می 2014 به اطلاعات سرور این صرافی دست یافت. اما تا دسامبر 2014 دست به کار نشد و در این تاریخ اقدام به انتقال بیت کوین ها نمود.
10	NiceHash	دسامبر 2017	4700 BTC	این سایت اسلونیایی قربانی حمله پیشرفته هکری شد و در زمان خود معادل 64 میلیون دلار، مورد سرقت قرار گرفت. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.
11-	Supernova	می 2017	107 میلیون دلار	حمله 51٪ به یک استخراج و سرقت هش به نرخ 1000 دلار در دقیقه. کوین مورد سرقت، XVG است. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.
12-	Bitcoin Gold	نوامبر 2017	3.3 میلیون دلار	این واقعه، هک نیست و در حقیقت، یک کلاهبرداری از کابرابی است که می خواستند بیت کوین گلد تازه منشعب شده خود را به دست آورند. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.

این سرقت از کاربرانی انجام شد که از Seed generator های آنلاین استفاده می کردند. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.	4 میلیون دلار	ژانویه 2018	IOTA wallet	-13
این صرافی ژاپنی مورد حمله قرار گرفت و قربانی آن، دارایی NEM کاربران بود. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.	550 میلیون دلار	ژانویه 2018	Coincheck	-14
توکن شبکه Stellar که لومن (XLM) نام دارد، مورد سرقت قرار گرفت. به نظر می رسد حمله از نوع DNS hijacking بوده است. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.	669920 XLM معادل 400 هزار دلار	فوریه 2018	Blackwallet	-15
توکن های متعددی از جمله توکن های بر پایه اتریوم، مورد سرقت قرار گرفتند. جزئیات کامل سرقت را از اینجا مطالعه فرمایید.	40 میلیون دلار	ژوئن 2018	Coinrail	-16





چطور کیف پول خود را امن تر کنیم؟

روشن است که از سرمایه گذاران، انتظار تخصص در زمینه امنیت شبکه و آشنایی با زیر بنای امنیتی صرافی های آنلاین وجود ندارد؛ بنابراین، باید مراقب سرویس های ارائه دهنده آنلاین بیت کوین باشید! بسیاری از صرافی ها که حتی در گذشته هدف حملات هکری قرار گرفته اند، هنوز از زیربنای مطلوب شبکه، برخوردار نیستند و همچنان مستعد بروز هک و دزدی اند. صرافی ها و پلتفرم های حرفه ای و با سابقه را بشناسید و با دقت، محل کیف پول آنلاین خود را تعیین کنید.



- مقادیر کمی از بیت کوین در حد استفاده روزانه، در دسترس موبایل و اینترنت قرار دهید! بقیه را به صورت آفلاین (cold storage)، نگهداری کنید.
- از کیف پول خود back up تهیه کنید.
- گذرواژه ای قوی انتخاب کنید و هرگز آن را فراموش نکنید. رمز عبور خود را به طور مرتب عوض کنید.
- از نرم افزار های شناخته شده و معتبر برای مدیریت گذرواژه های خود استفاده کنید.
- محتوای ایمیل های مشکوک یا ناشناس را هرگز دانلود نکنید.
- از سیستم تایید دو مرحله ای که یکی از آن شامل تایید SMS است، برای حساب گوگل یا کیف پول، استفاده نکنید!
- در غیر این صورت امکان رخنه SS7 و هک شدن حساب کاربری شما وجود دارد.
- به افراد ناشناس اعتماد نکنید و اطلاعات حساب یا حتی ایمیل خود را به آن ها ندهید.



در صورتی که از کیف پول کاغذی استفاده می کنید:

- به هیچ وجه، کلید خصوصی دارایی رمزنگاری شده خود را در هیچ وب سایتی وارد نکنید. (برای اطلاع از موجودی حساب خود، کلید عمومی را در کاوشگر بلاکچین مربوطه، وارد نمایید).
- از کلید های خصوصی، بهتر است یک بار بیشتر استفاده نکنید.

در صورتی که از کیف پول های سخت افزاری استفاده می کنید:

- بک آپ یا واژه های پشتیبان آن را در محل امنی نگه داری کنید.

بیشتر بخوانید:

[کلاهبرداری در لباس پروژه مبتنی بر بیت کوین را چگونه شناسایی کنیم؟](#)

[تلاش برای دو بار خرج کردن بیت کوین کش لو رفت!](#)

[سوء استفاده وب سایت ها از سیستم کاربران برای استخراج + راه مقابله](#)

منابع:

<https://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps>

<https://www.cryptocoinsnews.com/stealing-bitcoin-with-a-name-and-a-phone-number/>

<https://coins.newbium.com/post/655-the-10-biggest-bitcoin-hacks-in-history>

<https://bitcoin.org/en/secure-your-wallet>

