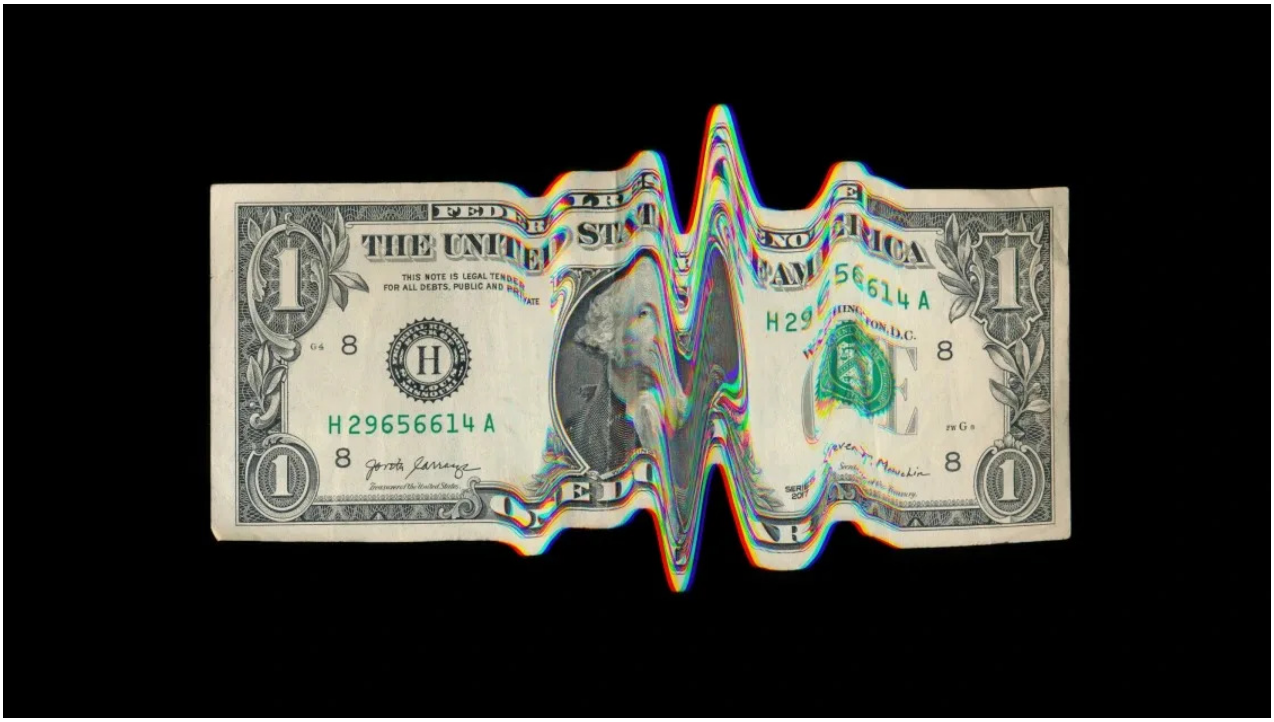
كيف تصادر الحكومات الملايين من العملات المشفرة المسروقة؟



سُجّلت مؤخرًا العديد من سرقات العملات المشفرة التي تقدر بملايين الدولارات، وكان من الصعب اقتفاء أثرها. وقد تصدّرت الجريمة المنظمة واختراق الأمن السيبراني والتجسس لأغراض مالية والجرائم من جميع الأنواع عناوين الأخبار الرئيسية لدرجة أنه حتى عمليات السرقة الضخمة يمكن أن تمر دون أن يلاحظها أحد.

لكن الحكومة تكون في بعض الأحيان قادرة على استعادة تلك الأموال. وفي الأسبوع الماضي، صادرت الولايات المتحدة 500 ألف دولار من العملات المشفرة من قراصنة يزعم أنهم من كوريا الشمالية حصلوا عليها عن طريق ابتزاز المنظمات الطبية الأمريكية. وهذه السرقة مجرد غيض من فيض بالنظر إلى إجمالي عمليات السرقة: صادرت مصلحة الضرائب وحدها 3.5 مليار دولار من العملات المشفرة في سنة 2021. ولكن كيف يمكن الاستيلاء على العملات المشفرة بالضبط؟

ماذا يحدث في البداية عند سرقة العملات المشفرة؟

يدرك اللصوص أنهم بحاجة إلى تنظيف أموال السرقات القذرة. ويعتبر غسيل الأموال نشاطًا قديمًا هدفه جعل رأس المال المكتسب من نشاط غير قانوني يبدو كما لو أنه لا علاقة له بالجريمة نفسها، بحيث يمكن استخدام الأموال بعد ذلك بحريّة.

يوضّح كريستوفر جانجفسكي، الذي كان وكيل حالة رئيسي في دائرة الإيرادات الداخلية متخصص في قضايا العملات المشفرة، لمجلة "إم آي تي" تكنولوجي ريفيو سابقًا: "أود أن أقول إن غسيل الأموال عملية معقدة أكثر مما يفعله المتسللون أنفسهم". وفي سنة 2021، تم غسيل أكثر من 8.6 مليار دولار بنجاح من خلال العملة المشفرة.

تتفرّد كوريا الشمالية من بين جميع الدول باستخدام سرقة العملة المشفرة كوسيلة لتمويل نظامها المعزول ماليًا. تستخدم بيونغ يانغ العملة المشفرة للالتفاف على القيود المفروضة عليها ودفع ثمن كل السلع من الأسلحة إلى الكماليات.

إن تكتيكات غسيل الأموال في تطور دائم. من خلال اعتماد طريقة "بيل تشين" يتم نقل العملة المشفرة عبر آلاف المعاملات للتعتيم على المصدر والوجهة. أما طريقة "تشين هوبينغ" فتكون عبر تجاوز البلوكتشين والعملات. في المقابل، تقوم طريقة "خلاطات العملات المشفرة" على أخذ المعاملات من أي شخص ثم إيداعها في محافظ مختلفة أو حتى بعملات مختلفة في محاولة لفصل الإيداعات والسحوبات. كل هذا بهدف تضليل المحققين.

كيف تتبع جهات إنفاذ القانون المال المسروق؟

استثمرت الحكومة الأمريكية بشكل كبير في أدوات مراقبة وتحليل البلوكتشين.

تبيع شركات مثل "تشين أنالسيز" و"تي آر إم لابز" و"إيلبتيك" برامج لتتبع وتحليل النظام الإيكولوجي للعملات المشفرة. لقد استثمرت الحكومات بكثافة في هذه الصناعة الناشئة كطريقة لكشف سرقة المتسللين وغسيل الأموال وصرف الأموال المستمدة من العملات المشفرة غير المشروعة.

يعد برنامج "تي آر إم فورنزيكس" مثلا منتجًا مصممًا لتتبع معاملات العملات المشفرة عبر 26 سلسلة مختلفة من البلوكتشين، وتبيّن تدفق الأموال، وتحديد المحافظ التي وصلت إليها العملات المشعرة. وبالمثل، يوفر تطبيق "تشين أناليسيز رياكتور" مراقبة مستمرة لأصول مختلفة من العملات المشفرة بحيث يمكن للعميل، مثل وكالة حكومية أمريكية، معرفة ما إذا كانت محفظة معينة تنتمي إلى سوق مظلمة أو بورصة عملات مشفرة عالية الخطورة أو كازينو عبر الإنترنت.

تُوفر هذه البرامج نتائج تُقدّم مجموعات دقيقة من تصورات البيانات الجاهزة للتحقيقات الحكومية، التي ستؤدي في نهاية المطاف إلى الملاحقات القضائية. لكن برمجيات تعقب الأموال لا يمكنها استعادة أو استرجاع الأموال المسروقة.

كيف تصادر الحكومة المال المسروق بالفعل؟

يقول آري ريدبورد، المدعي الفيدرالي السابق ورئيس الشؤون الحكومية في "تي آر إم لابز" حاليًا، إن "البحث عن الأموال المفقودة مجرد أداة واحدة في صندوق الأدوات. ثم يتطلب الأمر فيما بعد تدخل الشرطة الذين يعد عملهم استقصائيًا". وهناك ثلاث طرق أساسية يمكن للحكومة الأمريكية من خلالها الوصول بشكل قانوني إلى الأموال واستردادها.

جدّت أكبر عملية مصادرة فردية في تاريخ الولايات المتحدة هذه السنة عندما استحوذت وزارة العدل على 3.6 مليار دولار من العملات المشفرة التي يُزعم أنها سُرقت خلال اختراق سنة 2016 لبورصة بيتفينكس، وهي بورصة عملات افتراضية. من جوانب عديدة، كانت هذه القضية أبسط بكثير بالنسبة للشرطة الأمريكية لأنه قبض على شخصين مقيمين في مانهاتن.

أظهر تحليل البلوكتشين أنه تم نقل العملة المسروقة، بعد محاولات عديدة ولكن فاشلة لغسل الأموال، إلى حسابات يسيطر عليها المشتبه بهم. وقد حصلت الشرطة على أمر تفتيش لحساب التخزين السحابي للمشتبه بهم يحتوي على ملف مشفر. تم فك تشفير الملف وُوجد أنه يحتوي على 2000 عنوان للعملات المشفرة ومفاتيح خاصة. تم ربط كل محفظة تقريبًا مباشرة باختراق بيتفينكس. وقد تلقت سلطات إنفاذ القانون مذكرة مصادرة وأصبحت الأموال في حوزة الحكومة، ناهيك عن اعتقال اثنين من المشتبه بهم.

يتمتع النظام الإيكولوجي للعملات المشفرة بسمعة في الخيال الشعبي باعتباره مكانا يشبه إلى حد ما الغرب المتوحش. ولكن في محاولة للقيام بالأعمال التجارية وكسب المال في الدول الغنية، أصبحت البورصات وغيرها من شركات العملات المشفرة أكثر امتثالا لتطبيق القانون الغربي على مر السنين.

هناك العديد من "المناطق المارقة" البارزة حول العالم التي لا تمتثل للقواعد الدولية لمكافحة غسيل الأموال، بما في ذلك كوريا الشمالية وإيران

بعد تلبية متطلبات السبب المحتمل وعبء الإثبات، يمكن لسلطات إنفاذ القانون الحصول على أوامر مصادرة لأي أموال غير مشروعة تتدفق في نهاية المطاف إلى البورصات الممتثلة للمعايير الدولية – والعديد من صناديق الاستثمار في النهاية. وستعمل سلطات إنفاذ القانون بعد ذلك مع شركة العملات المشفرة لنقل الأموال إلى محفظة تسيطر عليها الحكومة أو تقوم بتجميدها.

يقول جورفايس غريغ، الذي كان مساعدًا لمدير مكتب التحقيقات الفيدرالي قبل أن يصبح مسؤول تنفيذي في "تشين أناليسيز"، إن هناك طريقة أخرى لمصادرة الأموال تتمثل في تعاون الخصم أو أحد مرتكبي الجريمة من خلال تقديم مفاتيح خاصة للحكومة كجزء من مفاوضات الإقرار بالذنب أو التعاون لخدمة مصالحهم بطريقة ما".

ويتمثل الاحتمال الثالث في تعريض أمن الهدف للخطر – ويمكن تنفيذ هذه المهمة بعدة طرق. يضيف ريدبورد أنه "عندما تتحدث عن بلد مثل كوريا الشمالية أو المنظمات الإجرامية الإلكترونية الروسية، فقد يستغرق الأمر سنوات من بناء شبكات من المخبرين السريين والعمل مع الحكومات الأخرى، حتى تلك التي ليست دائمًا حليفة لنا". ويتابع "من المحتمل أن يحدث ذلك من خلال اختراق خادم أو جهاز أو من خلال إجراء أجهزة الشرطة عملا استقصائيا مكثفا".

تعد عملية تتبع القراصنة خارج الولايات المتحدة مهمة أصعب. قد يكون الاعتقال مستحيًلا إذا كان المشتبه به في بلد يرفض التعاون مع واشنطن، لذلك يتغاضى المدعون العامون عن مثل هذه القضايا.

ويوضح ريدبورد، الذي كان مدعيًا عامًا لمدة 11 سنة، أن "المدعين الجيدين يدركون أن الملاحقة الجنائية ليست سوى جزء من تحقيق أكبر يساعد على اكتشاف مثل هذه الأنواع من القضايا" بدلا من ذلك يوجهون جهودهم نحو البحث عن طرق لاسترداد المال.

تنطوي مثل هذه القضايا على جوانب أخرى وهي التنظيم والسياسة والدبلوماسية. يقول غريغ إن هناك العديد من "المناطق المارقة" البارزة حول العالم التي لا تمتثل للقواعد الدولية لمكافحة غسيل الأموال، بما في ذلك كوريا الشمالية وإيران. ويضيف "لكن تلك الأجزاء من العالم باتت محاصرة أكثر". ويرجع ذلك لسببين، إذا كنت تملك نشاطًا تجاريًا، فإن الامتثال للقواعد الدولية يعني أن لديك فرصة للوصول إلى أغنى أسواق العالم؛ أما إذا كنت كيانا دوليا، فهذا يعني أنه عليك احترام القوانين المحلية في المقابل.

ماذا سيأتي بعد ذلك؟

مع أن الحكومات اتبعت نهجا فعالا في مراقبة العملات المشفرة والاستيلاء عليها، يستمر المتسللون في تطوير تكتيكات إجرامية جديدة.

تعتبر خلاطات العملات المشفرة تكتيكًا شائعًا للقراصنة هذه الأيام، حيث يأخذون الأموال من أصول مختلفة، ويجمعونها معًا، ثم يرسلون الأموال مرة أخرى عشوائيًا كطريقة للتعتيم على مصدرها ووجهتها النهائية. ورغم وجود العديد من الأسباب لاستخدام هذه الطريقة إلا أن عملاءهم الرئيسيين كانوا دائمًا مجرمين ومتسللين.

وفقًا لتقرير حديث من تشين أناليسيز، تم عبر هذه الطريقة نقل أكثر من 50 مليون دولار شهريًا في المتوسط هذه السنة، أي ضعف ما تم نقله في العام الماضي. وتسعى شركات تحليل البلوكتشين إلى معالجة المشكلة و"فصل" الأموال بشكل موثوق، ولكن في الوقت الحالي، لا تزال الخلاطات من

أفضل الأدوات التي يستخدمها المجرمون لنقل أموالهم.

اختارت وزارة الخزانة الأمريكية نهجًا آخر أكثر أهمية: في أيار/ مايو 2022، أصدرت الولايات المتحدة أول عقوبات ضد خلاط العملات المشفرة. ويُزعم أنه تم استخدام هذا الخلاط لغسيل العملات المشفرة بعد سرقة 600 مليون دولار من قبل قراصنة من كوريا الشمالية.

حيال هذا الشأن، يقول غريغ إنه في الفترة الأخيرة شهدنا زيادة في تعدد الهجمات. ويشبه الأمر محاولة الآلاف من الحيوانات البرية عبور النهر في وقت واحد حتى لا تتمكن التماسيح سوى من الحصول على عدد قليل منها. وبالمثل، تنامت أعداد الهجمات، على أمل جعل إمساك السلطات بأحد المشتبه بهم صعبًا. وتتمثل المشكلة في أن المحققين يمكنهم ربط ما يبدو أنه هجمات متباينة بالقيادة المركزية، وفي بعض الحالات قد يسهل هذا على الحكومة إثبات وجود مؤامرة كبيرة".

ستصبح جهود تعقب الأموال وتجميدها والاستيلاء عليها أكثر أهمية. ومن المؤكد تمامًا أن المليارات ستستمر في التسلل خارج الكثير من البلدان بطريقة غير مشروعة. وقبل أن تتصدر أنباء احتجاز الولايات المتحدة للقراصنة الكوريين الشماليين عناوين الصحف، أطلقت مجموعة أخرى من كوريا الشمالية حملة قرصنة دولية بواسطة برامج الفدية الخبيثة.

المصدر: تكنولوجي ريفيو

رابط المقال: https://www.noonpost.com/44830/