Version française ci-dessous/Versión española a continuación/Versão em português abaixo

Crypto-currencies: a practical example of a criminal investigation

Alice was in a taxi checking her e-mail on her cellphone. She opened an e-mail that came from a client. The message had an attachment, which Alice understood to be an invoice. She downloaded the attachment to her phone but was unable to open it. She continued checking her e-mails until she arrived at her home in the evening. The next morning while having breakfast, she tried to open her cellphone unsuccessfully. She was locked out. Her password and her other methods of identification did not work. After contacting her service provider, she was able to re-gain access to her cellphone. She immediately opened the app of her cryptocurrencies exchange and to her surprise her account balance was 0.

Un unknown attacker had gained access to her phone and accessed her account. She went directly to the police and filed a report. In her report she claimed that the attacker unlawfully extracted 3 BTC, 10 ETH, and 50000 USDT.

Alice submitted her cellphone to the authorities. A judge ordered complete analysis of its contents. The prosecutor's office analyzed the movements of Alice's account and determined that several transactions had taken place which had emptied the balance of Alice's account.

After tracing the different transactions, the investigator determines that the destination of one of the USDT transactions is a known Exchange in your country, where the recipient of the funds has exchanged 20.000 USDT for US dollars.

1. What is the possible explanation for this transaction?
2. What are other services of ways of converting crypto-currencies to cash?
3. Does your country have a specific legal framework that regulates this type of activity (crypto exchanges)?
4. As a prosecutor what investigative measures would you request or take with regards to the exchange, in order to identify who made the transaction?

An analysis of the seized documents reveals that one of them contains several lists of words. Each of these lists contains exactly 12 words. With these words you are able to reconstruct several wallets that the person controlled. After analyzing the transactions related to these wallets, you conclude that part of the stolen assets from Alice's phone are registered there.

1. As a prosecutor, what measures would you take in this scenario?
2. Can more than one individual control a wallet?
3. How would you proceed with regards to the seizure and recovery of the assets?
4. Does your country have legislation that regulates the seizure of crypto-currencies?
5. In the absence of specific regulations what would you do with the seized assets?

Français

Crypto-monnaies : un exemple pratique d'enquête criminelle

Alice est dans un taxi et consulte son courrier électronique sur son téléphone portable. Elle ouvre un e-mail provenant d'un client. Le message contient une pièce jointe, qu'Alice pense être une facture. Elle télécharge la pièce jointe sur son téléphone, mais ne peut pas l'ouvrir. Elle continue à consulter ses e-mails jusqu'à ce qu'elle arrive à son domicile le soir. Le lendemain matin, alors qu'elle prend son petit-déjeuner, elle tente d'ouvrir son téléphone portable, sans succès. Elle se retrouve bloquée. Son mot de passe et ses autres moyens d'identification ne fonctionnent pas. Après avoir contacté son fournisseur de services, elle retrouve l'accès à son téléphone portable. Elle ouvre immédiatement l'application de sa bourse de crypto-monnaies et, à sa grande surprise, le solde de son compte est 0.

Un attaquant inconnu avait réussi à accéder à son téléphone et à son compte. Elle s'est rendue directement à la police et a porté plainte. Dans son rapport, elle affirme que l'attaquant a illégalement extrait 3 BTC, 10 ETH et 50000 USDT.

Alice a remis son téléphone portable aux autorités. Un juge a ordonné l'analyse complète de son contenu. Le bureau du procureur a analysé les mouvements du compte d'Alice et a déterminé que plusieurs transactions avaient eu lieu qui avaient vidé le solde du compte d'Alice.

Après avoir retracé les différentes transactions, l'enquêteur détermine que la destination de l'une des transactions en USDT est une bourse connue dans votre pays, où le destinataire des fonds a échangé 20 000 USDT contre des dollars américains.

1. Quelle est l'explication possible de cette transaction ?
2. Quels sont les autres services permettant de convertir des crypto-monnaies en espèces ?
3. Votre pays dispose-t-il d'un cadre juridique spécifique qui réglemente ce type d'activité (bourses de crypto-monnaies) ?
4. En tant que procureur, quelles mesures d'enquête demanderiez-vous ou prendriez-vous concernant l'échange, afin d'identifier qui a effectué la transaction ?

L'analyse des documents saisis révèle que l'un d'entre eux contient plusieurs listes de mots. Chacune de ces listes contient exactement 12 mots. Ces mots permettent de reconstituer plusieurs portefeuilles que la personne contrôlait. Après avoir analysé les transactions liées à ces portefeuilles, vous concluez qu'une partie des actifs volés sur le téléphone d'Alice y est enregistrée.

1. En tant que procureur, quelles mesures prendriez-vous dans ce scénario ?
2. Plusieurs personnes peuvent-elles contrôler un portefeuille ?
3. Comment procéderiez-vous à la saisie et au recouvrement des avoirs ?
4. Votre pays dispose-t-il d'une législation régissant la saisie des crypto-monnaies ?
5. En l'absence de réglementation spécifique, que feriez-vous des actifs saisis ?

Español [traducción automática]

Criptomonedas: un ejemplo práctico de investigación criminal

Alice se encontraba en un taxi consultando su correo electrónico en el móvil. Abrió un correo electrónico que procedía de un cliente. El mensaje tenía un archivo adjunto, que Alice entendió que era una factura. Descargó el archivo adjunto en su teléfono pero no pudo abrirlo. Siguió revisando sus correos electrónicos hasta que llegó a su casa por la noche. A la mañana siguiente, mientras desayunaba, intentó abrir su móvil sin éxito. Se quedó bloqueada. Su contraseña y sus otros métodos de identificación no funcionaban. Tras ponerse en contacto con su proveedor de servicios, pudo recuperar el acceso a su teléfono móvil. Inmediatamente abrió la aplicación de su bolsa de criptomonedas y, para su sorpresa, el saldo de su cuenta era 0.

Un atacante desconocido había conseguido acceder a su teléfono y había entrado en su cuenta. Fue directamente a la policía y presentó una denuncia. En su denuncia afirmaba que el atacante había extraído ilegalmente 3 BTC, 10 ETH y 50000 USDT.

Alice entregó su teléfono móvil a las autoridades. Un juez ordenó el análisis completo de su contenido. La fiscalía analizó los movimientos de la cuenta de Alice y determinó que se habían producido varias transacciones que habían vaciado el saldo de la cuenta de Alice.

Tras rastrear las distintas transacciones, el investigador determina que el destino de una de las transacciones de USDT es una conocida casa de cambio de su país, donde el destinatario de los fondos ha cambiado 20.000 USDT por dólares estadounidenses.

1. ¿Cuál es la posible explicación de esta transacción?
2. ¿Cuáles son otros servicios de formas de convertir criptomonedas en dinero en efectivo?
3. ¿Dispone su país de un marco jurídico específico que regule este tipo de actividad (criptointercambios)?
4. Como fiscal, ¿qué medidas de investigación solicitaría o adoptaría en relación con el intercambio, con el fin de identificar a quien realizó la transacción?

El análisis de los documentos incautados revela que uno de ellos contiene varias listas de palabras. Cada una de estas listas contiene exactamente 12 palabras. Con estas palabras se pueden reconstruir varias carteras que la persona controlaba. Tras analizar las transacciones relacionadas con estos monederos, usted concluye que parte de los activos robados del teléfono de Alice están registrados allí.

1. Como fiscal, ¿qué medidas tomaría en este escenario?
2. ¿Puede más de un individuo controlar un monedero?
3. ¿Cómo procedería con respecto a la incautación y recuperación de los activos?
4. ¿Existe en su país una legislación que regule la incautación de criptomonedas?
5. En ausencia de normativa específica, ¿qué haría con los activos incautados?

Portugues [tradução automática]

Cripto-moedas: um exemplo prático de uma investigação criminal

Alice estava num táxi a consultar o seu e-mail no telemóvel. Abriu uma mensagem de correio eletrónico de um cliente. A mensagem tinha um anexo, que Alice entendeu ser uma fatura. Descarregou o anexo para o seu telemóvel, mas não o conseguiu abrir. Continuou a verificar as mensagens de correio eletrónico até chegar a casa ao fim da tarde. Na manhã seguinte, enquanto tomava o pequeno-almoço, tentou abrir o telemóvel, sem sucesso. Ficou bloqueada. A sua palavra-passe e os seus outros métodos de identificação não funcionaram. Depois de contactar o seu fornecedor de serviços, conseguiu voltar a ter acesso ao seu telemóvel. Abriu imediatamente a aplicação da sua bolsa de criptomoedas e, para sua surpresa, o saldo da sua conta era 0.

Um atacante desconhecido tinha obtido acesso ao seu telemóvel e acedido à sua conta. Dirigiu-se diretamente à polícia e apresentou queixa. No seu relatório, afirma que o atacante extraiu ilegalmente 3 BTC, 10 ETH e 50000 USDT.

Alice entregou o seu telemóvel às autoridades. Um juiz ordenou a análise completa do seu conteúdo. O gabinete do procurador analisou os movimentos da conta de Alice e determinou que tinham ocorrido várias transacções que esvaziaram o saldo da conta de Alice.

Depois de rastrear as diferentes transacções, o investigador determina que o destino de uma das transacções de USDT é uma bolsa conhecida no seu país, onde o destinatário dos fundos trocou 20.000 USDT por dólares americanos.

1. Qual é a explicação possível para esta transação?
2. Quais são os outros serviços de conversão de criptomoedas em dinheiro?
3. O seu país dispõe de um quadro jurídico específico que regule este tipo de atividade (bolsas de criptomoedas)?
4. Como procurador, que medidas de investigação solicitaria ou tomaria em relação à bolsa, a fim de identificar quem fez a transação?

A análise dos documentos apreendidos revela que um deles contém várias listas de palavras. Cada uma destas listas contém exatamente 12 palavras. Com estas palavras, pode reconstruir várias carteiras que a pessoa controlava. Depois de analisar as transacções relacionadas com estas carteiras, conclui que parte dos bens roubados do telemóvel da Alice estão aí registados.

1. Enquanto procurador do Ministério Público, que medidas tomaria neste cenário?
2. Pode haver mais do que um indivíduo a controlar uma carteira?
3. Como procederia em relação à apreensão e recuperação dos bens?
4. O seu país tem legislação que regula a apreensão de criptomoedas?
5. Na ausência de regulamentação específica, o que faria com os bens apreendidos?