

Investigación sobre Extorsión con Bitcoin y Análisis de la Dirección

Alumno: Dragos Cornel Iván Andrei

Imagina que la empresa XX de tu cliente ha recibido un mensaje de una organización de cibercriminales en el que te comunican que la información bancaria de un listado parcial de tus clientes podría haber sido publicada en la web Pastebin (<https://pastebin.com/>) con un mensaje similar a la pantalla que reproducimos a continuación, con el siguiente mensaje:

«Las cuentas de sus clientes han sido hackeadas. Si no paga 2 bitcoins en la siguiente dirección 1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLD, procederemos a hacer públicos 6 937 081 archivos relativos a su empresa y sus clientes».

El CEO, muy preocupado, contrata tus servicios de investigación para ver si sería posible investigar los hechos. Debes realizar una investigación de la dirección de bitcoin y aportar toda la información posible referente a tus indagaciones. Responde a las siguientes cuestiones concretas:

1. ¿Con qué delitos está relacionada la mencionada dirección de bitcoin y en qué se basa cada uno de los hechos delictivos que comenta? (Máximo de respuesta: 10 líneas de texto). (1 punto)
2. Emplea herramientas como bitcoinabuse <https://www.bitcoinabuse.com/>, la propia web <https://www.blockchain.com/com> de exploración bloques <https://www.blockchain.com/explorer> y <https://www.walletexplorer.com/> y recopila la información técnica de utilidad sobre dicha dirección (correos electrónicos, direcciones Ip, etc. (2 puntos)

- Indica qué pasos deberías realizar para obtener información en fuentes abiertas acerca de la procedencia de los datos técnicos que pudiste encontrar en tu investigación. (2 puntos)

(Máxima extensión de texto de esta pregunta: 2 folios, no incluidos imágenes o capturas que necesite aportar).

- Ahora, con la información de la que dispones, ¿existen posibilidades reales de rastrear el monedero de bitcoin o de saber quiénes son los autores? Tanto en caso positivo como negativo, justifica tu respuesta (2 puntos).
- Indaga en la investigación de tres herramientas (quedan FUERA DE SU PROPUESTA bitcoinabuse <https://www.bitcoinabuse.com/>, la propia web <https://www.blockchain.com/com> de exploración bloques <https://www.blockchain.com/explorer> y <https://www.walletexplorer.com/>) que podrían ser de utilidad para seguir la trazabilidad de las criptomonedas y explorar sus movimientos, ya sea de las propias transacciones como de las billeteras desde donde salen o se reciben dichas transacciones de criptomonedas. No debe estar referida únicamente al bitcoin, sino que debe ser válido para cualquier criptomoneda. (3 puntos).1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd

1. Delitos Relacionados con la Dirección de Bitcoin

Se ha encontrado que con la dirección de Bitcoin

1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLD en general y desde 2020 se han denunciado 8 delitos relacionados con sextortion, 4 ransomware, y 4 de otros tipos relacionados con blackmailing, la mayoría de ellos en idioma croata.

Destacan algunos como:

- Extorsión (Ransomware):** Se han registrado casos donde se exige un pago en Bitcoin a cambio de no divulgar información sensible obtenida ilícitamente. (chainabuse.com)
- Fraude Informático:** Los delincuentes buscan obtener dinero de empresas, ya sea a través de engaños o amenazas relacionadas con la seguridad de la

información.

(chainabuse.com)







3. **Lavado de Dinero.** Se compone de aquellos procedimientos y mecanismos encargados de adquirir y ocultar activos de origen delictivo para introducirlos en el mercado dándoles apariencia de legalidad.

(mandiant.com)

4. **Acceso Ilegítimo a Datos:** Por último, la publicación o venta de datos personales sin consentimiento es una práctica ilegal y ha sido reportada en múltiples ocasiones en relación con direcciones de Bitcoin utilizadas en actividades delictivas. (chainabuse.com)

5. **Sextorsion:** los delincuentes extorsionan a sus víctimas con amenazas de publicar intimidades

A continuación se reflejan algunos de ellos:

| | | |
|---------------------------|--|---|
| Other Blackmail Scam — | Same scam as last, same BTC address - usual scam - sextortion blackmail to my leaked email address, in Croatian language, asking for ,C~950. | ↑ 1 ↓ |
| | Submitted in Bitcoinabuse on Feb 12, 2020 | 0 |
| Reported Address |  1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd  |  |
| Other Blackmail Scam — | Usually scam - sextortion blackmail to my leaked email address, in Croatian language, asking for ,C~950. | ↑ 1 ↓ |
| | Submitted in Bitcoinabuse on Feb 12, 2020 | 0 |
| Reported Address |  1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd  |  |

| | | |
|---|--|-------------|
| Ransomware — | This is abuser | ↑ 1 ↓ |
| Submitted in Bitcoinabuse on Feb 12, 2020 | | 0 |
| Reported Address | 1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd | |
| Sextortion Scam — | Sent on Croatian language. Wants money to not publish a sex video. | ↑ 1 ↓ |
| Submitted in Bitcoinabuse on Feb 12, 2020 | | 0 |
| Reported Address | 1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd | |
| Sextortion Scam — | Sent on Croatian language. Wants money to not publish sex video. Received: from m33-136.eu.mailgun.net (m33-136.eu.mailgun.net. [141.193.33.136])_x000D_ ivana milin (unregistered: i****@adria- | ↑ 1 ↓ |

2. Recopilación de Información Técnica

Para analizar la dirección de bitcoin proporcionada, utilizaremos herramientas como:

- **Bitcoin Abuse Database** (<https://www.bitcoinabuse.com>)
- **Blockchain Explorer** (<https://www.blockchain.com/explorer>)



1Fnjx-dtpLd

Base58 (P2PKH)



Bitcoin Address

1Fnjx9acfxzh9jaL21nsxbx2rrMHydtPLd

Bitcoin Balance

0.00000000 • \$0.00

Summary

This address has transacted 4 times on the Bitcoin blockchain. It has received a total of 0.30524907 BTC \$29,891.60 and has sent a total of 0.30524907 BTC \$29,891.60 The current value of this address is 0.00000000 BTC \$0.00.

Total Received

0.30524907 BTC
\$29,891.60

Transactions

4

Total Sent

0.30524907 BTC
\$29,891.60









Total Volume

0.61049814 BTC
\$59,783.20

Lo primero que salta a la vista es que esta cartera (**1Fnjx9acfxzh9jaL21nsxbx2rrMHydtPLD**) está ya vaciada. En la parte de abajo de la imagen podemos ver un resumen de transferencias y volumen de dinero manejado ("Total Received", "Total Sent" etc.).


En cuanto al historial de transacciones generales en la imagen de abajo encontramos 1 transacción saliente (como la primera con flecha hacia arriba, y 3 transacciones entrantes.

Transactions

| | | | | |
|---|--|--|--|---|
|  | ID: 2344-c2f9 2/26/2020, 06:44:18 | From 139 Inputs To 3Nbe-HHXX | -0.30524907 BTC • -\$29,846.43 Fee 1.4M Sats • \$1,330.28 |  |
|  | ID: c5c5-856d 2/12/2020, 11:25:55 | From 159F-VRQV To 1Fnj-tpLd | 0.10027291 BTC • \$9,804.41 Fee 8.6K Sats • \$8.43 |  |
|  | ID: 298f-5b11 2/12/2020, 09:43:27 | From 328w-bfmN To 17 Outputs | 0.09920625 BTC • \$9,700.12 Fee 21.1K Sats • \$20.66 |  |
|  | ID: 5dab-ec06 2/11/2020, 15:24:19 | From 335F-mad5 To 2 Outputs | 0.10576991 BTC • \$10,341.90 Fee 4.7K Sats • \$4.63 |  |


Si desglosamos la primera transacción, obtendremos que su ID es 2344-c2f9, con el hash 234489228a71563911171fe5c36ea89c833390af2009e757138aa8f72a24c2f9, También se observa el ID del blockchain, el número de posición, la antigüedad, los impuestos que ha pagado por transacción (fee) etc.

Advanced Details

| | | | |
|-------------|---|--------------|----------------------|
| Hash | 2344-c2f9  | Block ID | 619,036 |
| Position | 78 | Time | 26 Feb 2020 06:44:18 |
| Age | 4y 11m 11d 5h 27m 57s | Inputs | 139 |
| Input Value | 6.98347613 BTC | Outputs | 1 |
| | \$684,733 | Output Value | 6.96987089 BTC |
| Fee | 0.01360524 BTC | | \$683,399 |
| | \$1,334.00 | Fee/B | 66.209 sat/B |
| Fee/VB | - | Size | 20,549 Bytes |
| Weight | 82,196 | Weight Unit | 16.552 sat/WU |
| Coinbase | No | Witness | No |
| RBF | No | Locktime | 619,034 |
| Version | 2 | BTC Price | \$98,050.57 |

Aquí observamos más detalles, entre los que destaca que parece que la dirección **1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd** haya recibido fondos de **139 inputs diferentes**. Lo que indica que ha sido usada como **dirección de recepción de múltiples pagos**.

Reports submitted for

3NbeS1bAV9Kh3arFNBtVfmKgE5zZSaHHXX 

No Reports SORT BY ▼

Unreported addresses might still be used in scams so caution is advised. If you suspect this address is being used in a scam, please report it.

Luego, hemos notado que todos esos fondos se enviaron a **una única dirección final: 3NbeS1bAV9Kh3arFNBtVfmKgE5zZSaHHXX**

Características interesantes en la imagen anterior:

- Solo **1 output**, lo que indica que es una transacción de consolidación.
- Esta dirección no tiene registros de actividad delictiva.

Es posible que sea una dirección de cobro "limpia".

De ello deducimos las siguientes explicaciones:

1. Dirección de consolidación de fondos

- A menudo, los ciberdelincuentes recogen pagos en una dirección y luego los transfieren a otra "limpia".
- Esto sirve para **ocultar el origen ilícito** de los fondos antes de moverlos a exchanges o plataformas de conversión.

2. Uso de mezcladores (Bitcoin Tumbling)

- Como decíamos, si la dirección **3NbeS1bAV9Kh3arFNbtVfmKgE5zZSaHHXX** no tiene historial delictivo, podría estar siendo usada para "limpiar" fondos.
- Puede estar asociada a un servicio de mezclado de Bitcoin (tumblers o mixers), que combinan BTC de múltiples fuentes para ofuscar el rastro.

3. Exchanges o Casas de Cambio

- Algunas plataformas de criptomonedas usan direcciones únicas para depósitos, por lo que esta podría ser una cuenta de un **exchange** donde el dinero se retirará o será convertido a otra criptomoneda.

Direcciones IP vinculadas, correos, dominios:

La primera información que nos encontramos son estos dominios:

- **hsi-kbw-046-005-253-181.hsi8.kabel-badenwuerttemberg.de**
- **ip5f5be1c2.dynamic.kabel-deutschland.de**

Posible indicio:

- Son direcciones de servicios de Internet alemanes.
- Probablemente se usaron **VPNs o proxies** para ocultar la ubicación real del atacante.

Correoselectrónicos asociados:

A través de la herramienta <http://www.bitcoinwhoswho.com/>

Hemos encontrado algunos correos asociados en

<https://www.bitcoinwhoswho.com/address/1Fnjx9acfxzh9jaL21nsxbx2rrMHydtPLd>

jjoyce@erdman.co

ainza@millicom.com.ar

comercial@serinfo.com

| Scam Alert | | | |
|---|---|-------|--------------|
| Scam Name | URL | Image | Date |
| — sextortion | | | Feb 11th, 20 |
| jjoyce@erdman.co> | | | |
| Provjerite integritet svojih podataka (prema našoj sigurnosnoj službi važi je račun hakiran | | | Feb 11th, 20 |
| — naguayo@puc.cl | | | Feb 11th, 20 |
| Classic sextortiin | | | |
| — Typical sextortion blackmail scam with leaked email | | | Feb 12th, 20 |
| Feb 11, 2020. at 13:01 CET, ainza@millicom.com.ar via hsi-kbw-046-005-253-181.hsi8.kabel-badenwuerttemberg.de and Feb 11, 2020. at 13:29 CET comercial@serinfo.com.co via ip5f5be1c2.dynamic.kabel-deutschland.de | | | |
| — Poruka preko oglasnika njuskalo | https://www.njuskalo.hr/ | | Feb 12th, 20 |

Se ha encontrado este correo escrito en croata, que vamos a traducir:

Pozdrav!

Ja sam profesionalni haker koji ima pristup vašem operativnom sustavu.
Također imam puni pristup vašem računu.

Promatram te već nekoliko mjeseci.
Činjenica je da ste bili zaraženi zlonamjernim softverom putem web mjesta za odrasle koje ste posjetili.

Ako niste upoznati s tim, objasnit ću vam.
Trojanski virus pruža mi potpuni pristup i kontrolu nad vašim računalom ili bilo kojim drugim uređajem.
To znači da mogu vidjeti sve na vašem zaslonu, uključiti kameru i mikrofoni, ali vi ne znate za to.

Također imam pristup svim vašim kontaktima i svu vašu prepisku.

Zašto vaš antivirus nije otkrio zlonamjerni softver?
Odgovor: Moj zlonamjerni softver koristi upravljački program, ažuriram njegove potpise svaka 4 sata kako bi antivirus bio tih.

Napravio sam video koji prikazuje kako masturbirate u lijevoj polovini ekrana, a u desnoj polovici vidite video koji ste gledali.
Jednim klikom miša mogu poslati ovaj video na sve vaše e-poruke i kontakte na društvenim mrežama.
Jesam također mogu objaviti pristup svim vašim e-mail prepiskama i glasniciima koje koristite.

Ako to želite spriječiti, prenesite iznos od 950€ na moju bitcoin adresu (ako ne znate kako to učiniti, napišite Googleu: "Kupi bitcoin").

Moja bitcoin adresa (BTC novčanik) je: 1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd

Nakon primitka uplate, izbrisat ću videozapis i više me nikada nećete čuti.
Dajem vam 48 sati da platite.

Traducción:

"¡Saludo! Soy un hacker profesional que tiene acceso a su sistema operativo. También tengo acceso completo a su cuenta. Te he estado observando durante unos meses. El hecho es que ha sido infectado con malware a través de un sitio web para adultos que visitó. Si no lo conoces, te lo explico. Un virus troyano me da acceso y control completos sobre su computadora o cualquier otro dispositivo. Esto significa que pueden ver todo lo que hay en tu pantalla, encender la cámara y el micrófono, pero tú no lo sabes. También tengo acceso a todos sus contactos y a toda su correspondencia. ¿Por qué el antivirus no detectó el malware?

Respuesta: Mi malware usa un controlador, actualizo sus firmas cada 4 horas para mantener el antivirus en silencio. Hice un video que te muestra masturbándote en la mitad izquierda de la pantalla, y en la mitad derecha ves el video que viste. Con un solo clic del ratón, puedo enviar este video a todos sus correos electrónicos y contactos de redes sociales.

También puedo publicar el acceso a toda su correspondencia por correo electrónico y mensajeros que utiliza. Si quieres evitarlo, transfiere la cantidad de 950€ a mi dirección de bitcoin (si no sabes cómo hacerlo, escribe a Google: "Comprar bitcoin"). Mi dirección de bitcoin (billetera BTC) es:

1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd Después de recibir el pago, eliminaré el video y nunca más me volverás a escuchar. Te doy 48 horas para pagar. Tengo una notificación de lectura y el temporizador funcionará cuando vea esta carta. Presentar una queja en algún lugar no tiene sentido, porque este correo electrónico no se puede rastrear como mi dirección de bitcoin. No cometo ningún error. Si descubro que ha compartido este mensaje con otra persona, el video se distribuirá de inmediato. ¡Saludos!"

Este tipo de campaña de sextorsión suele estar relacionada con otros delitos como **fraude masivo (Email Spoofing & Phishing)**. También es típico el uso de **direcciones IP dinámicas**, uso de redes VPN o direcciones IP falsas para dificultar el rastreo. Clara **vinculación con el crimen organizado**. Estas campañas suelen ser operadas por grupos organizados en Europa del Este, Rusia o África.

3. Investigación en Fuentes Abiertas

Para profundizar en la procedencia de los datos encontrados, los pasos a seguir serían:

- **Análisis de foros de cibercrimen** en la deep web para encontrar posibles listados de la dirección de bitcoin.

Buscadores en la Dark Web:

- Usé Onion Search para buscar menciones de la dirección BTC.
- Introduje en la barra de búsqueda:

"1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd" site:.onion



Onion Search Engine

"No cookies, no javascript, no trace. We protect your privacy"

* Onion service: [Hidden 1](#), [Hidden 2](#)

El paso anterior me llevó a esta web:

<https://checkbitcoinaddress.com/bitcoin-abuse?address=1Fnjx9acfxzh9jaL21nsxbx2rrMHydtPLd>

Aquí hemos encontrado esto:

~RansomwareAbuser: Fraud mail "Hacked mail and webcam" Croatia, 2020-02-11 11:24:31



~RansomwareAbuser: ramsmrams@oriolbalaguer.com Got e-mail from this IP adress 114.29.236.151. Croatia, 2020-02-11 11:40:10



~SextortionAbuser: kzcgq@web-mail.com.ar Typical sextorsion Croatia, 2020-02-11 11:47:39



~Blackmail scamAbuser: jeanette@nextel.com.ar Blackmailing into sending 950eu otherwise, the hacker will send your masturbation video to all your contacts. Croatia, 2020-02-11 11:52:15



~RansomwareAbuser: melchiori@munchis.com.ar Got a e-mail from this IP [212.156.246.74. static.turktelekom.com.tr](http://212.156.246.74.static.turktelekom.com.tr) Croatia, 2020-02-11 11:54:15



~SextortionAbuser: voice7@a-b-c-plus.com Classic sextortion Croatia, 2020-02-11 12:17:09



~SextortionAbuser: piperoni njuškalo sextortion Croatia, 2020-02-11 12:19:33



~SextortionAbuser: Received: from [113.162.65.19] in croatian language Croatia, 2020-02-11 12:24:20



~SextortionAbuser: ctdonate@iserve.net.mx scam sextortion Croatia, 2020-02-11 12:54:39



~RansomwareAbuser: Ransomware Provjerite integritet svojih podataka (prema našoj sigurnosnoj službi vaš je račun hakiran Croatia, 2020-02-11 13:37:19



~SextortionAbuser: Not known Variation of already seen sextortion mail Croatia, 2020-02-11 14:55:25



~SextortionAbuser: red@tokenads.com Masturbation video Croatia, 2020-02-11 14:57:42 Blackmail scamAbuser: cbermudez@iqaccess.com.mx



~SextortionAbuser: dmunbomb@scarlos.com.ar in croatian language Croatia, 2020-02-11 15:24:29



~SextortionAbuser: ventasangelopolis@harmonymexico.com.mx Received email claiming to have access to my PC and asking for 950€ otherwise he will publish video. Croatia, 2020-02-11 16:48:47



~SextortionAbuser: kubo1967@cavelpropiedades.cl Sextortion mail Croatia, 2020-02-12 09:02:51



~SextortionAbuser: eledesma@ceajalisco.gob.mx Sent on Croatian language. Wants money to not publish a sex video. Croatia, 2020-02-12 12:07:28



En este punto la investigación se retroalimenta a sí misma, de modo que toda la información que hemos encontrado nueva la vamos sometiendo nuevamente a las herramientas usadas hasta ahora. Si hay suerte, la cantidad de información que se va revelando acabará siendo exponencial a medida que avanza la investigación. De modo que habrá que ser ordenado y cauteloso a la hora de gestionarla. Este es un hábito que suele infravalorarse con facilidad.

He verificado los registros de IPs y dominios asociados a los correos electrónicos encontrados a través de la plataforma whois.com

<https://www.whois.com/>

He averiguado lo siguiente:

Con respecto a este dominio “ramsmrams@oriolbalaguer.com” tenemos esta información:

| | |
|----------------|--|
| Domain: | oriolbalaguer.com |
| Registered On: | 2001-06-18 |
| Expires On: | 2025-06-18 |
| Updated On: | 2024-06-11 |
| Status: | client delete prohibited client transfer prohibited |
| Name Servers: | ns.dinahosting.com ns6.hospedajewindows.com |

Registrar Information

| | |
|--------------|-------------------------------|
| Registrar: | Dinahosting s.l. |
| IANA ID: | 1262 |
| Abuse Email: | abuse-domains@dinahosting.com |
| Abuse Phone: | +34.981040200 |



Registrant Contact

| | |
|---------------|---------------------|
| Organization: | PastisProjects S.L. |
| City: | BARCELONA |
| Postal Code: | ES |

related domain names

[verisign.com](https://www.verisign.com) [dinahosting.com](https://www.dinahosting.com) [hospedajewindows.com](https://www.hospedajewindows.com) [icann.org](https://www.icann.org)

Con respecto a esta IP "212.156.246.74" tenemos esta información:

% Abuse contact for '212.156.246.0 - 212.156.246.255' is 'abuse@turktelekom.com.tr'

```
inetnum:      212.156.246.0 - 212.156.246.255
netname:      TurkTelekom
descr:        ADSL-ALC-Dynamic Pool
country:      tr
admin-c:      TTBA1-RIPE
tech-c:       TTBA1-RIPE
status:       ASSIGNED PA
mnt-by:       as9121-mnt
created:      2005-04-20T13:37:42Z
last-modified: 2005-04-20T13:37:42Z
source:       RIPE # Filtered

role:         TT Administrative Contact Role
address:      Turk Telekomunikasyon A.S Turgut Ozal Blv. Aydinlikevler
address:      06103 ANKARA TURKEY
phone:        +90 312 555 0000
fax-no:       +90 312 313 1924
admin-c:      BADB3-RIPE
abuse-mailbox: abuse@turktelekom.com.tr
tech-c:       BADB3-RIPE
tech-c:       BADB3-RIPE
tech-c:       BADB3-RIPE
nic-hdl:      TTBA1-RIPE
mnt-by:       AS9121-MNT
created:      2002-02-28T12:22:28Z
last-modified: 2022-01-28T07:15:56Z
source:       RIPE # Filtered
```

% Information related to '212.156.240.0/21AS9121'

```
route:        212.156.240.0/21
descr:        TurkTelekom
origin:       AS9121
mnt-by:       AS9121-MNT
created:      2011-05-25T14:06:17Z
```

Con respecto a esta IP "113.162.65.19" tenemos esta información:


```
% Abuse contact for '113.160.0.0 - 113.191.255.255' is 'hn-changed@vnnic.vn'

inetnum:      113.160.0.0 - 113.191.255.255
netname:      VNPT-VN
descr:        Vietnam Posts and Telecommunications Group
descr:        No 57, Huynh Thuc Khang Street, Lang Ha ward, Dong Da district, Ha Noi Ci
country:      VN
admin-c:      PTH13-AP
tech-c:       PTH13-AP
remarks:      for admin contact mail to Nguyen Xuan Cuong NXC1-AP
remarks:      for Tech contact mail to Nguyen Hien Khanh KNH1-AP
status:       ALLOCATED PORTABLE
mnt-by:       MAINT-VN-VNNIC
mnt-lower:    MAINT-VN-VNPT
mnt-routes:   MAINT-VN-VNPT
last-modified: 2018-01-25T03:55:17Z
mnt-irt:      IRT-VNNIC-AP
source:       APNIC

irt:          IRT-VNNIC-AP
address:      Ha Noi, VietNam
phone:        +84-24-35564944
fax-no:       +84-24-37821462
e-mail:       hn-changed@vnnic.vn
abuse-mailbox: hn-changed@vnnic.vn
admin-c:      NTTTT1-AP
tech-c:       NTTTT1-AP
auth:         # Filtered
mnt-by:       MAINT-VN-VNNIC
last-modified: 2017-11-08T09:40:06Z
source:       APNIC

person:       Pham Tien Huy
address:      VNPT-VN
country:      VN
phone:        +84-24-37741604
```

Con respecto a este dominio tdonate@iserve.net.mx hemos encontrado esto:

Raw Whois Data

```
Domain Name:      iserve.net.mx

Created On:       1995-11-29
Expiration Date:  2025-11-28
Last Updated On:  2024-11-06
Registrar:       AKKY ONLINE SOLUTIONS, S.A. DE C.V.
URL:             http://www.akky.mx
Whois TCP URI:    whois.akky.mx
Whois Web URL:    http://www.akky.mx/herramientas/whois.jsf

Registrant:
  Name:          Servicios Administrados Mexis S.A. de C.V.
  City:          Mexico
  State:         Distrito Federal
  Country:       Mexico

Administrative Contact:
  Name:          Contacto Administrativo Mexis
  City:          Mexico
  State:         Distrito Federal
  Country:       Mexico

Technical Contact:
  Name:          Contacto Tecnico Mexis
  City:          Mexico
  State:         Distrito Federal
  Country:       Mexico

Billing Contact:
  Name:          Contacto Pagos Mexis
  City:          Mexico
  State:         Distrito Federal
  Country:       Mexico
```

Parece que no hay mucha información relevante en lo anterior. Los atacantes posiblemente usaran VPN y obfuscaran bien sus huellas.

Para seguir pasé además cada IP y correos mencionados hasta ahora los filtré por aplicaciones web como www.dehashed.com o <https://haveibeenpwned.com/> para buscar información extra, sin resultado interesante.

Otro apunte es que explorar las direcciones IPs a través de otras herramientas como Shodan no es nada resultante en mi caso, ya que Shodan no guarda historial de las actividades de direcciones IP tan antiguas en su versión gratuita, quizás si en la versión premium.

También descubrí que la dirección bitcoin "1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd" estaba relacionada con un troyano. La información la encontré en:

<https://feedreader.com/observe/deletetrojaninfection.com/tips-for-removing-1fnjx9acfxzh9jaL21nsxbx2rrmhydtpLd-from-windows-7%3F+itemId=8606253770>

¿Por qué se relaciona con un troyano y cómo se comporta este en nuestro caso?

Muchas veces, direcciones de Bitcoin aparecen vinculadas a malware o troyanos porque los ciberdelincuentes las usan para recibir pagos de sus víctimas. Esto ocurre en varios tipos de ataques, por ejemplo **Ransomware, Crypto-minería, phishing, troyanos bancarios, etc.**














El artículo de [Deletetrojaninfection.com](https://deletetrojaninfection.com) nos informa sobre cómo funciona el malware relacionado a esta dirección bitcoin con la que estamos trabajando. Este malware se infiltra sin el conocimiento del usuario, se replica a sí mismo y se inserta en otros programas o archivos, alterando la configuración del navegador y encriptando archivos esenciales, lo que los vuelve inaccesibles. Además, recopila información personal y la transmite a ciberdelincuentes, desactiva las herramientas de seguridad del sistema y degrada el rendimiento general del PC. El malware se propaga a través de métodos como la transferencia de archivos infectados, descargas de software pirata, visitas a sitios web para adultos y clics en enlaces sospechosos.

En un escenario profesional estudiaría el comportamiento y los metadatos de este troyano en cuestión en un entorno seguro mediante análisis estático y dinámico.

4. Posibilidad de Rastrear a los Autores

El rastreo de una billetera de bitcoin puede ser complicado debido a la naturaleza seudónima de la blockchain. Sin embargo, vamos a intentarlo:


Empezemos estudiando el historial de transacciones:

| date | | received/sent | balance | transaction |
|--|--|--|------------|-----------------------|
| 2020-06-21 18:26:06 | | -0.05239422  [e2c199afa9] (-0.00014534) fee | 0. | d77cfec43569395acdfa_ |
| 2020-06-16 06:44:52 |  [001e29be74] | +0.05003956 | 0.05253956 | 3c08abe474da3a313d9c_ |
| 2020-06-11 05:12:54 |  [9c20994bd9] | +0.0025 | 0.0025 | 9ff3e5eef3f8b5c933af_ |
| 2020-05-19 10:21:11 | | -0.53673597  [c594e57c1d] (-0.0028223) fee | 0. | 22a501381bf5fc76f663_ |
| 2020-05-17 02:52:47 |  [730ad2f29e] | +0.10378055 | 0.53955827 | 6ee2641c7ce22b5b3cff_ |
| 2020-05-14 15:51:31 |  [6c4f2a5003] | +0.00213614 | 0.43577772 | a2b8ccc991493f1f54b7_ |
| 2020-05-14 10:08:17 |  [d32e0242a0] | +0.09956087 | 0.43364158 | c3eccc74734ccfb60ad6_ |
| 2020-05-13 13:32:18 |  [0000a6978d] | +0.054837 | 0.33408071 | d22f1e37f7528fad11fd_ |
| 2020-05-13 06:51:14 |  [001e29be74] | +0.05432325 | 0.27924371 | 8deca65db5d5938b8502_ |
| 2020-05-12 08:39:53 |  [7a2cb2429b] | +0.058 | 0.22492046 | d52a1b967cf200bd2ed9_ |
| 2020-05-12 07:34:28 |  [006422e0b8] | +0.01237 | 0.16692046 | 2b41f5edbed3cfa8deaf_ |
| 2020-05-12 01:44:01 |  [d0e6df820f] | +0.03120057 | 0.15455046 | be212fab45da6c230ee7_ |
| 2020-05-12 00:57:43 |  [3ed4587186] | +0.01565719 | 0.12334989 | 1370f680993f084ff630_ |
| 2020-05-11 18:16:54 |  Binance.com | +0.05607488 | 0.1076927 | c5346855434dcf7940fb_ |
| 2020-05-11 09:01:22 |  [0000789bb9] | +0.05161782 | 0.05161782 | c5977789b135cfbcf6a0_ |
| 2020-05-05 21:58:46 | | -0.26314497  [00b0d01f04] (-0.00063342) fee | 0. | 71b4b1ccb0a36d53dd96_ |
| 2020-04-27 11:26:17 |  [7ccb515ca2] | +0.01493883 | 0.26377839 | 28ceeaba9786e793f745_ |
| 2020-04-24 03:11:32 |  [000203ba6e] | +0.13400984 | 0.24883956 | 5f8e423163d844da82cf_ |
| w.wallexplorer.com/wallet/e2c199afa9d5cba4 | | +0.09222972 | 0.11482972 | 5c6e4850ec7cdf68f1e5_ |




A continuación vamos a intentar identificar si los fondos se transfieren a un exchange que requiera verificación KYC, o pasa por mixers.

Con [Wallexplorer.com](https://www.wallexplorer.com) hemos encontrado algunos exchangers:

Wallexplorer.com: smart Bitcoin block explorer

Wallet  [3e970ff2ac] [\(show wallet addresses\)](#)

Page 1 / 1 (total transactions: 3) [Download as CSV](#)

| date | | received/sent | balance | transaction |
|---------------------|--|---------------|------------|-----------------------|
| 2025-02-03 11:14:12 |  BitZlato.com | +1.79805866 | 3.64494458 | d4e045a523b6f69617f1_ |
| 2024-08-27 07:54:35 |  BitZlato.com | +1.5 | 1.84688592 | b742233fda9a8964e1d1_ |
| 2024-08-27 07:54:35 |  BitZlato.com | +0.34688592 | 0.34688592 | 198929d915a0fd98a9a4_ |

Page 1 / 1 (total transactions: 3) [Download as CSV](#)

Además encontramos la siguiente información valiosa con respecto al exchanger BitZlato.com



La noticia dice “El 18 de enero de 2023, la Red de Ejecución de Delitos Financieros (FinCEN) del Departamento del Tesoro de EE. UU. designó al intercambio de criptomonedas **Bitzlato** Limited como una "preocupación principal de lavado de dinero" debido a su conexión con finanzas ilícitas rusas.

FinCEN determinó que Bitzlato desempeña un papel crítico en el lavado de criptomonedas al facilitar transacciones ilícitas para actores de ransomware operativos en Rusia, incluyendo al grupo Conti, vinculado al gobierno ruso. Además, Bitzlato ha facilitado transacciones para mercados darknet conectados a Rusia, como Hydra, BlackSprut, OMG!OMG! y Mega."

De modo que, a la pregunta de si existen posibilidades reales de rastreo, diríamos que si los fondos fueran movidos a un exchange regulado, no siendo este el caso, sí sería posible solicitar información legalmente.

Hemos encontrado además en varias transacciones esta información relacionada con Coinjoin:

| | | | | |
|---------------------|----------------|---------------|----------------|-----------------------|
| 2025-02-05 02:03:15 | ■ [0d942fd9b2] | +0.00489231 | 12970.96118676 | 571de69534385d0bcb85_ |
| 2025-02-05 02:03:15 | | -0.30103 | | |
| | | -0.0051074 | | |
| | | -0.00335178 | | |
| | | -0.00054 | | |
| | | (-0.0001) fee | 12970.95629445 | ad3eee538d4020921dfd_ |

CoinJoin es una estrategia de anonimato que oscurece direcciones y cantidades de transacciones. Utiliza contratos inteligentes entre varias partes para mezclar sus monedas en varias transacciones diferentes. Es por tanto un método de mezcla (*mixing*) de transacciones de Bitcoin diseñado para mejorar la privacidad.

<https://www.investopedia.com/terms/c/coinjoin.asp>

| date | received/sent | balance | transaction |
|---------------------|---|------------|---|
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00001652 | cadc208e14262320b02c... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00002478 | 013eb62d78d369192fa1... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00003304 | 8455a4c331b8a8265e81... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.0000413 | 3759ba3598bff2725e3d... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00004956 | 3534e1a48f5a083aa275... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00005782 | 530064981fde99a62119... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00006608 | 39fed17c9edf13a160f5... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00007434 | 1776693c33e7d6c470be... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.0000826 | 409ac7ce50ea529ec369... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00009086 | aa8e0d0aa716130f8b9a... |
| 2025-02-05 02:03:15 | -0.00000546  CoinJoinMess (-0.0000028) fee | 0.00009912 | fb1685bb847f35e4c72f... |

En el siguiente paso intentando rastrear a los criminales, hemos guardado la info como CSV para visualizar mejor los datos. De modo que al abrir el documento CSV, y con "Ctrl + F" buscamos por palabras claves. Así hemos encontrado más información de exchangers:

| | | |
|---------------------|--|------------|
| 2020-03-20 21:47:39 | Binance.com (00000b55c1bcbc1f) | 0.1223 |
| 2020-03-20 16:02:13 | fb5bef0b2dcf0952 | 0.22300659 |
| 2020-03-20 15:54:03 | 411fa4d830e49fdc | 0.04417 |
| 2020-03-20 09:58:36 | 8c8dcac007495204 | 0.5509345 |
| 2020-03-20 01:08:32 | fb5bef0b2dcf0952 | 0.00804553 |
| 2020-03-19 22:44:09 | b250bb41b22d0ce6 | 0.24443822 |
| 2020-03-19 19:05:17 | 00080077b89ef565 | 0.02326912 |
| 2020-03-19 15:51:24 | 6be860b4e80e038f | 0.05057751 |
| 2020-03-19 14:41:46 | 9dbc2c6596c5338b | 0.256585 |
| 2020-03-19 14:16:07 | Kraken.com (00001012b1848923) | 0.1726 |
| 2020-03-19 14:16:07 | b4563323e77da61b | 0.07755894 |
| 2020-03-19 12:35:05 | 0009e0caa9054c28 | 0.16951811 |
| 2020-03-19 10:27:11 | Kraken.com (00001012b1848923) | 0.1851 |
| 2020-03-19 07:59:20 | 900ef50e27cf6203 | 0.27538 |
| 2020-03-19 07:03:30 | c194105ec7318e19 | 0.00001001 |
| 2020-03-18 17:31:02 | Binance.com (00000b55c1bcbc1f) | 0.2906 |

Además chat GPT nos ayudó bastante en partes de la tarea como esta:

que más palabras claves puedo buscar en un documento CVS para encontrar exchangers o mixers

Si tienes un documento **CSV** con transacciones de Bitcoin y quieres identificar **exchanges** o **mixers**, puedes buscar las siguientes **palabras clave** en las direcciones o etiquetas asociadas:

Palabras clave para identificar exchanges

Busca nombres de exchanges conocidos, ya que muchos marcan sus direcciones en exploradores de blockchain:

- **Exchange generales:**

- `binance`
- `kraken`
- `coinbase`
- `bitstamp`
- `kucoin`



Palabras clave para identificar *mixers*

Los mezcladores de Bitcoin pueden ocultar transacciones. Busca estas palabras:

- `coinjoin` (relacionado con Wasabi Wallet y JoinMarket)
- `mixer`
- `tumbler`
- `whirlpool` (usado por Samurai Wallet)
- `blender` (mezclador sancionado por EE.UU.)
- `helix`
- `chipmixer`
- `wasabi`
- `samurai`
- `anon`
- `privacy`



Habiendo encontrado estos últimos datos, y retomando la pregunta 4 con el enunciado "¿existen posibilidades reales de rastrear el monedero de bitcoin o de saber quiénes son los autores? " diría que las probabilidades están en 50-50% . ¿Por qué? porque hemos encontrado información que señala que al haberse encontrado mixers y exchangers como Blitzlato, ello apunta a la imposibilidad de rastreo debido a su naturaleza delictiva.

Por otro lado sí hay probabilidad de encontrar información valiosa, ya que hemos visto que se han usado exchangers como binance.com, kraken.com. Tanto **Binance** como **Kraken** implican intercambios centralizados, lo que significa que operan bajo un sistema que controla las transacciones y mantiene registros.

Como los intercambios como Binance y Kraken cooperan con investigaciones legales, en un contexto legal adecuado podrían ser obligados a entregar la información de los usuarios.

5. Herramientas para el Análisis de Criptomonedas

Herramienta 1: Chainalysis

- **URL:** <https://www.chainalysis.com>
- **Finalidad:** Análisis y seguimiento de transacciones en blockchain.
- **Criptomonedas soportadas:** Bitcoin, Ethereum, Litecoin y otras.
- **Modelo de uso:** Privativo.
- **Datos obtenibles:** Direcciones vinculadas, patrones de lavado de dinero, conexiones con exchanges.

Herramienta 2: Graphsense

- **URL:** <https://graphsense.org/>
- **Finalidad:** Plataforma de análisis de cryptoactivos que enfatiza la soberanía total de los datos, la transparencia algorítmica y la escalabilidad.
- **Criptomonedas soportadas:** Bitcoin, Bitcoin Cash, Litecoin, Zcash, Ethereum y Tron.
- **Modelo de uso:** Código abierto y gratuito.

- **Datos obtenibles:** Búsqueda cruzada por dirección, etiqueta, transacción o bloque en varias cadenas de bloques; navegación en abstracciones de redes de transacciones; inspección de metadatos; búsqueda automática de rutas de transacción entre dos nodos; soporte para análisis basados en datos a través de la API REST; organización de etiquetas de atribución en TagPacks públicos o privados.

<https://www.iknaio.com/book-demo>

Herramienta 3: Elliptic

- **URL:** <https://www.chainalysis.com/>
- **Finalidad:** Proporcionar soluciones de análisis de blockchain para ayudar a agencias gubernamentales, empresas de criptomonedas e instituciones financieras a interactuar con confianza con las criptomonedas.
chainalysis.com
- **Criptomonedas soportadas:** Bitcoin, Ethereum y otras criptomonedas principales.
chainalysis.com
- **Modelo de uso:** Servicios comerciales con opciones de prueba gratuita y demostraciones disponibles.
- **Datos obtenibles:** Análisis de transacciones en blockchain, monitoreo de actividades ilícitas, cumplimiento normativo, inteligencia de mercado y generación de informes detallados sobre el uso de criptomonedas.

ANEXO:

1. Como apunte sería interesante en una investigación de criptomonedas crear alertas en aplicaciones como whale alert: <https://whale-alert.io/>

Whale Alert es una plataforma que monitorea en tiempo real las tendencias del mercado de criptomonedas y las transacciones de gran volumen. Ofrece a los usuarios la posibilidad de establecer alertas personalizadas, ver actualizaciones de precios en vivo y analizar datos de criptomonedas a través de visualizaciones avanzadas.

Además, Whale Alert proporciona una API que permite a los desarrolladores integrar alertas en tiempo real y datos agregados avanzados en sus aplicaciones. Esta API ofrece notificaciones personalizadas basadas en el valor de la transacción, el símbolo de la criptomoneda, el tipo de transacción y la blockchain específica.

2. Segundo apunte: para **monitorear una IP a lo largo de cierto tiempo**, puedes configurar alertas en Shodan para que te notifiquen si se detecta esa IP en futuras exploraciones y filtrar por regiones geográficas, etc. Esto te puede ayudar a hacer un seguimiento continuo de esa IP en lugar de buscar fechas pasadas.
3. Les he escrito un correo a GraphSense pidiendo acceso a su demo. En caso positivo lo incorporaré a esta investigación.

UNIR, Dragos Cornel  Recibidos x

Karl Zettl <notifications@iknaio.odoo.com>
para mí ▾

14:23 (hace 11 minutos) ☆ 😊 ↩ ⋮

Dear Dragos,

thank you for the request, we'll prepare the account and send you the login details. But may I ask you before for your profession and company profile so that we can support you in the best way?

thank you
Karl

--

Karl Zettl

dragoshu junior

para Dragos ▾

14:35 (hace 0 minutos) ☆ 😊 ↩ ⋮

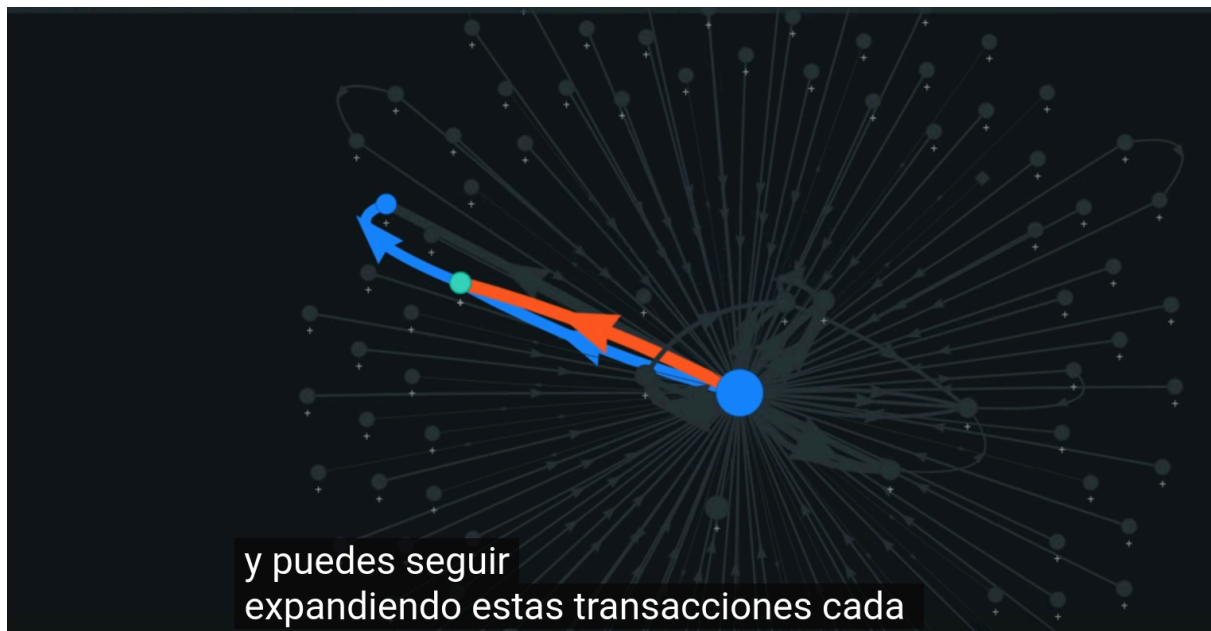
Thank you for answering me so soon. I am a student in the master's degree in Private Detective and Cyber Investigation at the UNIR university, Spain. I would like to test your application and include it in my final paper. The main use would be tracking down a bitcoin wallet (1Fnjx9acfxzh9jaL21nsxbx2rrMHdtpLd) , extract as much information as possible, and explore the GUI of the app.

I've heard very well about yours and wanted to try it.

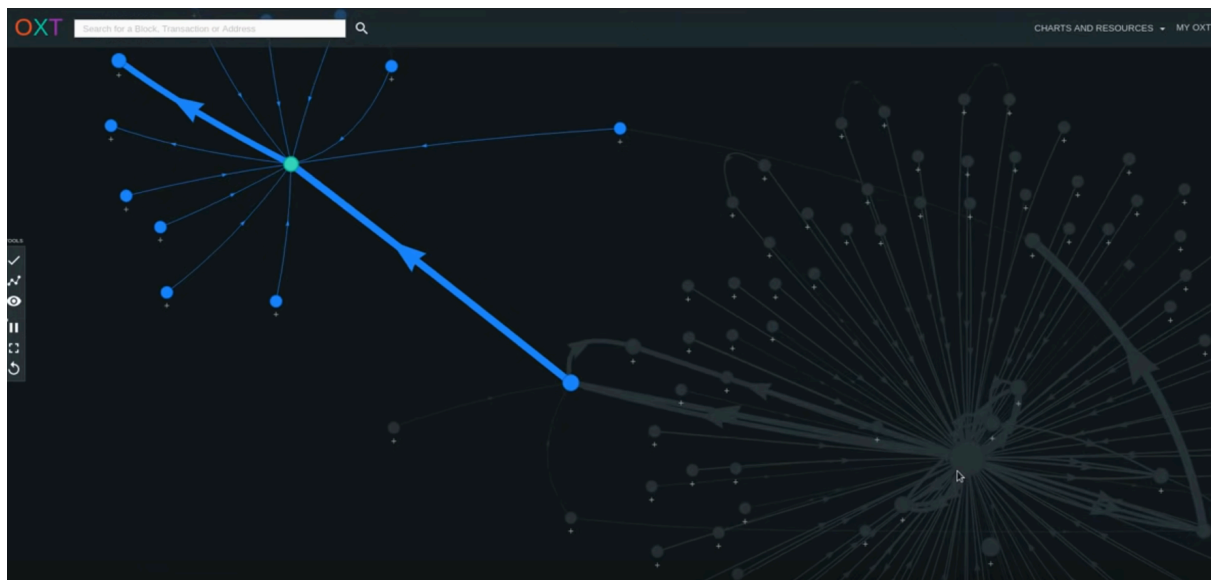
I attach my LinkedIn for more information. www.linkedin.com/in/dragos-cia5

Thank you very much in advance!

4. Esta es la app OXT haciendo un seguimiento de otra actividad delictiva. Me ha interesado este apunte por la segunda diapositiva de abajo:



Esta segunda y tercera imagen reflejan un comportamiento gráfico típico de estos delitos. Ese alejarse bruscamente del centro y luego expandirse, refleja una alta posibilidad de que se estén haciendo transacciones a un mixer. Se roba, se aleja, y se divide en varias transacciones pequeñas para mixear rapido y que le pierdan el rastro.



Me ha parecido muy interesante la observación gráfica de patrones de comportamiento en este tipo de delitos.