گزارش خبر
NEWSREPORT
کد خبر: ۴۵۲۲۰۲
یکشنبه ۲۳ خرداد ۱۴۰۰ ۱۵:۴۳

قابلیت رهگیری تراکنش‌های ارزهای دیجیتال در کشورهای تحت‌تحریم ؛

تهدید جدی ارزهای دیجیتال برای خریداران ایران

شرکت سایفرتریس (CipherTrace)، فعال در زمینه تحلیل داده و رهگیری تراکنش‌های مرتبط با ارزهای دیجیتال، در گزارش ماه گذشته خود اعلام کرده است بیش از ۷۲,۰۰۰ آدرس IP منحصربه‌فرد ایرانی با بیش از ۴.۵ میلیون آدرس منحصربه‌فرد بیت کوین در ارتباط هستند.

به گزارش خبرنگاران اقتصاد گزارش خبر، طبق این گزارش، شرکت سایفرتریس با نظارت بر آدرس‌های IP مرتبط با کشورهای تحریم‌شده توسط ایالات متحده و بررسی ارتباط آن‌ها با بلاک چین بیت کوین، دریافته است که این آدرس‌های IP ایرانی یا به‌طور مستقیم در تراکنش‌های ارز دیجیتال شرکت داشته‌اند و یا از آنها برای کاوش شبکه‌های بلاک چین (به‌منظور کنترل موجودی آدرس‌های ارزهای دیجیتال) استفاده شده است.
قیمت بیت کوین در آینده/ شرط بندی نجومی روی بیت کوین ۲۰۰ هزار دلاری!
آنچه که در ادامه می‌خوانید، شرح کامل گزارش سایفرتریس درباره الزامات امنیتی مؤسسات مالی، برای جلوگیری از نقض تحریم‌هاست. با وجود لحن ایران‌ستیزانه‌ای که در اغلب بخش‌های این گزارش به کار رفته و همچین استفاده از اصطلاحات فنی غیردقیق، ترجیح دادیم این گزارش را بدون دخل و تصرف و دقیقاً به‌همان شکلی که هست ترجمه کنیم.
بسیاری از آدرس‌های بیت کوین نشان‌دارشده (تگ‌شده)، با چندین آدرس IP ایرانی در ارتباط هستند که این موضوع، احتمالاً نشان‌دهنده استفاده از کیف پول‌های موبایلی متصل به اوپراتورهای مختلف اینترنتی در ایران است. ارائه‌دهندگان خدمات اینترنتی، آدرس‌های IP دستگاه‌های تلفن همراه را پس از هر مرتبه بازنشانی اتصال، تغییر می‌دهند.
این IPها به‌طور مستقیم در بلاک چین قابل‌مشاهده نیستند؛ به این معنی که بانک‌ها، شرکت‌های مرتبط با امور مالی و همچنین صرافی‌های ارزهای دیجیتال، به‌طور مستقیم نمی‌توانند ارتباط بین آدرس‌های بیت کوین و کاربرانی که از کشورهای تحریم‌شده با این آدرس‌ها تعامل دارند را مشاهده کنند.
بعد از قانونی‌شدن استخراج بیت کوین در ایران و اختصاص برق ارزان‌قیمت به فارم‌های ماینینگ، بخشی از فعالیت‌های حوزه ارزهای دیجیتال در این کشور، به استخراج بیت کوین و فروش آن در بازارهای جهانی اختصاص یافته است. در صورتی که ارتباط آدرس‌های حاوی بیت کوین‌های استخراج‌شده با IPهای صاحبان این آدرس‌ها بررسی و ردیابی نشود، در اغلب موارد نمی‌توان تشخیص داد که این دارایی‌ها متعلق به کدام منطقه از جهان هستند.
وقتی صحبت از دورزدن تحریم‌ها با استفاده از ارزهای دیجیتال به میان می‌آید، باید اقداماتی بیش از نظارت بر آدرس‌ها و افراد ذکرشده در لیست تحریم‌های یک کشور را مدنظر قرار داد. این لیست‌ها معمولاً شامل برخی از آدرس‌های ارزهای دیجیتال مرتبط با اشخاص هستند؛ اما با این حال، اغلب آنها ناقصند و بسیاری از آدرس‌های موجود در کیف پول‌های این اشخاص را شامل نمی‌شوند. در چنین شرایطی، ابزارهای تحلیل بلاک چین می‌توانند این خلأها را پر کنند.
مؤسسات باید بازبینی دفترکل‌های بلاک چین را به‌منظور ردیابی فعالیت‌هایی که مبدأ یا مقصد آنها به ایران مرتبط است، در دستور کار خود قرار دهند.
شبکه اقدام علیه جرایم مالی ایالات متحده
مؤسسات مالی، باید در مواجه با چالش‌های احتمالی مرتبط با تحریم‌ها، رویکرد پیشگیرانه اتخاذ کنند. این مؤسسات می‌توانند برای بررسی مشکوک‌بودن یک تراکنش، شاخصه‌های اضافی همچون سابقه فعالیت‌های مشتری و سایر علائم هشدارآمیز را تحت‌نظر بگیرند.
داده‌های IP، می‌بایست تمامی استراتژی‌های پیشگیرانه تحریم‌ها را در بر داشته باشند تا اطمینان حاصل شود که مؤسسات مالی، هیچ‌گونه معامله‌ای با کشورهای تحریم‌شده ندارند. در حال حاضر، متداول‌ترین روش برای ثبت اطلاعات IP مشتریان، کنترل IP آنها در هنگام ورود (login) به وب‌سایت‌ها و پلتفرم‌های مالی است؛ اما این روش به‌تنهایی برای شناسایی و جلوگیری از تراکنش‌های مرتبط با کشورهای تحریم‌شده کافی نیست و تأثیر آن، اغلب با استفاده از VPNها به‌راحتی خنثی می‌شود. مؤسسات مالی با استفاده از اطلاعات تکمیلی به‌دست‌آمده از تعامل IPها با بلاک چین، می‌توانند استراتژی‌های تحریمی خود را بهبود بخشیده و نظارت دقیق‌تر خود بر موقعیت جغرافیایی مشتریان را تضمین کنند.
سایفرتریس، تاکنون چندین میلیون IP قابل‌شناسایی را از کشورهای تحریم‌شده نظیر کره شمالی، سوریه و ایران را جمع‌آوری کرده است. لازم به ذکر است که تحلیلگران سایفرتریس، طی سال گذشته، شاهد رشد چشمگیر تعامل آدرس‌های IP ایرانی با بلاک چین بیت کوین، در مقایسه با سایر کشورهای تحریم شده بودند.
تحریم‌های ایالات متحده، صادرات کالا، خدمات و تکنولوژی به ایران را به‌طور کلی منع می‌کند. اگر مؤسسات مالی نظیر صرافی‌های ارز دیجیتال، امکان پرداخت را برای اشخاص یا شرکت‌های ایرانی فراهم کنند، در واقع برخلاف این تحریم‌ها به ایران خدمات صادر کرده‌اند.
یکی از توضیحات احتمالی برای افزایش تعامل IPهای ایرانی با بلاک چین بیت کوین، افزایش استخراج بیت کوین توسط فعالان ایرانی این صنعت است. بسیاری از آدرس‌های (بیت کوین) جدید مرتبط با ایران، با استخرهای استخراج تعامل دارند.

داده‌های مکانی به‌دست‌آمده از جستارهای بلاک چین با IPهای ایرانی؛ بیشترین مراکز فعالیت در حومه تهران هستند.
توصیه‌هایی برای تضمین اجرای دقیق تحریم‌ها:
VASPها (سرویس‌دهندگان دارایی‌های مجازی) علاوه بر کنترل اطلاعات IP مشتریان در هنگام ورود به سیستم‌ها، باید آدرس‌های مرتبط با IP آنها را نیز زیرنظر گرفته و ارتباط آنها با کشورهای تحریم‌شده را بررسی کنند.
VASPها نباید تنها به آدرس‌های مورداشاره در لیست تحریم‌ها اکتفا کنند؛ زیرا در اغلب موارد، آدرس‌های مرتبط دیگری نیز در همان کیف پول وجود دارند که در لیست تحریم‌ها به آن اشاره‌ای نشده و شخص یا سازمان تحریم‌شده، از آنها استفاده می‌کند.
ارزهای دیجیتال و تحریم‌ها
در تاریخ ۲۸ نوامبر ۲۰۱۸، اداره کنترل دارایی‌های خارجی وزارت خزانه‌داری ایالات متحده (OFAC)، برای اولین بار، دو آدرس بیت کوین را به لیست

تحریمی ویژه خود (SDN) اضافه کرد. این دو آدرس متعلق به دو کارگزار ارزهای دیجیتال در ایران بود که ۶,۰۰۰ بیت کوین متعلق به گردانندگان باج‌افزار سَم‌سَم (SamSam) را از طریق ۴۰ صرافی پول‌شویی کرده‌اند.
از سال ۲۰۱۸ تاکنون، اوفک ۶۷ آدرس دیگر، از جمله آدرس‌های بیت کوین، اتریوم، لایت کوین، بیت کوین اس‌وی، بیت کوین گلد، دَش، زی‌کَش و مونرو را نیز به فهرست تحریم‌های خود افزوده است. با این حال، تحلیلگران سایفرتریس دریافته‌اند که آدرس‌هایی که در لیست SDN اوفک قرار می‌گیرند، تعداد انگشت‌شماری از مجموعه آدرس‌های تحت‌اختیار اشخاص تحریم‌شده و یا آدرس‌های موجود در کیف پول‌های آنها را تشکیل می‌دهند. به همین دلیل استفاده از تحلیل‌های بلاک چین، به‌منظور کشف سایر آدرس‌های تحت‌کنترل اشخاص تحریم‌شده (که در لیست‌های تحریمی ذکر نشده) امری ضروری است.
اگر مؤسسات مالی از این آدرس‌های اضافی اطلاع نداشته باشند، در معرض انجام معامله نادانسته بافراد تحریم‌شده خواهند بود.
سیگال مندلکر (Sigal Mandelker) معاون وزارت خزانه‌داری ایالات متحده در امور تروریسم و اطلاعات مالی:
وزارت خزانه‌داری، سیاست‌های سختگیرانه‌ای را در قبال ایران و سایر رژیم‌های سرکشی که با سوءاستفاده از ارزهای دیجیتال و بهره‌گیری از ضعف‌های سازمان‌های سایبری، پادمان‌های مبارزه با پول‌شویی و تأمین مالی تروریسم، برای پیشبرد اهداف مجرمانه خود استفاده می‌کنند، اتخاذ خواهد کرد.
با اضافه‌شدن ارزهای دیجیتال به لیست تحریم‌های ایالات متحده، وزارت خزانه‌داری تصریح کرده است که آدرس‌های ارزهای دیجیتال ذکرشده در لیست SDN جامع نیستند و سایر آدرس‌های مرتبط با آدرس‌های تعیین‌شده نیز باید مسدود شوند.
اطلاعات IP، باید در تمامی برنامه‌های انطباق با تحریم‌ها که سطح فعالیت‌های تحت‌وب اجرا می‌شوند (مانند معاملات ارزهای دیجیتال)، گنجانده شوند. ناشناسی که معاملات مبتنی بر اینترنت ارائه می‌دهند، اغلب تحریم‌های مالی را تحت‌تأثیر قرار می‌دهند. در حال حاضر بسیاری از شرکت‌های خدمات مالی مبتنی بر اینترنت، توانایی مسدودکردن آدرس‌های IP را دارند. با این حال، این روش‌ها معمولاً محدود به تشخیص داده‌های IP مشتریان در هنگام ورود به وب‌سایت‌ها و اپلیکیشن‌ها هستند. اگرچه این رویکرد می‌تواند در ابتدای امر مؤثر باشد، اما نمی‌تواند اجرای قوانین مالی در مؤسسات تحت‌وب را به‌طور کامل تضمین کند.
فناوری بلاک چین به مؤسسات مالی اجازه می‌دهد اطلاعات IP بیشتری را درباره مشتریان خود جمع‌آوری کنند که مشاهده این اطلاعات، در معاملات سنتی تحت‌وب امکان‌پذیر نیست. این اطلاعات اضافی می‌تواند به پیروی مؤسسات مالی از قوانین تحریم و آگاهی آنها از اینکه مبدأ و مقصد تراکنش‌ها در کشورهای تحریم‌شده قرار دارند، کمک کرده و از تخلفات احتمالی جلوگیری کند.
داده‌های IP بلاک چین، سازگاری با تحریم‌ها را افزایش می‌دهد
شرکت سایفرتریس تاکنون بیش از ۷۲,۰۰۰ آدرس IP یکتای ایرانی را جمع‌آوری کرده است. بسیاری از این آدرس‌ها، پیش‌تر با صرافی‌های بزرگ در کشورهایی که تابع قوانین تحریمی هستند، از جمله صرافی‌های خود ایالات متحده امریکا، ارتباط داشته‌اند.

برخلاف مؤسسات مالی سنتی، ارائه‌دهندگان خدمات دارایی‌های مجازی یا VASPها به‌دلیل ماهیت ناشناس و بین‌المللی این تکنولوژی و همچنین دسترسی آزاد جهانی به ارزهای دیجیتال، خطر معاملات ناخواسته با مناطق تحریم‌شده را افزایش می‌دهند. VASPها برای افزایش انطباق‌پذیری خود با برنامه‌های تحریمی و کاهش خطرات دورزدن تحریم، باید از داده‌های IP حاصل از تحلیل بلاک چین استفاده کنند.
تراکنش‌های ارسال‌شده یا دریافت‌شده از آدرس‌های مرتبط با IP کشورهای تحت‌تحریم، باید برای همه صرافی‌های ارز دیجیتال (و سایر ارائه‌دهندگان خدمات مجازی) هشدارآمیز باشد. اگرچه داده‌های بلاک چینی IP نمی‌توانند با اطمینان تضمین کنند که یک آدرس کیف پول به شهروندان کشورهای تحریم‌شده تعلق دارد یا نه، اما کافی است که علاقه و فعالیت قابل‌توجهی از یک شخص در کشورهای تحریم‌شده را نشان دهند که بر اساس همین موضوع، باید سطح نظارت‌ها بر دارنده این حساب‌ها و انجام تراکنش از آدرس‌های تحریم‌شده احتمالی را افزایش داد.
[توضیح مترجم: به‌عنوان مثال فرض کنید شخصی با IP ایرانی وارد اکسپلورر بلاک چین بیت کوین شده و تراکنش‌های مربوط به یک آدرس خاص را چک کند. در چنین مواردی نمی‌توان با قطعیت تشخیص داد که آن آدرس بیت کوین متعلق به همان صاحب IP است یا خیر. اما درصورت تکرار این موضوع، می‌توان آدرس بیت کوین موردنظر و تراکنش‌های بعدی آن را زیرنظر گرفت و ارتباطی میان این آدرس و آدرس‌های متعلق به کشور ایران پیدا کرد.]
مؤسسات مالی موظفند تحقیقات و استعلام‌های لازم را انجام دهند تا اطمینان حاصل کنند که نتایج ارزیابی عملکردشان، در راستای سیاست‌های داخلی پیروی از قوانین تحریم است. آدرس‌های IP همچنین می‌توانند توسط مؤسسات مالی به‌منظور کشف ارتباط میان سایر آدرس‌های بیت کوین مرتبط با یک مشتری یا طرف معامله، استفاده شوند. این اطلاعات اضافی می‌تواند برای ارزیابی خطرات و تهدیدات مؤسسات و ارائه گزارش‌های مرتبط با تراکنش‌های مشکوک مفید باشد.
هشدارهای مربوط به مبهم‌سازی تراکنش‌ها و گریز از تحریم
افراد تحریم‌شده، اغلب تلاش می‌کنند تا فعالیت‌های غیرقانونی خود را پنهان کنند؛ بنابراین، اطلاع از روش‌های شناسایی تحرکات مشکوک برای پنهان‌کردن موارد نقض تحریم، برای تمامی تیم‌های اجرایی قوانین تحریمی ضروری است.
برخلاف مؤسسات مالی سنتی، VASPها می‌توانند مستقیماً وجوهی را به کیف پول‌های خصوصی ارز دیجیتال در هرکجای دنیا ارسال کنند که این موضوع، خطرات گریز از تحریم را برای آنها افزایش می‌دهد. برای کمک به کاهش این خطرات، مؤسسات مالی باید بتوانند علائم هشدارآمیز زیر را شناسایی کنند:
هشدار اول: زمانی که یک مشتری، مبالغی را به یک آدرس کیف پول مرتبط با چندین آدرس IP از کشورهای تحریم‌شده ارسال، و یا مبالغی را از این آدرس‌ها دریافت می‌کند.
هشدار دوم: زمانی که آدرس سپرده‌گذاری (Deposit address) یک مشتری در مؤسسه شما، از طریق یک آدرس IP متعلق به کشورهای تحریم‌شده، وارسی شده باشد.
هشدار سوم: زمانی که مشتری، مبلغی را به آدرسی دیگر از همان کیف پولی که آدرس تحریم‌شده در آن قرار دارد ارسال و یا از آن دریافت می‌کند.
جریمه شرکت‌های بیت‌گو و بیت‌پی برای نقض تحریم‌ها
در پایان سال ۲۰۲۰، اوفک اولین اقدام اجرایی خود علیه VASPها را به‌دلیل نقض تحریم‌ها اعمال کرد. طبق گزارش اوفک، شرکت بیت‌گو (BitGo)، به‌عنوان سرویس نهادی ارائه‌دهنده خدمات امانی ارزهای دیجیتال و اوپراتور کیف پول، در جلوگیری از افتتاح حساب و ارسال ارزهای دیجیتال (از طریق این پلتفرم) توسط افرادی که ظاهراً در حوزه‌های تحریمی ایالات متحده واقع شده بودند، ناتوان بوده است.
سرانجام، اوفک و بیت‌گو بر سر جریمه ۹۳,۸۳۰ دلاری بیت‌گو به تفاهم رسیدند. اوفک در این اقدام اجرایی تأکید کرد که تعهدات پیروی از تحریم‌ها، در مورد همه امریکایی‌ها از جمله افرادی که در ارائه خدمات مربوط به ارزهای دیجیتال نقش دارند، اعمال می‌شود.

این اقدام اوفک، دو ماه پس از صدور هشداری مبنی بر نقض احتمالی تحریم‌ها، در پی پرداخت مشتریان مؤسسات مالی به باج‌افزارها صورت گرفت.
اوفک در این گزارش اعلام کرد که در تراکنش‌هایی مجموعاً به ارزش ۹,۰۰۰ دلار که از طریق پلتفرم بیت‌گو به کوبا، ایران، سودان، سوریه و منطقه کریمه در اوکراین ارسال شده بود، ۱۸۳ مورد تخلف آشکار وجود داشت. در این گزارش همچنین ادعا شده است که بر اساس اطلاعات IP جمع‌آوری‌شده از مشتریان در هنگام ورود به پلتفرم، شرکت بیت‌گو شواهد کافی را برای تشخیص اینکه این کاربران در مناطق تحریم‌شده قرار دارند، در اختیار داشته؛ اما فاقد هرگونه مکانیسم کنترلی برای جلوگیری از دسترسی این کاربران به خدمات پلتفرم خود بوده است.
بعد از این نیز، در تاریخ ۱۸ فوریه ۲۰۲۱، اوفک با شرکت بیت‌پی (BitPay)، ارائه‌دهنده خدمات پرداخت ارزهای دیجیتال، بر سر پرداخت جریمه ۵۰۷,۰۰۰ دلاری به توافق رسید. در گزارش مربوط به این اقدام اجرایی، ادعا شده است که بیت‌پی، به افرادی از حوزه‌های تحریم‌شده مانند کره شمالی، ایران، سودان و سوریه، اجازه داده است که با استفاده از خدمات پرداخت ارز دیجیتال پلتفرم بیت‌پی، با بازرگانان ایالات متحده معامله کنند.
در حالی که بیت‌پی مشتریان مستقیم خود (یعنی بازرگان‌ها و فروشندگان) را بر اساس لیست تحریمی ویژه اوفک (SDN) غربال کرده و با نظارت مداوم اطمینان حاصل کرده است که این فروشندگان در کشورهای تحریم‌شده ساکن نیستند، اوفک مدعی است که بیت‌پی در غربال کردن اطلاعات مکانی که از خریداران به دست آمده، ناتوان بوده است. این کوتاهی، در نهایت منجر به ۲۱۰۲ معامله موفق از طرف افرادی شد که بر اساس آدرس‌های IP، در کشورهای تحریم‌شده قرار داشتند.
این دومین اقدام اجرایی اوفک علیه خدمات‌دهندگان دارایی‌های مجازی، به‌دلیل نقض تحریم‌های ایالات متحده بوده است. این دو اقدام اخیر، نشان می‌دهد که غربال‌کردن داده‌های IP مشتریان، برای پرهیز از تسهیل تراکنش‌های نقض‌کننده تحریم، تا چه اندازه اهمیت دارد.
این گزارش بیش از پیش نشان می‌دهد که تراکنش‌های بیت کوین و سایر ارزهای دیجیتال تا چه حد می‌توانند قابل‌رهگیری باشند. بنابراین برای افرادی که در کشورهای تحت‌تحریم در حوزه ارزهای دیجیتال فعالیت می‌کنند، این گزارش می‌تواند به‌عنوان یک زنگ‌خطر دیده شود.