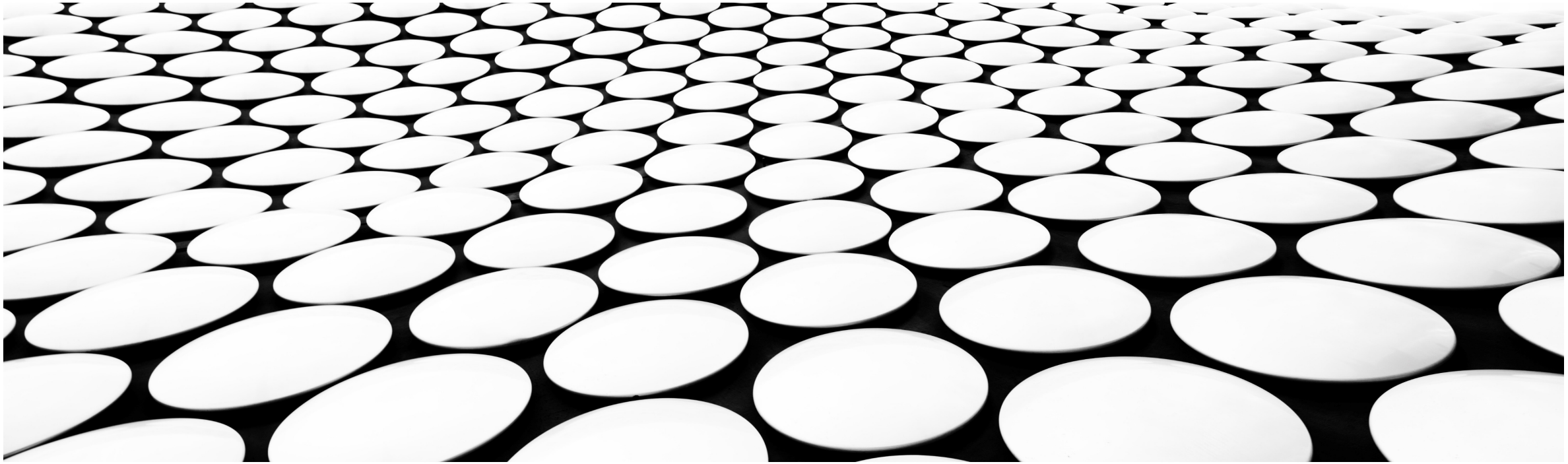
ACTIVOS VIRTUALES: MÁS UNA EVOLUCIÓN QUE UNA REVOLUCIÓN



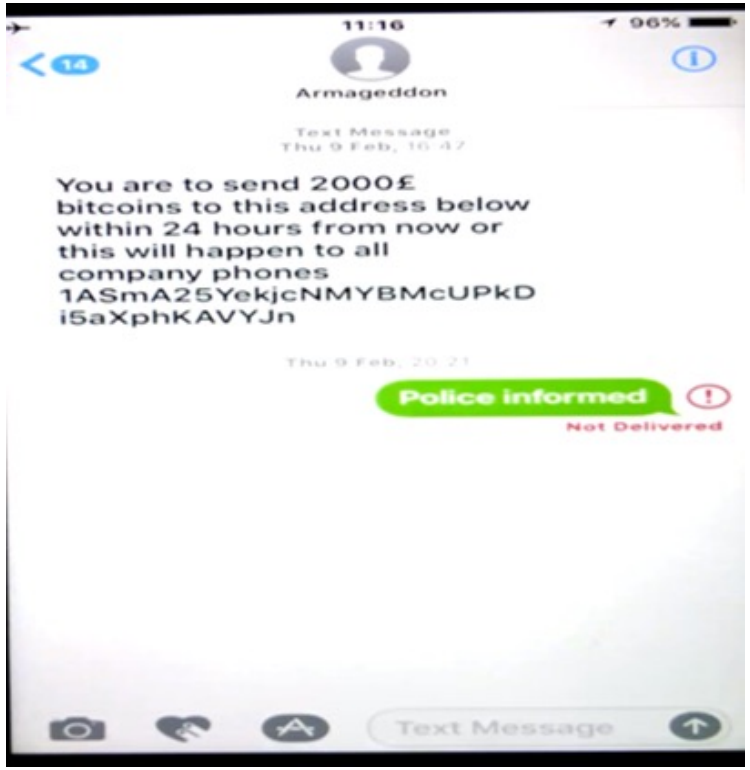
ADVERSARIOS DINÁMICOS

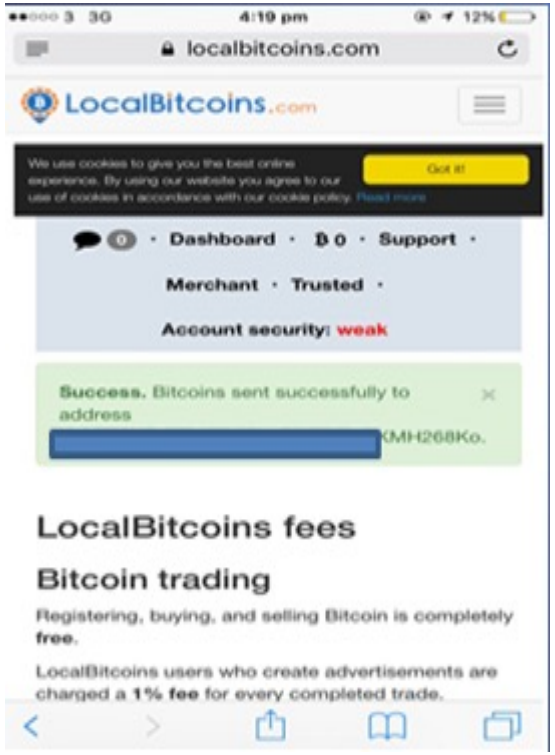
- La capacidad de la los delincuentes para adaptarse rápidamente y desarrollar nuevos métodos delictivos en función de las posibilidades tecnológicas y del entorno es un hecho ampliamente constatado. Las criptomonedas/activos virtuales no son una excepción, y cada vez son más las investigaciones que detectan su presencia en distintos tipos de lavado de activos.
- A menudo, el carácter técnico de este tipo de activos se percibe como una barrera para investigar eficazmente la comisión de un delito. No obstante, se trata de una percepción errónea. Las tácticas de blanqueo de capitales son evolutivas. Sus rasgos más característicos permanecen y se van perfilando a medida que los delincuentes se adaptan a los cambios en su entorno.
- Esto significa que los cambios en los distintos métodos de lavado de activos suelen ser graduales y no revolucionarios. Para los investigadores, muchas de las competencias actuales seguirán siendo pertinentes en investigaciones relacionadas con los activos virtuales, ya que solo serán un aspecto de una estrategia de lavado de activos mucho más amplia.

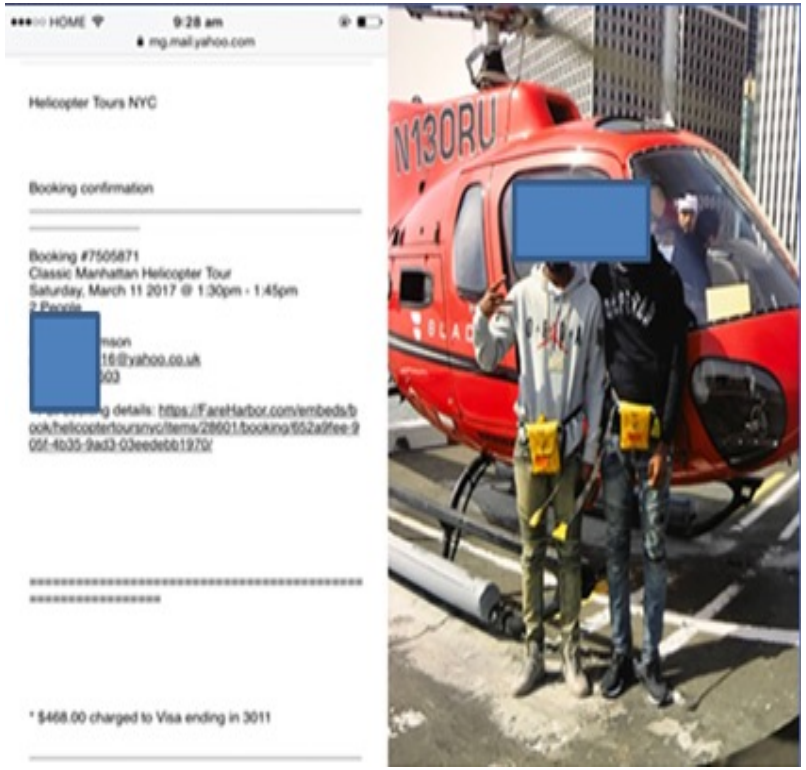
INTRODUCCIÓN

- El lavado de activos es la principal amenaza derivada de la rápida adopción generalizada de criptomonedas/activos virtuales. Esto no se limita a la delincuencia digital.
- Las investigaciones sobre delitos adquisitivos de casi cualquier naturaleza se están topando con estos activos.
- Centrarse únicamente en la «ciberdelincuencia» es un enfoque demasiado estrecho para desplegar eficazmente la capacidad de las fuerzas policiales.
- Casi todos los delitos relacionados con las criptomonedas comprenden también otros mecanismos financieros.
- En consecuencia, es vital tener en cuenta que los equipos de investigación han de disponer tanto de conocimientos financieros como digitales.
- Es necesario considerar el proceso integral de recopilación de pruebas relevantes en materia de criptomonedas, es decir, la información de inteligencia, la obtención de pruebas, así como la presentación procesal de pruebas documentales y periciales.
- El análisis forense digital es un componente clave en este sentido. Si bien en esta materia hay determinados conceptos avanzados relevantes (configuraciones de minería, carteras de hardware seguras, etc.), es mucho lo que se puede hacer con herramientas convencionales.
- En particular, el análisis de los teléfonos móviles puede proporcionar pruebas clave para el avance de las investigaciones.

ADQUISICIÓN DEL SOFTWARE GRAYKEY

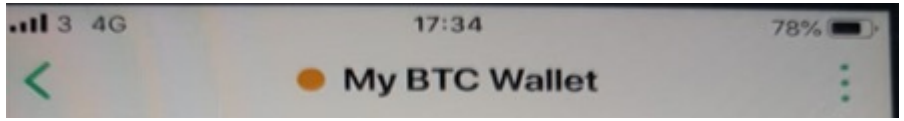




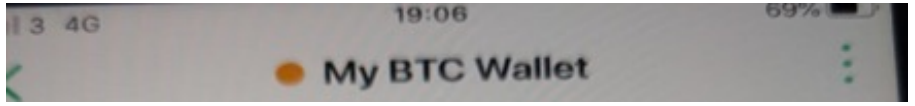


EJEMPLO 2

• El sospechoso actúa como intermediario entre las partes que llevan acabo el lavado de activos: destaca que tienen un «*nuevo colaborador que vende Bitcoins por "papel" (dinero en efectivo), 5% (el vendedor se lleva un 5% extra en efectivo sobre el importe de la venta de Bitcoins)*».



A partir de estas fotos tomadas por el sospechoso se pudo identificar el movimiento de 300.000 libras en Bitcoins a un integrante de un grupo de delincuencia organizada.



In the video identifying the "bitcoin.com" wallet it is possible to identify that the suspect has several other cryptocurrency related applications:

- Shapeshift: Allows for trading and conversion between different cryptocurrencies
- Two Factor authentication applications: Used as added security feature on the majority of cryptocurrency applications to authorise access/transactions.
- Swap wallet: Unknown if this is a cryptocurrency app, search on iOS store cannot find a result for this. Open source also unclear.
- Telegram: Numerous groups and bots available for transacting cryptocurrencies.

APROVECHAR LAS COMPETENCIAS ACTUALES

- Como se ha señalado anteriormente, en la mayoría de los casos, para disfrutar del producto del delito sigue siendo necesario integrarse en el sistema financiero tradicional. De ahí que, un análisis global del estilo de vida financiero del sospechoso permitirá identificar las posibilidades clave para llevar a cabo una investigación, independientemente de los conocimientos técnicos sobre criptomonedas.
- Utilizar los informes de actividades sospechosas (Suspicious Activity Reports) para identificar el uso de activos virtuales y desarrollar eficazmente esta información no requiere tener un conocimiento especializado de los activos virtuales. La investigación sobre individuos, empresas vinculadas, cuentas financieras, huellas digitales y colaboradores puede hacer progresar significativamente una investigación relacionada con activos virtuales.
- Utilizar de forma proactiva las disposiciones normativas sobre el producto del delito relativas a las órdenes de embargo puede evitar una serie de preocupaciones sobre la disipación e incautación de activos virtuales. Recurrir a medidas patrimoniales, como las órdenes de privación del patrimonio no justificado (Unexplained Wealth Orders), también puede resultar útil para perseguir a quienes utilizan activos virtuales para el lavado de activos.
- La presencia de activos virtuales no es óbice para examinar las posibilidades que ofrece el análisis forense digital a la hora de identificar las conexiones con los distintos métodos de lavado de activos. En todo caso, el uso de criptomonedas dejará una mayor huella digital y proporcionará muchas oportunidades de obtener pruebas.
- Actualmente, los conceptos avanzados no son una práctica generalizada, ya que todavía no resultan indispensables, lo que supone una oportunidad de prepararse para el momento en que sí lo sean. Esta labor podría encomendarse a equipos de investigación y desarrollo especializados.

DEBATE EN GRUPO

- ¿Qué dispone la legislación de su jurisdicción sobre el producto del delito?
- ¿Qué eficacia tiene el régimen SAR/STR en su jurisdicción?
- ¿De qué capacidades de análisis forense digital dispone su Administración?
- ¿Ha investigado alguna vez casos relacionados con criptomonedas?