

MINISTERIO
DEL INTERIOR



DIRECCIÓN GENERAL DE
LA GUARDIA CIVIL



INFORME TÉCNICO

Número: 0001

Juzgado de Instrucción nº 1 de Fuengirola

Diligencias Previas 161/2022

Unidad solicitante:

Unidad Orgánica de Policía Judicial de Málaga

Asunto:

Análisis transacciones de criptomonedas

**JEFATURA DE POLICÍA JUDICIAL
UNIDAD TÉCNICA DE POLICÍA JUDICIAL
GRUPO DE CIBERINTELIGENCIA CRIMINAL**



JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

INDICE

1.- Antecedentes 3

2.- Muestras para analizar 4

3.- Cuestiones que se plantean 4

4.- Resolución 4

4.1.- Análisis de las direcciones 5

4.1.1.- Dirección de Bitcoin 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE..... 5

4.1.2.- Dirección de Ethereum 0xd0E6c719259955b3815e67ac22755fCdb72Ef06A..... 12

4.1.3.- Dirección de ETH 0x2EDD429e53dD6C3bf33830103b736462587416D8 16

4.1.4.- Dirección de ETH 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C 17

4.1.5.- Respuestas de exchanger Binance..... 21

4.1.6.- Respuestas de Exchanger Whitebit 23

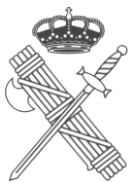
4.1.7.- Respuestas de procesador de pagos BitPay 25

5.- Conclusiones 26

6.- Entrega del Informe Técnico..... 28

GLOSARIO DE TERMINOS..... 29





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

Juzgado de Instrucción nº 1

Fuengirola

Diligencias Previas 161/2022

Los miembros de la Guardia Civil con Tarjeta de Identidad Profesional número, T89891S y J65728P, especialistas del Grupo de Ciberinteligencia Criminal, de la Unidad Técnica de la Jefatura de Policía Judicial, por el presente Informe hacen constar:

1.- Antecedentes

El día 1 de febrero se recibe por parte de la Unidad que suscribe una petición para la elaboración de un informe técnico sobre la trazabilidad de las criptomonedas con motivo de la investigación en curso, bajo el amparo de las Diligencias Previas 161/2022, Juzgado de Instrucción nº 1 de Fuengirola.

El personal de este Grupo con Tarjeta de Identidad Profesional número T89891S y J65728P, en calidad de experto inició las actuaciones, el análisis se realiza siguiendo las transacciones públicas en blockchain de Bitcoin, Ethereum y USDT para un mejor entendimiento y visualización se utiliza la herramienta de conocido prestigio Chainalysis-Reactor, testada y utilizada por diferentes agencias policiales, EUROPOL y plataformas de servicio de criptomonedas.

Como consta en el acta se realiza el estudio sobre las direcciones bitcoin proporcionadas por la Unidad en su investigación, la trazabilidad y rastreos se relaciona en los apartados siguientes indicando el destino final de los fondos.

Todas las actividades y actuaciones llevadas a cabo sobre las direcciones han sido realizadas utilizando herramientas y procedimientos, corroborados y extensamente utilizados por la comunidad internacional.

Se hace constar Glosario de Términos para su consulta.





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

2.- Muestras para analizar

A continuación se relaciona las direcciones de Bitcoin y Ethereum sobre las que se realiza el pertinente estudio. El presente análisis se realiza sobre las direcciones de criptomonedas facilitadas por la víctima a los investigadores como destinatarias de los fondos.

Todos los fondos se dirigen a las siguientes direcciones:

1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

0xd0E6c719259955b3815e67ac22755fCdb72Ef06A

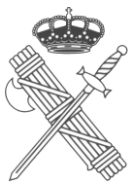
3.- Cuestiones que se plantean

El citado estudio se plantea para el análisis y trazabilidad de los fondos a través de las diferentes direcciones de criptomonedas, teniendo como finalidad identificar el destino final de los fondos y los usuarios receptores de estos.

4.- Resolución

Se realiza el estudio solicitado, de acuerdo con lo descrito a continuación en el presente Informe Técnico, en este Informe Técnico se analizan las transacciones y operativas de criptomonedas más relevantes.



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

4.1.- Análisis de las direcciones

4.1.1.- Dirección de Bitcoin 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

Esta dirección recibe la totalidad de los fondos robados de la dirección de la billetera de la víctima.

Root Address	Balance:	0,00 BTC	Transfers:	111
1GLefw1owvMqs5azmjV79NH4Fgd...	Sent:	29,125304 BTC	Withdrawals:	81
	Received:	29,139736 BTC	Deposits:	30
	Total Fees:	0,014432 BTC	Addresses:	1

Imagen 1. Composición billetera 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

En la imagen 1 se muestra la composición de esta billetera que está formada por UNA dirección de bitcoin que recibe 29.13 BTCs y envía 29.12 BTCs en 111 transacciones. Esta billetera tiene un balance de 0 BTCs el día 22 de junio de 2022.

El día 8 de junio de 2021 a las 14:37 horas se realizan las siguientes transacciones desde las direcciones de la víctima:

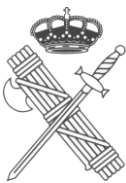
* Transacción con hash
be633331eb837db53be6928d89b099cf28edcf1d1e5e277af6265103babd0c8a por valor
de 19.01563316 btcs desde la dirección 1JdSjGFaq6fVX95sVbShb7WTNuLwngWvaR a
la dirección 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

* Transacción con hash
6b6c105eb13fd507549db713c640bf034f60fe1042b04371db8446df3fba64d8 por valor de
1.99011852 btcs desde la dirección 38hwA6dVomoCTRKKGyXkdAPHh5hATMjH a la
dirección 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

* Transacción con hash
4777a5725d56fc4bb2c67ae0b196876419b40c6e216145ceb976246ce1d08479 por valor
de 1.13853362 btcs desde la dirección 3GS68FuYdfEc9X4PE2gmVBTWYzL3Jada3c a la
dirección 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

* Transacción con hash
ed7871fa0683a55a149c149221ca69a6b10e5f73f092064f1bd40e9be7c379cb por valor de



DIRECCIÓN GENERAL
DE LA GUARDIA CIVIL

JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

0.99642007 btcs desde la dirección 3Nq4WfzkCqAj2wKB1rYPDCxCYF6ihyavy9 a la dirección 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

* Transacción con hash ec3cc95f018bf39ead1b6f346f1277be20a9cb601009c58207dd08812564511f por valor de 0.82581676 btcs desde la dirección 36YaVZhybRQ36X4PZpPkYm9cCy9G4o4CrE a la dirección 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

* Transacción con hash 1bf22b44bbb32be05b70b653942c48c3d10c945b48b9a712376a7691ec1f610a por valor de 0.49850585 btcs desde la dirección 38rz84UCPfYUoUhUiwERNaDknCdZZxttoy a la dirección 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

En total se han sustraído de las direcciones de la víctima una cantidad de 24.46502798 btcs.

En la imagen 2 se observa la salida de fondos desde las direcciones de la víctima hacia la dirección sospechosa 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE. Las cantidades en dicha imagen están redondeadas para una mejor visualización.

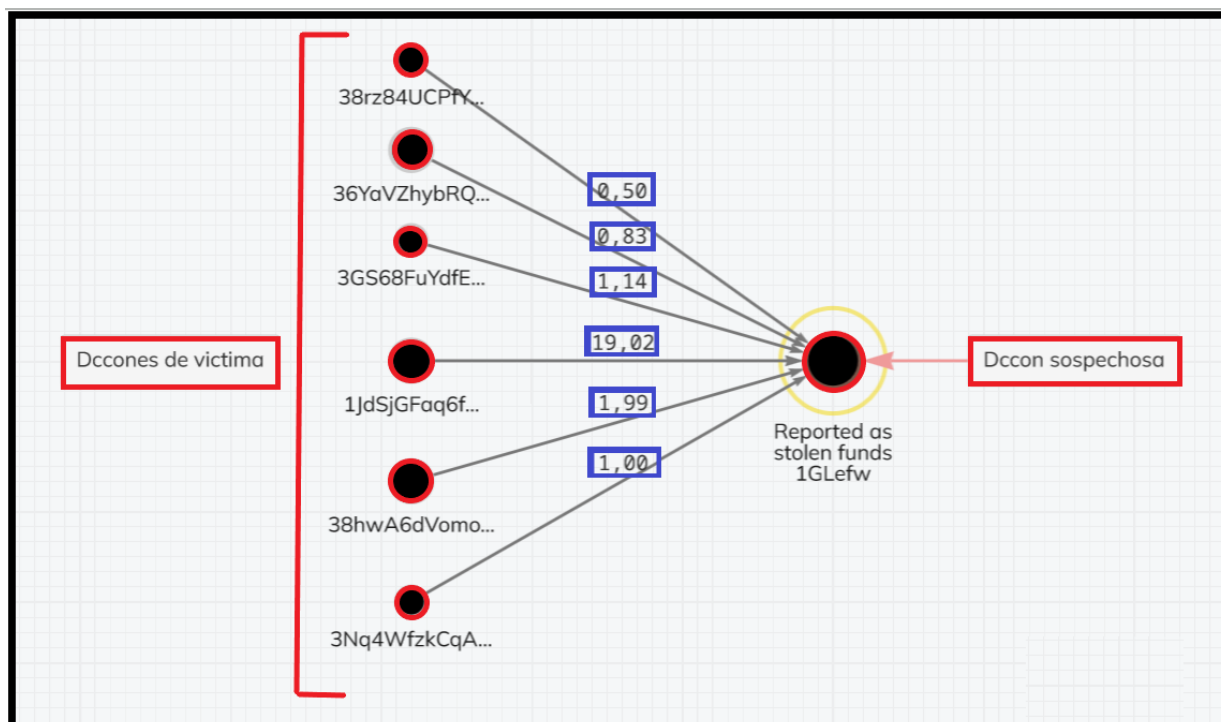


Imagen 2. Salida de las billeteras de la víctima



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

La dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** tiene entrada de fondos hasta el día 6 de octubre sin tener ninguna salida de fondos.

Al analizar la operativa de salida se detecta que entre los días 6 y 8 de octubre de 2021 la totalidad de los fondos de la dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** son enviados al exchanger **Huobi** a través de tres direcciones **1LNvm9RLLkz5bXqwWcsQ9Zo7XuKAH6jRSp** (Huobi 1), **1MB8JPgu2T8J7MSQCZpfbgYLwhBxNsFZGE** (Huobi 2) y **1ANWDqQtLwVQqNHuRmxbPbPmrcLPtTz188** (Huobi 3).

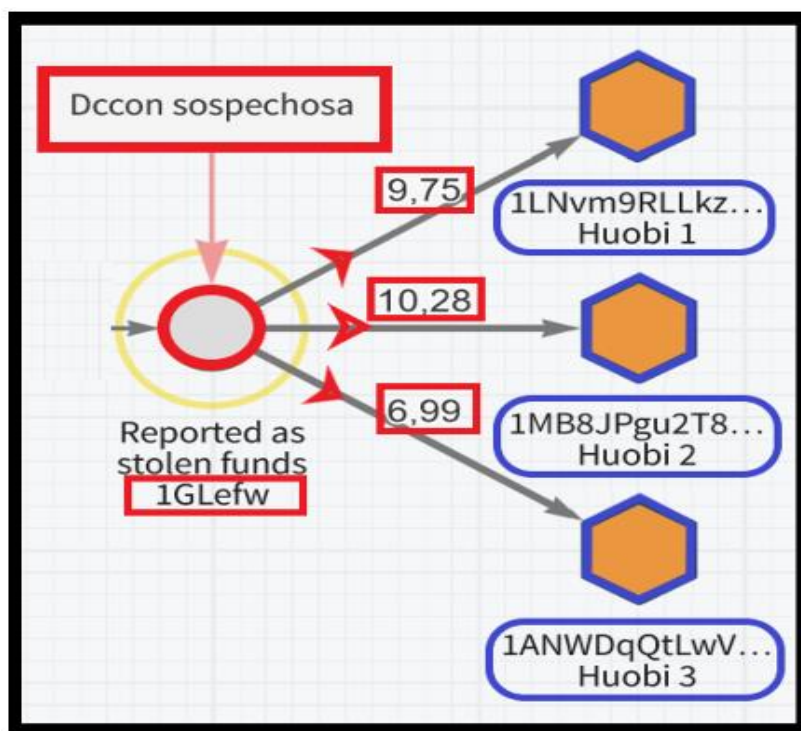


Imagen 3. Salida de la billetera 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

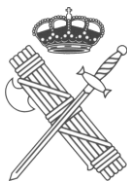
En la imagen 3 se muestra la salida total de los fondos de esta billetera que son remitidos en TREINTA transacciones que se detallan a continuación en las que se envían 27,022487 BTCs de manera directa a las direcciones de bitcoin del exchanger **Huobi** **1LNvm9RLLkz5bXqwWcsQ9Zo7XuKAH6jRSp** (Huobi 1), **1MB8JPgu2T8J7MSQCZpfbgYLwhBxNsFZGE** (Huobi 2) y **1ANWDqQtLwVQqNHuRmxbPbPmrcLPtTz188** (Huobi 3).

La salida de fondos hacia la dirección **1LNvm9RLLkz5bXqwWcsQ9Zo7XuKAH6jRSp** (Huobi 1) ha sido realizada a través de las transacciones con hash:

434b74344e90ceb0dd4cba33840efb22ba52d173e8c93fbac5d884c85c32845b

b5f6f9926732327c43b41dd4ca8a11d772a20f2ca7c81278ceb88164a13f969d





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

445addb4e6c7f8b21c03c013bf9593dc264f220662e4094732c5af9175e9a9e9
6d7a62779530d3923b52c78e79e96d77c6f4d8eac0fa5816fbe35618629d8bd1
e8160ef4af9a300df5f04e431be701987609e6b9a5698c558664c497443b14d9
764e9aeec6412a845175e1e98704f458bbf9fcd5869291cd237853d9d372f729
a8324798c2d520247b8d775648f923c0c4f2eee746bad123e183112190501c50

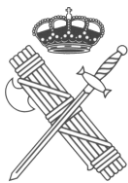
La salida de fondos hacia la dirección **1MB8JPgu2T8J7MSQCZpfbgYLwhBxNsFZGE (Huobi 2)** ha sido realizada a través de las transacciones con hash:

d535499d0fb8c74eb54c4a21fda7897141e1724d34a2380002763edd296687a3
2a5c7cf4ab7963e83eeb739cd19ae19c5fd6b8e62b14f788841e6399bbc01632
238d5d582cbcd63b47705b31cf8177c1cdee7fb9ff8ff46d24e643e7ac2d2bb8
c3e1b66fbec4b9e56987bae70ea543445bd5fbc366ad690e59be272138ec4d37
b3ebe716e5fe7cf83f37d1f61025d2207457b95d6bca95c2e67b0cb91b1fcf82
7c0c62ab23dd72258b3b25fcd998503ba0744983580ccafbe632a18f411d3c0d
8a356007e5e1edb13fbec69519fbf6103dbaaf7ee07a7678a77f3ebf62442226
1e3df5c53a3d1c36b0e577f1542e8ef5c5331a7fe60f5dedf790c48f26a90af3
9d1dcd37a5add89354a91a43b1210ae54158bcf7ab550cb90806f3c31967cd69
c5094929a2850a54d4ea525c2bb119a3167ae94c85b566ebf4c7273b5fe8749f

La salida de fondos hacia la dirección **1ANWDqQtLwVQqNHuRmxbPbPfcMrCLPtTz188 (Huobi 3)** ha sido realizada a través de las transacciones con hash:

4de4f4f6187133f0e704b132550381875393849f79d39bb72ba0b818c514a1be
def1e74fd82bf33c24fea1045e594c17264098b6bc6bd6af3310a9281dd431b6
37787590f5ce145fbc2a1d7a17668b787f266d69dbeaf642a97d4afab0af64fd
c2078c2aaedcf49923fabb96fe6d8ee2c708d74857fb0e94f6450bcd5189ecdc
cb97ede4e17b50526a162de6edb3be79107e7091c0209256017937d48f78c4e6
9f14b665e708a994d585f2356b0635ac0b08b3f5b4742f0f2c678d79135f259f



DIRECCIÓN GENERAL
DE LA GUARDIA CIVILJEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

6ce4454c105e3cdeca5ce4f3477b6f5f2f524c7a861379a6c3be5e7626e4b74d

ed5d46d2a71b33423ae42ab449647e8245763e7803508594fb1211120d236b9e

eab35bb542f4ea3b1648ecd4fab28d10ef6284b1befce8082e27474386936241

Esto nos indica que los fondos de la víctima han sido enviados en su totalidad a las direcciones del Exchange Huobi nombradas.

Desde la dirección sospechosa el día 7 de Junio de 2022 se realiza una transacción por valor de 0.06 BTCs a la dirección **31y27ae5KdSPUj1SN2hhV5skVjuGDBijZ3** a través del hash **0d91c8df6c222ce3df9cd4c7244956d610281bb68902c296a7113777ed7aa19d**. Esta dirección pertenece al Exchange Changenow y se nombra como **Changenow 1**.

Esto se muestra en la imagen 4.

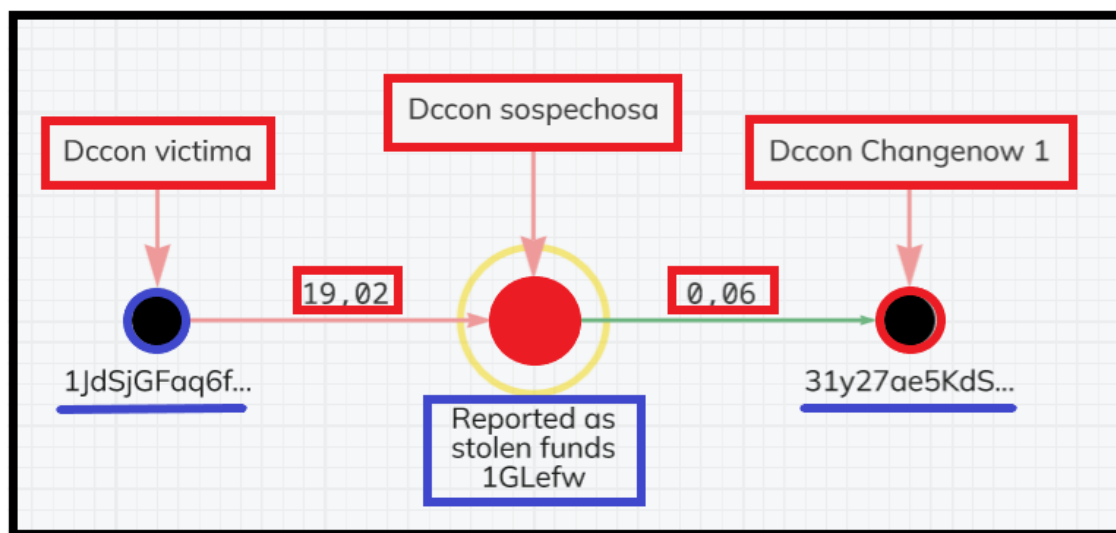


Imagen 4. Entrada de la billetera 31y27ae5KdSPUj1SN2hhV5skVjuGDBijZ3



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

Dicho Exchanger comunica que internamente se ha hecho un swapping (intercambio de criptomonedas) de fondos hacia la dirección **0xA2A158D15e4411Ce505b648faCd114CE004643C9** por la cantidad de 2123.4935 USDTs con el hash **0x888d75413fb99f9d2bf7a4c04419d2019cd6c323362a60036b4f3474dd01feaf**.

El 22 de diciembre de 2021 se realizan dos pagos al Exchanger Bitpay desde la dirección investigada **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE**. Se envían 0.02 BTCs a la dirección **1ABko4cYwKpqAX1RWZvwEBjCY7LroL3xpN** (Bitpay 1) a través del hash **ac23473da2aec17f8075dbf7c61efc90737f2cd0f97260966fd874100fd63208** y 0.02 BTCs a la dirección **1D1K5HDR62JrimpcavzJcAMiK4vRxk8KfD** (Bitpay 2) a través del hash **79591db93f22fbc1f82b37ba099a7b9b51f4abc41edceade4e437f3f55464510**.

Se representa en la Imagen 5.

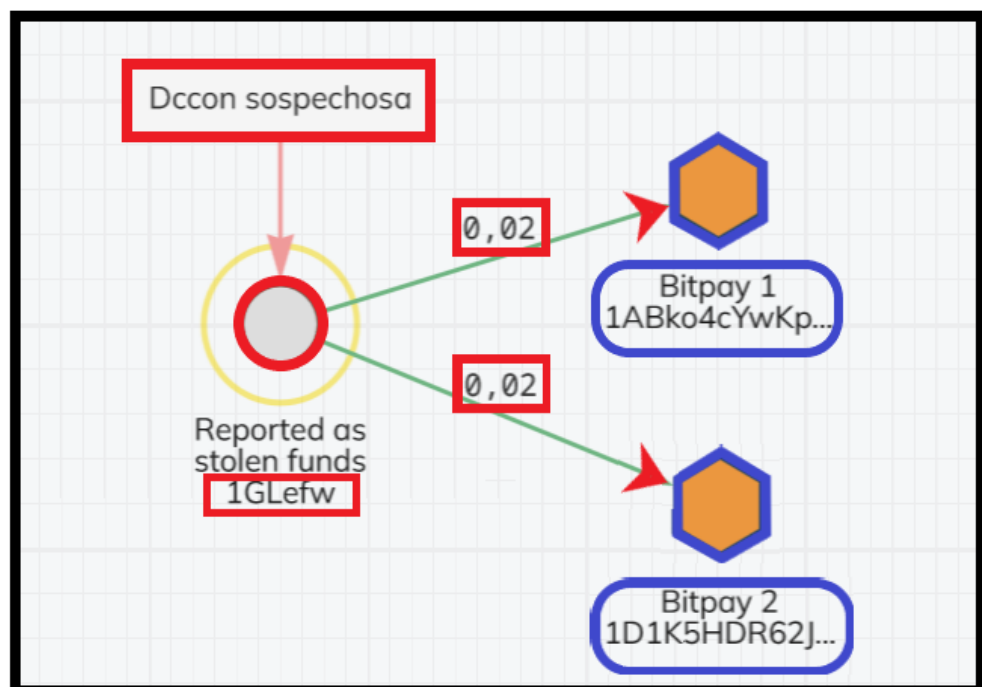
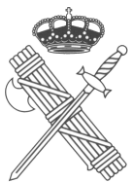


Imagen 5. Salida hacia Bitpay de la billetera 1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE

Tras recibir respuesta del Exchanger Bitpay este contesta lo siguiente:

1.- La dirección **1D1K5HDR62JrimpcavzJcAMiK4vRxk8KfD** (Bitpay 2) está vinculada al usuario con email: filippovaxx@mail.ru y la IP de conexión **31.185.9.236**. Dicha IP está localizada en **Volgograd (Rusia)**, la misma no pertenece a ningún servicio VPN/TOR o similar. Los fondos se envían a una plataforma asociada a la empresa Red-Spark. Dicha plataforma se denomina www.rtxplatform.com. Dicha empresa está localizada en: **3675 Market Street Suite 900 Philadelphia PA United States**.



JEFATURA DE POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

Este usuario también ha usado otra IP dentro de Bitpay para realizar pagos, la cuál es:

31.185.12.99. Dicha IP está localizada en **Volgogrado (Rusia).**

2.- La dirección **1ABko4cYwKpqAX1RWZvwEBjCY7LroL3xpN (Bitpay 1)** está vinculada al usuario con email: krasnovaaz@mail.ru y la IPs de conexión **77.51.87.181 / 213.178.153.21 / 95.73.176.36 / 217.107.127.236**. Todas las Ips están localizadas en la **región de Moscú (Rusia)**, las mismas no pertenecen a ningún servicio VPN/TOR o similar exceptuando la dirección **217.107.127.236** la cuál es un servicio VPN. Los fondos se envían a una plataforma asociada a la empresa Red-Spark. Dicha plataforma se denomina www.rtxplatform.com. Dicha empresa está localizada en: **3675 Market Street Suite 900 Philadelphia PA United States.**

Este usuario también ha usado otras Ips dentro de Bitpay para realizar pagos, las cuales son:

188.255.115.200 / 213.79.89.166 / 212.34.48.14 / 90.154.72.159, todas ellas asociadas a un servicio VPN en Rusia.

La dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** recibe su primera transacción el día 06 de Junio de 2021 a las 07:00 horas a través de la transacción con hash **2d1eb7dd1d53377ebbea23e1502d420d2191c80fa923ce9765a53fdbb9873476**, desde la dirección **3AjepToUrVFDDTWPAQNvFhoreKzE4YjBPA** con la cantidad 0.060328 BTCs.

> 06/06/2021 07:00	2d1eb7dd1d53377eb...	0,060328	1GLefw1owvMqs5azmjV79NH...	● 3AjepToUrVFDDTWPAQNvF...
--------------------	----------------------	----------	----------------------------	----------------------------

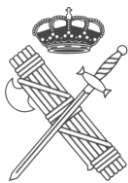
Imagen 6. Transacción de entrada de fondos de la dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE**

Se procede a analizar de dónde proceden los fondos de la dirección **3AjepToUrVFDDTWPAQNvFhoreKzE4YjBPA**, la cual puede tener vinculación importante ya que es la que envía fondos por primera vez a nuestra dirección sospechosa original.

Además en dicha transacción no existe dirección creada con los fondos sobrantes, por lo cual existe una fuerte evidencia de que la dirección **3AjepToUrVFDDTWPAQNvFhoreKzE4YjBPA** y la sospechosa original pueden pertenecer al mismo propietario.

La transacción con hash **b92b22b6ffb42272e050101d8fa5eef189c70724770a4f251c94fded60ffe15c** que recibe la dirección **3AjepToUrVFDDTWPAQNvFhoreKzE4YjBPA** desde la dirección **bc1q5haydyr5z9hq3uez5k084c9jkl6u55jeyzkrnq** consiste en la misma cantidad 0.0603 BTCs y además no hay dirección que acoja a fondos sobrantes por lo cual se evidencia, igual que anteriormente, que la dirección **bc1q5haydyr5z9hq3uez5k084c9jkl6u55jeyzkrnq** y la dirección **3AjepToUrVFDDTWPAQNvFhoreKzE4YjBPA** pertenezcan al mismo propietario.



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

La dirección **bc1q5haydyr5z9hq3uez5k084c9jkl6u55jeyzkrnq** recibe el día 05/06/2021 todos sus fondos desde una dirección del Exchanger Binance a través del hash **de2204c532afba00fe8e2a423ad39c7992b327f5b64074407badf88c46c9758a** por la cantidad descrita anteriormente 0.0603 BTCs.

Solicitada información al Exchanger Binance, la dirección que envía los fondos pertenece al usuario: **BARIS SONMEZ**. Existen varias evidencias de que dicho usuario o la persona que controla dicha cuenta de Binance es el que pueda tener el control de la dirección sospechosa original.

De dicho usuario se da una descripción más amplia en el punto de Respuesta del Exchanger Binance.

En la Imagen 7 se muestra toda la operativa de entrada de la operación sospechosa.

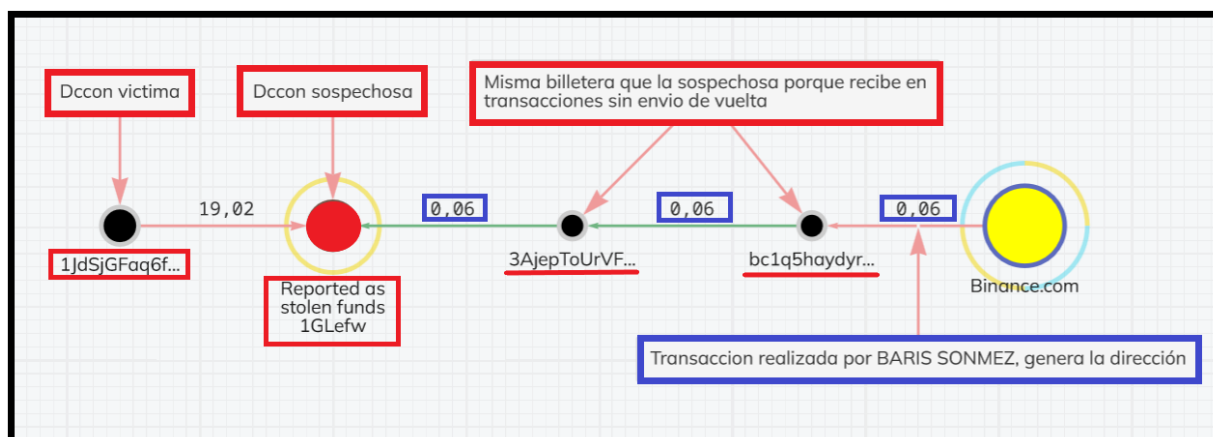


Imagen 7. Flujo de entrada de fondos de la dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** desde Binance

4.1.2.- Dirección de Ethereum **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A**

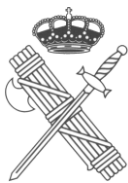
Esta dirección recibe desde la dirección de la víctima **0x802f4501e5632f7934d3011aB2d8263C91d0cB63** el día 8 de junio de 2021 los 13.53 ETHs sustraídos a través de las transacciones:

0x11a2a1e80035c2befc8a152af955d020b475b1ae29e0b7be07b799079cc6389e

0x2e8dcdf831642f495d087d64be260adbc3601bd39f721ec32839de547bef40ea

La billetera **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A** se compone de una única dirección y ha realizado 184 transferencias dónde ha recibido 23.311412 ETHs y ha enviado 22.651929 ETHs.



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

0xd0E6c719259955b3815e67ac22755fCdb72Ef06A			
Balance:	0,000573 ETH	Transfers:	184
Sent:	22,651929 ETH	Withdrawals:	136
Received:	23,311412 ETH	Deposits:	48
Total Fees:	0,658909 ETH	Addresses:	1

Imagen 8. Composición billetera 0xd0E6c719259955b3815e67ac22755fCdb72Ef06A

En la Imagen 9 se observa como desde la dirección **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A** se han enviado de manera directa 9.88 ETHs a la dirección **0x52dE8D3fEbd3a06d3c627f59D56e6892B80DCf12**, la cuál está alojada en el Exchanger Bitpay a través de VEINTIDOS transacciones entre el 17 de Junio de 2021 y el 21 de Septiembre de 2021.

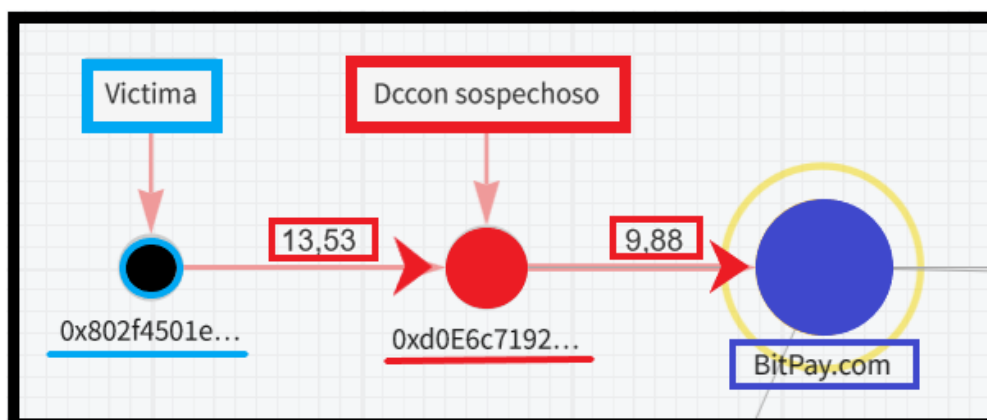


Imagen 9. Salida directa billetera 0xd0E6c719259955b3815e67ac22755fCdb72Ef06A hacia Bitpay

Las transacciones hacia el Exchanger Bitpay tienen los siguientes hash:

0xa526f3da2827615488b284754f7b9be5683041e37d6584e12d80c98bad085dfb

0xb8e83afe32d4e039db06dc9995fb03726beb7277accb8bd4b05a34c5e029fef5

0x52495c182d117380b7b0fd92726e1213c2ee897a5ace431c92e4dfaae908310b

0x2ce105c7be256ee2b5687ee541ccdbd79eedbc39cbb86c7bad4e13796060a7b

0x82c19d1a16832887a46c59a09a34582170f6eac75fdd7dd556f9df79e320d09c

0xb0a3b1591248193226b2b7e4678b1e62457275915c519d63c95d1ad9b7c245bc

0x90d2bd628f84b6d92a54b7ace325dbbcc94099184a61de4b11dfd83663312125





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

0xe636a5e8e2b858b49dedfb65fbed017e273d3ab8c80582d66b943fa9dda05163

0xc15557172e6cf4fc6193aa1fcc1c5587b2bea688209b00e32b3d4e51c2c4b9a5

0x11df470082a21ce86e66860c31b2a23745e2d3b21e97457140b8ec3958534763

0xb3f67c75fd4d3b733f48e703ad57b76df93ab36c56c0a1958de0897be40959c0

0x2837c7ce3fddd9c82522f6f00f16fe0b4c72944eb002b2cc9489dc53a9540074

0x54b86b0c79f616af3215caf0b235de97bd84e77b1d119c0472f1d5f465e89317

0x842de78b354c39deb2d6cc9e28b7ee37a7e615e01151441c2f522b6ec9854255

0x378b1f0321f947fec141aea56560a99da3d0293d0250148f7362edb31e8d3242

0xe03f3b8128c5fa02f44986d2c9f6d47b79954b85938d4c5f3579729f0eb6de74

0x490ebfaea0b3dec0c39d3920205228ef84ea659c6b6cf612600a8421111f1e11

0xa471e6c9061f1511a10c3cec59878622456bba88e40815cf944aec4f227f8a39

0x2ac5427c462c4bb9f8bd0f20e3de151c1ee24973513eede15eeb9dd99413a714

0x4fea3138de9e85377a4015f989166d0230ddda735f7ee8cd0065979c20e8b1b7

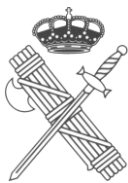
0x801b644fcf47cd99401f1766f7f83f802e69480702e09ee93f8c625b93f94b7d

0x386097c82b68c4c03cad9d97f50c455a784011ed01bb1f031ffff9356f265ce3

Tras solicitar información al Exchanger Bitpay se obtiene la siguiente respuesta:

yura.ishchuk@list.ru	0xc15557172e6cf4fc6193aa1fcc1c5587b2bea688209b00e32b3d4e51c2c4b9a5
yura.ishchuk@list.ru	0x90d2bd628f84b6d92a54b7ace325ddb9c94099184a61de4b11dfd83663312125
yura.ishchuk@list.ru	0x2ce105c7be256ee2b5687ee541ccdbd79eedbc39cbb86c7bad4e13796060a7b
yura.ishchuk@list.ru	0xa526f3da2827615488b284754f7b9be5683041e37d6584e12d80c98bad085dfb
nikitapss@bk.ru	0xe03f3b8128c5fa02f44986d2c9f6d47b79954b85938d4c5f3579729f0eb6de74
initpert@gmail.com	0x2837c7ce3fddd9c82522f6f00f16fe0b4c72944eb002b2cc9489dc53a9540074
initpert@gmail.com	0xe636a5e8e2b858b49dedfb65fbed017e273d3ab8c80582d66b943fa9dda05163
initpert@gmail.com	0x52495c182d117380b7b0fd92726e1213c2ee897a5ace431c92e4dfaae908310b
initpert@gmail.com	0x2fc5c580de1b94a6a352e9b37db7a08125a2a69f1ecb471328e1083963dcca98
initpert@gmail.com	0x47c14b60075cd2ecaeb53f314f8c35c5fdc7f991efc47dbe178967204986e55
initpert@gmail.com	0x3bff4b4ae009dd838c56c31853bcadc45fd586bd0b23a04f334626f1a7c2e70b
initpert@gmail.com	0x3dc6c62f729b85e60dbeb84ea31fd73f39c22a4bc8b4feaa5e1b0c24fd3ab18f
initpert@gmail.com	0x19f79d34fd1fc043a2a520b97ca99b7c3966d512fa2576061188ef494d5ed1c5
initpert@gmail.com	0x62415d98150fc3fc171893c248630a171e4b243e6e2c9275401a776ba8843d7e
initpert@gmail.com	0xd02aa9bc73561cdddc685043761ee55f8e4b3bb7580494616c30e3573e7f0a6
initpert@gmail.com	0xfec5fa92a7b75108f5fbb408e843fbf7774818f9b07df86504c8c5ed5b4277bb



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

antonianse@mail.ru	0x54b86b0c79f616af3215caf0b235de97bd84e77b1d119c0472f1d5f465e89317
kravcobn@yandex.ru	0x378b1f0321f947fec141aea56560a99da3d0293d0250148f7362edb31e8d3242
lancel@inbox.lv	0x4fea3138de9e85377a4015f989166d0230ddda735f7ee8cd0065979c20e8b1b7
lancel@inbox.lv	0x2ac5427c462c4bb9f8bd0f20e3de151c1ee24973513eede15eeb9dd99413a714
akruglovv@bk.ru	0xb3f67c75fd4d3b733f48e703ad57b76df93ab36c56c0a1958de0897be40959c0
akruglovv@bk.ru	0x11df470082a21ce86e66860c31b2a23745e2d3b21e97457140b8ec3958534763
akruglovv@bk.ru	0xb0a3b1591248193226b2b7e4678b1e62457275915c519d63c95d1ad9b7c245bc
akruglovv@bk.ru	0x82c19d1a16832887a46c59a09a34582170f6eac75fdd7dd556f9df79e320d09c
akruglovv@bk.ru	0xbec83afe32d4e039db06dc9995fb03726beb7277accb8bd4b05a34c5e029fef5
akruglovv@bk.ru	0x1524e6597bd65e81c8fd9d784d42a57bb95259d59ac24e7de5c01e5991df6f6
ziminakier@mail.ru	0xa471e6c9061f1511a10c3cec59878622456bba88e40815cf944aec4f227f8a39
ziminakier@mail.ru	0x490ebfaea0b3dec0c39d3920205228ef84ea659c6b6cf612600a8421111f1e11
efogore@yandex.ru	0x842de78b354c39deb2d6cc9e28b7ee37a7e615e01151441c2f522b6ec9854255
dementi@inbox.lv	0x386097c82b68c4c03cad9d7f50c455a784011ed01bb1f031ffff9356f265ce3
dementi@inbox.lv	0x801b644fcf47cd99401f1766f7f83f802e69480702e09ee93f8c625b93f94b7d

Imagen 10. Emails asociados a cada transacción en Bitpay

Todos los usuarios descritos en los cuadros de transacciones anteriores operan a través de IPs pertenecientes a VPNs y envían sus fondos a una plataforma asociada a la empresa Red-Spark. Dicha plataforma se denomina www.rtxplatform.com. Dicha empresa está localizada en: **3675 Market Street Suite 900 Philadelphia PA United States**.

Esta forma de envío de fondos es la misma utilizada por los usuarios que recibieron fondos sustraídos a través de Bitpay en las direcciones bitcoins.

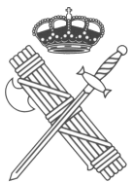
La dirección sospechosa también realiza 3 envíos al Exchanger Whitebit que serían los siguientes:

- **0x3b2f45cEf13dCe7422774E8d10590976eE8b3A4D** recibe 0.20 ETHs a través de la transacción con hash **0xb9050dfd16e774b10ced30dbb439a41f5dd61a6d297f0758acd642a9b81dfbb5**
- **0x6551ACC4946d932f30B398ab32d1277Bc9848C77** recibe 0.12 ETHs a través de la transacción con hash **0x6c706ae2d27859710f609b088b954762e8710dee62cc43ab13a367a6e667ceea**
- **0xB68EC00B541F09c3067933b92Fa744C3182550b0** recibe 0.19 ETHs a través de la transacción con hash **0xa8800a0f653a60cd2afd026a5247f2b4d2273b9ef4e34332284e02c3431b4952**

Tras solicitud al Exchanger Whitebit nos comunica que estas tres direcciones son usadas por su plataforma para realizar intercambio de Ethereum a otras criptomonedas. Nos facilita la siguiente información de las mismas:

- Tx **0xb9050dfd16e774b10ced30dbb439a41f5dd61a6d297f0758acd642a9b81dfbb5** enviada el 05 de Agosto de 2021 se han convertido los fondos a 503,19 Dólares americanos



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

y ha sido realizada por el usuario **koslok@pm.me**, a través de la conexión IP **84.237.179.41** y ha recibido la cuenta de la empresa Webmoney con número **Z120853428242**

- Tx **0x6c706ae2d27859710f609b088b954762e8710dee62cc43ab13a367a6e667ceea** enviada el 01 de Septiembre de 2021 se han convertido los fondos a 26487.39 Rublos y ha sido realizada por el usuario **koslok@pm.me**, a través de la conexión IP **188.112.162.67** y ha recibido el dinero a través de la plataforma Qiwi el número de teléfono **+79675554903**

- Tx **0xa8800a0f653a60cd2afd026a5247f2b4d2273b9ef4e34332284e02c3431b4952** enviada el 01 de Septiembre de 2021 se han convertido los fondos a 600,54 Dólares americanos y ha sido realizada por el usuario **koslok@pm.me**, a través de la conexión IP **188.112.162.67** y ha recibido la cuenta de la empresa Webmoney con número **Z120853428242**

Esta operativa se observa en la Imagen 11.

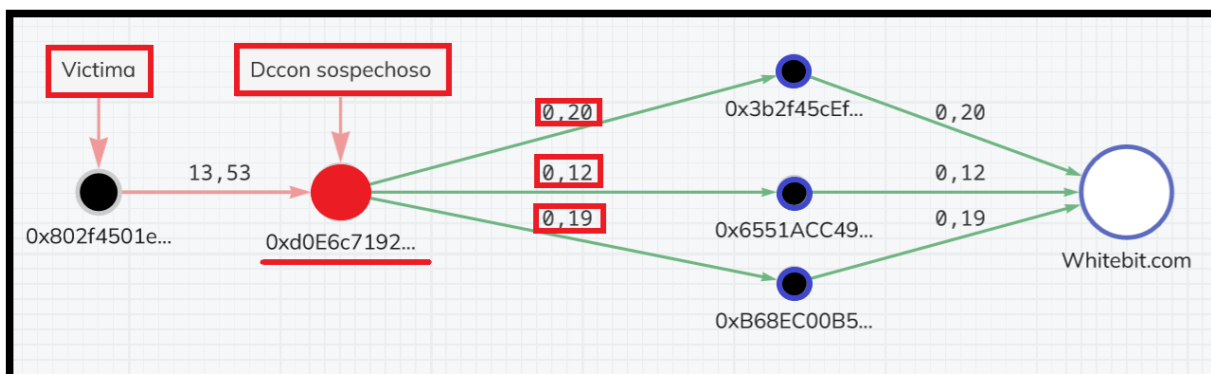


Imagen 11. Salida directa billetera 0xd0E6c719259955b3815e67ac22755fCdb72Ef06A a Whitebit

4.1.3.- Dirección de ETH 0x2EDD429e53dD6C3bf33830103b736462587416D8

Dicha dirección recibe 0.156590761 ETHs de la dirección sospechosa **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A** el 08/10/2021 a través de la transacción con hash **0xaa006104334fece956b8e52da84972d5dd3d44adc10c09f1fee3b1782e17eedb**.

La dirección **0x2EDD429e53dD6C3bf33830103b736462587416D8** envía 0.115225 ETHs a la dirección **0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C** el día 03/03/2022 a través de la transacción **0x338afe493b96daf0325eeb5f9ed0814b2c62a67bc6a997adcd90cfbe97e9277f**.



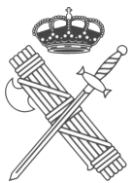
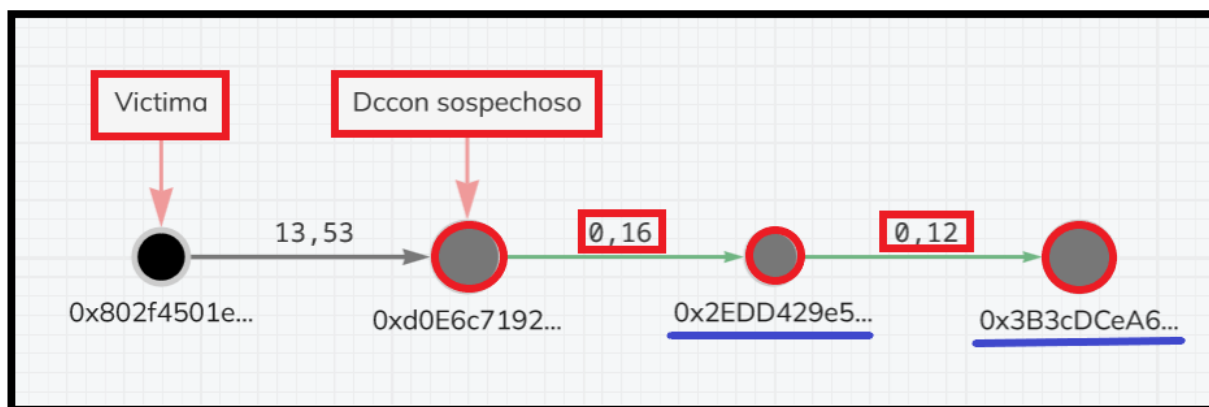
JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

Imagen 12. Vinculación dirección 0x2EDD429e53dD6C3bf33830103b736462587416D8 (ETH)

La dirección **0x2EDD429e53dD6C3bf33830103b736462587416D8** también hace un swap* de fondos a la criptomoneda USDC y envía 119772 USDCs a la dirección **0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C** a través de la transacción **0x209a953f74b7912330eba79546a5078f16179ee25e02c8a52296acf80f354607**. Dicha información está extraída del explorador de la blockchain de la red Ethereum <https://etherscan.io>



Imagen 13. Cambio a USDC hacia 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C

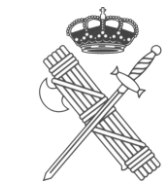
Esto vincula a estas dos direcciones debido a que reciben transacciones en dos distintas criptomonedas.

4.1.4.- Dirección de ETH 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C

Dicha dirección como se ha comentado anteriormente recibe 119772 USDCs de la dirección **0x2EDD429e53dD6C3bf33830103b736462587416D8**.

También recibe 0.15 ETHs de la dirección **0x23D76b0f15C87Bc116347595D7d6Cd13cf252C94** a través del hash **0xfeace26b47da97275427d2e994038446fcd190976146657694cc2571beaedeb0**. A su vez la dirección **0x23D76b0f15C87Bc116347595D7d6Cd13cf252C94** ha recibido 1.54 ETHs de la dirección **0xA2A158D15e4411Ce505b648faCd114CE004643C9** a través del hash **0x7b6f3367bedb63ef71675244471a90cb295e4e9f150d7eb592de74a105cab84a**. Esta última dirección es la que recibió los fondos de la dirección **31y27ae5KdSPUj1SN2hhV5skVjuGDBijZ3** que realizó el swap* en el Exchanger Changenow a USDT.





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

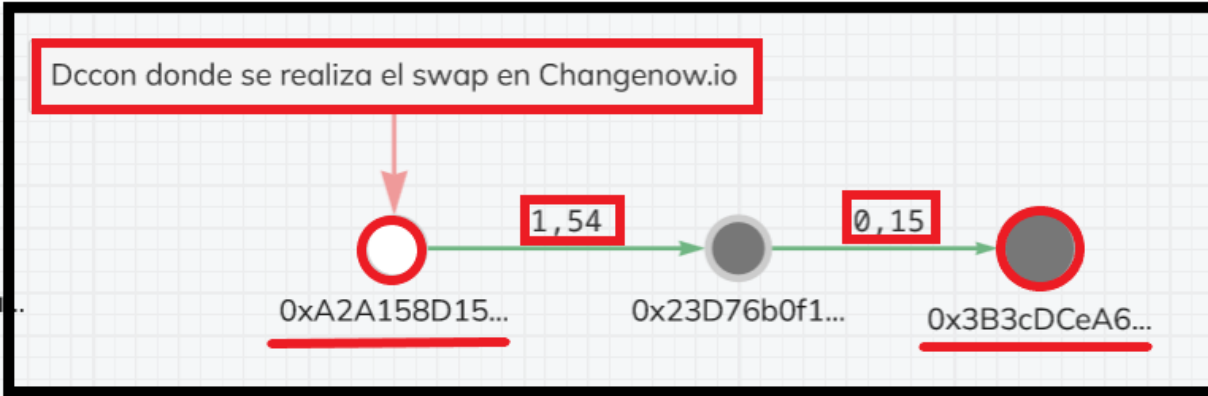


Imagen 14. Conexión de 31y27ae5KdSPUj1SN2hhV5skVjuGDBijZ3 con 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C

Estas evidencias demuestran que las direcciones 0xA2A158D15e4411Ce505b648faCd114CE004643C9, 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C y la dirección de BTC 31y27ae5KdSPUj1SN2hhV5skVjuGDBijZ3 están vinculadas.

Se procede a analizar más operativa de la dirección 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C, ya que la misma está siendo usada para aglutinar fondos y redistribuirlos entre otras direcciones tanto en Ethereum como en USDT.

Root Address	Balance:	0,00 USDT_ETH	Transfers:	24
0x3B3cDCeA62E8bb7d5000E875...	Sent:	1.199.012 USDT_ETH	Withdrawals:	13
	Received:	1.199.012 USDT_ETH	Deposits:	11
Watch	Total Fees:	0,00 USDT_ETH	Addresses:	1

Imagen 15. Composición dirección 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C (USDT)

En la imagen 15 se observa como la dirección 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C ha recibido y enviado un total de 1.199.012 USDT, que son equivalentes a 1.199.012 dólares americanos. Ha recibido un total de 11 depósitos y ha enviado un total de 13 transacciones de salida.



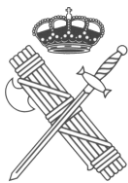
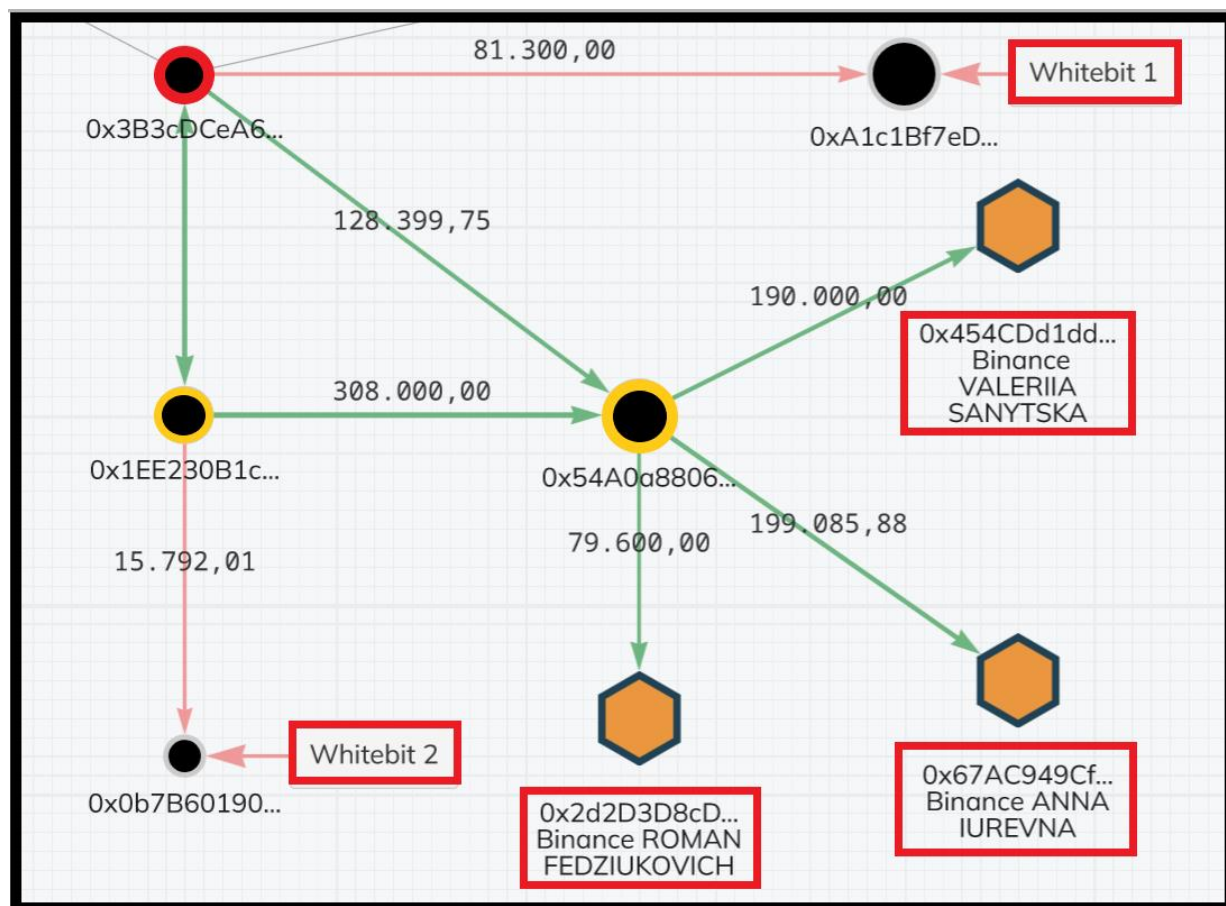
DIRECCIÓN GENERAL
DE LA GUARDIA CIVILJEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

Imagen 16. Operativa salida de la dirección 0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C

Se va a proceder al análisis de la Imagen 16 dónde se observa toda la operativa de salida de fondos de la dirección **0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C**.

Se envían 81.300 USDTs a la dirección **0xA1c1Bf7eDB87c6D73B7F3307274f19813B450cFe**, la misma pertenece al Exchanger Whitebit y se nombra como **Whitebit 1**. Tras solicitar información a dicho Exchanger nos comunica que es una dirección de tránsito usada para realizar cambios de criptomonedas y que en este caso dicha transacción se ha recibido por parte del siguiente usuario:

NikolayVasenkovich95@protonmail.com (Ilya)

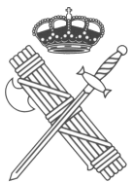
IP: 212.188.29.35 (Rusia)

Perfil de telegram: @askmeso

Se envían 128.399,75 USDTs a la dirección **0x54A0a8806834767915F981422f229a02718F49Cd**.

Se envían 686.167,55 USDTs a la dirección **0x1EE230B1c4A6c073482fF6eA6f339c15140b0EEa**.



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

Ambas direcciones, **0x54A0a8806834767915F981422f229a02718F49Cd** y **0x1EE230B1c4A6c073482fF6eA6f339c15140b0EEa** son usadas como acumuladores para poder realizar posteriores envíos a otras direcciones.

La dirección **0x1EE230B1c4A6c073482fF6eA6f339c15140b0EEa** realiza dos envíos:

- Uno de 308.000 USDTs a la dirección **0x54A0a8806834767915F981422f229a02718F49Cd**, con lo cuál se consolida la vinculación entre ambas y la dirección **0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C**

- Otro de 15.792,01 USDTs a la dirección **0x0b7B601900A846dafc95a781db6611A0664D5f7A**, la cuál pertenece al Exchanger Whitebit y se nombra como **Whitebit 2**. Tras solicitar la información a dicho Exchanger el mismo comunica que es una dirección de tránsito propia para realizar cambio a otras criptomonedas. Dicha transacción ha sido recibida por el usuario:

goshatihonovski@protonmail.com

IP: 46.164.228.239

Este usuario a su vez ha hecho una conversión de los fondos a la criptomoneda UAH por valor de 493000 UAHs.

Como último vínculo importante la dirección **0x54A0a8806834767915F981422f229a02718F49Cd** envía fondos a 3 direcciones pertenecientes al Exchanger Binance:

- La dirección **0x454CDd1dd133aD861114860Ac5252b64DA82999** recibe 190.000 USDTs, está asociada a la usuaria **VALERIIA SANYTSKA** y posteriormente se ampliará información de dicha dirección.

- La dirección **0x67AC949Cf1B5b1ffb4f2009c1BA661c58C2De08B** recibe 199.085,88 USDTs, está asociada a la usuaria **ANNA IUREVNA** y posteriormente se ampliará información de dicha dirección.

- La dirección **0x2d2D3D8cD3F83170f46fe912f2b698042cb561Be** recibe 79.600 USDTs, está asociada al usuario **ROMAN FEDZIUKOVICH** y posteriormente se ampliará información de dicha dirección.

4.1.5. Dirección **0xA2A158D15e4411Ce505b648faCd114CE004643C9**

Como se comentó anteriormente dicha dirección recibe fondos desde Changenow debido a un cambio de criptomoneda de 0.64 ETHs.

Esta dirección, como se muestra en la Imagen 16, recibe 1.55 ETHs de la dirección **0x04fc145Ba47Bc0952c6b90e3d3CdD42f5cA96333**, esta dirección recibe todos sus fondos desde la cuenta de Binance del usuario **BARIS SONMEZ**, del cuál se ha realizado una análisis previo en la criptomoneda BTC. Estos dos hechos vinculan directamente a dicho



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

usuario con las direcciones sospechosas, desconociéndose el papel del mismo pero pudiendo ser relevante.

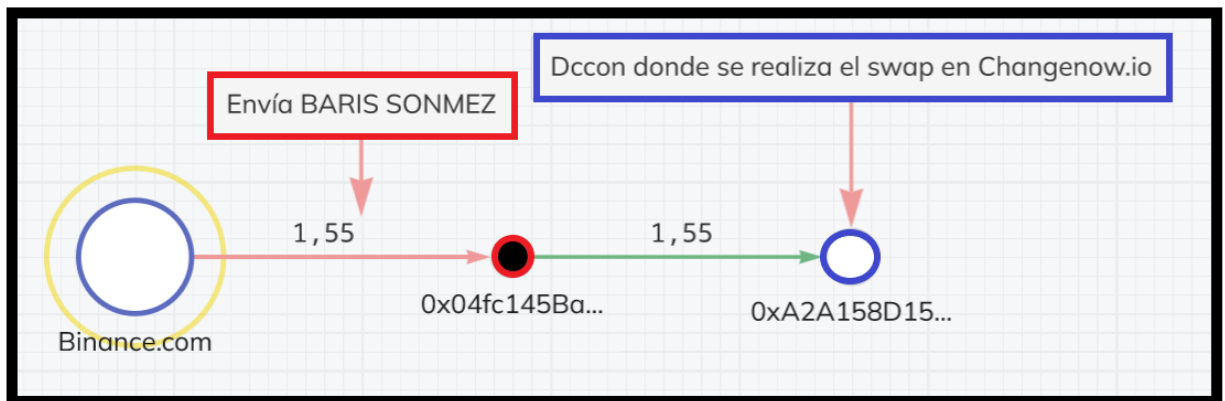


Imagen 17. Operativa entrada fondos de la dirección 0xA2A158D15e4411Ce505b648faCd114CE004643C9

En la Imagen 18 se observa la salida de fondos desde el usuario **BARIS SONMEZ** hacia al dirección **0x04fc145Ba47Bc0952c6b90e3d3CdD42f5cA9633**. Esta transacción se realiza el mismo día 05 de junio de 2021, al igual que la transacción de envío en BTCs a la dirección sospechosa original.

User ID	Currency	Amount	Destination Address	Apply Time
81800745	ETH	1.54441323	0x04fc145Ba47Bc0952c6b90e3d3CdD42f5cA96333	2021-06-05 11:34:19

Imagen 18. Operativa salida fondos ETH del usuario BARIS SONMEZ

4.1.5.- Respuestas de exchanger Binance

En base a lo expuesto en el informe se realiza solicitud policial al exchanger **Binance** para la obtención de información de los usuarios que gestionan las direcciones de este exchanger y que reciben fondos de las billeteras investigadas, en la respuesta de este exchanger se obtiene la siguiente información.

Binance nos facilita la información sobre las transacciones: **0xe13ef8c8895877c1f46d2bb0de06f764acac30315235909989ac4d09b8954eca** y **de2204c532afba00fe8e2a423ad39c7992b327f5b64074407badf88c46c9758a** están vinculadas el usuario: **BARIS SONMEZ**, nacido el 08-09-1986, con permiso de conducir holandés con número 5735082554, email barisvansonmez@hotmail.com y número de teléfono +31622305636.





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL



Imagen 20. Imagen de documentación y selfie recibida en Binance del usuario BARIS SONMEZ

La dirección **0x454CDd1dd133aD861114860Acf5252b64DA82999** nos facilita Binance que está asociada al usuario: **VALERIIA SANYTSKA**, nacida el 18 de septiembre de 2001, con pasaporte ucraniano número GB235999 y con email denisshnipov@gmail.com.



Imagen 21. Imagen de documentación y selfie recibida en Binance de la usuaria VALERIIA SANYTSKA

La dirección **0x67AC949Cf1B5b1ffb4f2009c1BA661c58C2De08B** nos facilita Binance que está asociada al usuario: **ANNA IUR'EVNA SHMYGLIA**, nacida el 03 de Octubre de 1992, con permiso de conducir ruso con número 7735727977 e email alexzmitrovich91@gmail.com.





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

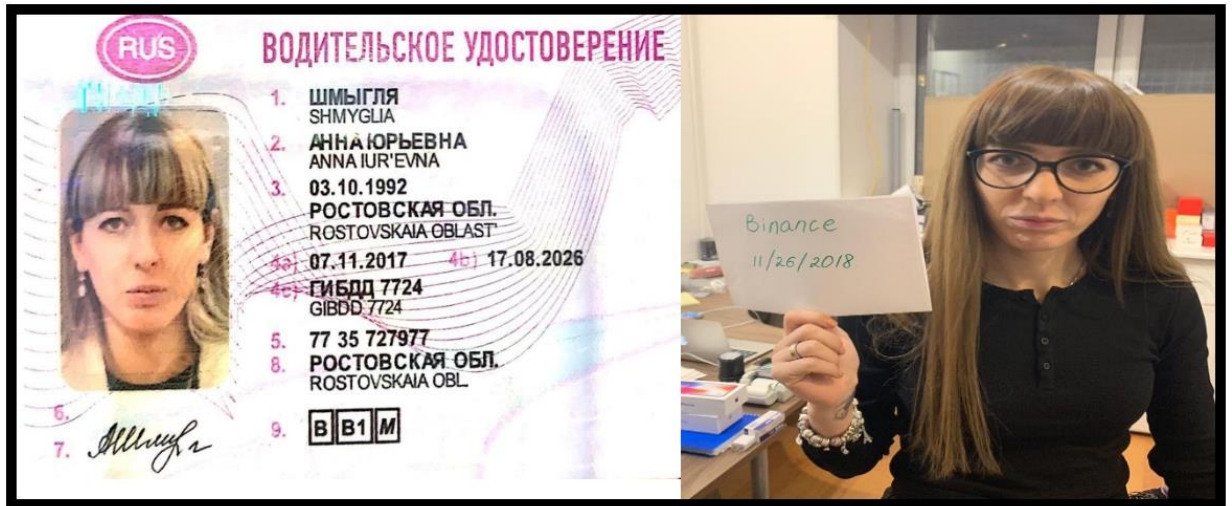


Imagen 22. Imagen de documentación y selfie recibida en Binance de la usuaria ANNA IUR'EVNA SHMYGLIA

La dirección **0x2d2D3D8cD3F83170f46fe912f2b698042cb561Be** nos facilita Binance que está asociada al usuario: **ROMAN FEDZIUKOVICH**, nacido el 24 de abril de 1997, con carnet de identidad de Polonia con número DBA799458, con email rfedyukovich@me.com y teléfono +48731262470.

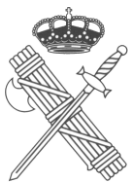


Imagen 23. Imagen de documentación y selfie recibida en Binance del usuario ROMAN FEDZIUKOVICH

4.1.6.- Respuestas de Exchanger Whitebit

La transacción **0xb9050dfd16e774b10ced30dbb439a41f5dd61a6d297f0758acd642a9b81dfbb5** ha sido realizada por el usuario:





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

koslok@pm.me

IP de conexión: 84.237.179.41

ID en Webmoney que recibe los fondos: Z120853428242

La transacción
0x6c706ae2d27859710f609b088b954762e8710dee62cc43ab13a367a6e667ceea ha sido
realizada por el usuario:

koslok@pm.me

IP de conexión: 188.112.162.67

Número de teléfono que recibe fondos a través de Qiwi: +79675554903

La transacción
0xa8800a0f653a60cd2afd026a5247f2b4d2273b9ef4e34332284e02c3431b4952 ha sido
realizada por el usuario:

koslok@pm.me

IP de conexión: 188.112.162.67

ID en Webmoney que recibe los fondos: Z120853428242

La dirección **0xA1c1Bf7eDB87c6D73B7F3307274f19813B450cFe (Whitebit 1)** recibe una
transacción la cuál ha sido recibida por el usuario:

NikolayVasenkovich95@protonmail.com (Ilya)

IP de conexión: 212.188.29.35 (Rusia)

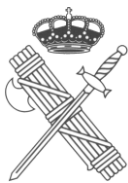
Perfil de telegram: @askmeso

La dirección **0x0b7B601900A846dafc95a781db6611A0664D5f7A (Whitebit 2)** recibe una
transacción la cuál ha sido recibida por el usuario:

goshatihonovskiy@protonmail.com

IP de conexión: 46.164.228.239 (Rusia)





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

4.1.7.- Respuestas de procesador de pagos BitPay

La dirección **1ABko4cYwKpqAX1RWZvwEBjCY7LroL3xpN (Bitpay 1)** está vinculada al usuario con email: krasnovaaz@mail.ru y la IPs de conexión **77.51.87.181 / 213.178.153.21 / 95.73.176.36 / 217.107.127.236**

La dirección **1D1K5HDR62JrimpcavzJcAMiK4vRxk8KfD (Bitpay 2)** está vinculada al usuario con email: filippovaxx@mail.ru y la IP de conexión **31.185.9.236**

Todas las transacciones realizadas en Ethereum hacia Bitpay son recibidas por los siguientes usuarios:

yura.ishchuk@list.ru

nikitapss@bk.ru

inipert@gmail.com

antonianse@mail.ru

kravcobn@yandex.ru

lancel@inbox.lv

akruglovv@bk.ru

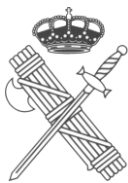
ziminakier@mail.ru

efogore@yandex.ru

dementi@inbox.lv

Todos los usuarios de Bitpay, después de recibir los fondos a través de la plataforma, son enviados a través de la empresa www.rtxplatform.com



JEFATURA DE POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

5.- Conclusiones

La dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** sospechosa que recibe los **24.46502798 bitcoins** robados de la víctima son enviados al exchanger **Huobi** a través de tres direcciones **1LNvm9RLLkz5bXqwWcsQ9Zo7XuKAH6jRSp** (Huobi 1), **1MB8JPgu2T8J7MSQCZpfbgYLwhBxNsFZGE** (Huobi 2) y **1ANWDqQtLwVQqNHuRmxbPbPmrcLPtTz188** (Huobi 3).

Los usuarios de dichas direcciones están vinculados directamente con la sustracción de fondos.

La dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** sospechosa envía 0.04 BTCs a dos direcciones del Exchanger Bitpay, siendo estas **1ABko4cYwKpqAX1RWZvwEBjCY7LroL3xpN** (Bitpay 1) y **1D1K5HDR62JrimpcavZJcAMiK4vRk8KfD** (Bitpay 2).

Los usuarios de dichas direcciones están vinculados directamente con la sustracción de fondos.

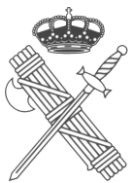
La dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** sospechosa recibe 0.06 a través de 3 direcciones vinculadas a ella directamente, siendo la última de estas una dirección vinculada el usuario del Exchanger Binance: **BARIS SONMAZ**.

Dicho usuario está involucrado en el envío de fondos a la dirección investigada mencionada anteriormente, desconociéndose actualmente el papel que desempeña, pudiendo:

1. Podría ser una víctima a la cuál se le han sustraído los fondos de su cuenta de Binance y se han enviado a la dirección sospechosa **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** para crearla.

2. Podría haber facilitado o ser coautor de la sustracción de fondos, ya que es la persona que realiza los envíos directamente a la dirección sospechosa **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE**.



JEFATURA POLICÍA
JUDICIALUNIDAD TÉCNICA DE
POLICÍA JUDICIALGRUPO DE
CIBERINTELIGENCIA
CRIMINAL

La dirección **1GLefw1owvMqs5azmjV79NH4Fgdwvq5sWE** sospechosa envía 0.06 BTCs a la dirección **31y27ae5KdSPUj1SN2hhV5skVjuGDBijZ3 (Changenow 1)**, que pertenece al Exchanger Changenow. Dicho Exchanger comunica que se han convertido a Ethereum y los fondos se han enviado a la dirección **0xA2A158D15e4411Ce505b648faCd114CE004643C9**. Después de analizar la operativa de salida de fondos del usuario de Binance **BARIS SONMAZ**, se observa que también ha enviado fondos a la dirección **0xA2A158D15e4411Ce505b648faCd114CE004643C9**.

La dirección sospechosa de Ethereum **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A** recibe 13,53 ETHs de la dirección de la víctima **0x802f4501e5632f7934d3011aB2d8263C91d0cB63**. Desde esta dirección sospechosa se envían 9,88 ETHs a varias direcciones del Exchanger Bitpay.

Los usuarios de dichas direcciones están vinculados directamente con la sustracción de fondos.

La dirección sospechosa de Ethereum **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A** envía 0.51 ETHs a 3 direcciones del Exchanger Whitebit.

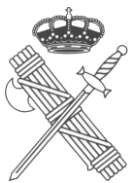
Los usuarios de dichas direcciones están vinculados directamente con la sustracción de fondos.

La dirección puente **0x3B3cDCeA62E8bb7d5000E8754a2f9ee0A80B7A0C**, usada como acumulador de fondos desde la dirección sospechosa **0xd0E6c719259955b3815e67ac22755fCdb72Ef06A** y desde la dirección sospechosa **0xA2A158D15e4411Ce505b648faCd114CE004643C9**, envía fondos a:

- 2 direcciones pertenecientes a dos usuarios del Exchanger Whitebit
- 3 direcciones pertenecientes a tres usuarios del Exchanger Binance

Los usuarios de dichas direcciones están vinculados directamente con la sustracción de fondos.





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

6.- Entrega del Informe Técnico

Se hace entrega del presente Informe Técnico.

El análisis detallado de las direcciones se entrega por conducto y con fecha 22 de junio de 2022 a la Unidad Orgánica de Policía Judicial de Málaga, para el estudio y valoración de la información extractada, dando por concluido este informe que consta de 29 folios útiles, incluyendo índice y portada.

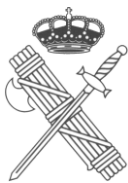
Madrid a 22 de junio de 2022

T89891S

Vº Bº

DIRECCIÓN TÉCNICA





JEFATURA POLICÍA
JUDICIAL

UNIDAD TÉCNICA DE
POLICÍA JUDICIAL

GRUPO DE
CIBERINTELIGENCIA
CRIMINAL

GLOSARIO DE TERMINOS

Blockchain o cadena de bloques: Es una base de datos pública, compartida y descentralizada que funciona como un libro donde se registran operaciones de compra-venta o cualquier otro tipo de transacción. Se utiliza como método de contabilidad para la moneda virtual Bitcoin, que usa Blockchain para garantizar la seguridad de las transacciones.

Chainalysis-Reactor: Reactor es un software de investigación que conecta las transacciones en criptografía con entidades del mundo real, permitiendo combatir la actividad delictiva en la cadena de bloques.

Criptomoneda: Es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido. El control de cada criptomoneda se ejerce mediante el uso de la tecnología Blockchain.

Dirección: Es una identificación alfanumérica única que te permite enviar y recibir criptomonedas de forma rápida, segura y sencilla.

EUROPOL: La Oficina Europea de Policía es el órgano encargado de facilitar las operaciones de lucha contra la delincuencia en el seno de la Unión Europea.

Exchanger/Exchanges: Plataformas o mercados de intercambio. Son plataformas digitales que permiten intercambiar monedas digitales por dinero fiat y/u otras criptomonedas o mercancías. Estas plataformas utilizan una política KYC que nos permite identificar a requerimiento policial o judicial a los titulares o proporcionar información relevante sobre las transacciones y accesos.

Wallet: Hace referencia a una cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos.

