Chainalysis

T E & I
telecom|energia|infotec

Policia Nacional de Colombia – ESU Medellin

Enero 2026

Pedro E. Mejia Ochoa

Mapa vial para la adopción efectiva de herramientas Chainalysis

T E & I
telecom|energia|infotec

Data	Apoyo a la Investigación (Servicios Profesionales)	Capacitación y Educación	Criterios de gestión del éxito
Generación de Pistas, Análisis de Amenazas	Multiplicador de fuerza, técnicas avanzadas e investigación y mejores prácticas	Fundamental para garantizar una adopción y una aplicación exitosas	Mirando más allá de las métricas de uso cuantitativas al valor real entregado (Pistas encontradas, casos cerrados, procesamientos y activos incautados)

Estrategia basada en datos

Soporte de investigación

Disponible globalmente - No repudiado - Datos enriquecidos

T E & I
telecom|energia|infotec

Nuestra cobertura

19.000+ Entidades del mundo real que operan en la Blockchain identificadas

13+ Millones de direcciones BTC con observaciones IP

Millones y millones de direcciones de billetera cripto atribuidas a entidades del mundo real

Regulado

- Exchange
- Billetera Alojada
- Servicios Mercantiles
- Minereía
- Mining Pool
- Otro
- ATM - Cajero Automatico
- Desconocida
- Contracto de Prestamo
- Contrato de intercambio descentralizado
- Smart Contract
- Smart Contract de Token

Amenazas

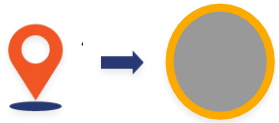
- Actor de amenazas
- Organización de actores ilícitos
- Tienda de fraudes
- Jurisdicción de alto riesgo
- Intercambio de alto riesgo
- P2P Exchange
- Abuso infantil
- Darknet Market
- Ransomware
- Financiamiento terrorista
- Estafa
- Fondos robados
- Juego - Casino
- Mixing
- Sanciones
- Infraestructura como un servicio

0day	ASEAN Market
AlphaBay Market	Apollon Market
Babylon Market	Bankomat.cc
BitBazaar	Black Bank Market
Brave Bunny Market	Brian Dumps
Cloud9 Market	Cocaine Market
DeDope Market	Docstagram Shop
East India Company Market	Ecards
Evolution Market	Exploit.in
French Connection Market	FuLLzShOp
Gvoice store	Hansa Market
Infinity	Isellz.cc
Korovka forum	LuxSocks.ru
Midland City Market	MyFakeID.biz
Olympus Market	Omerta Forum
Point Market (former Tochka)	Rescator.at
Sheep Marketplace	Silk Road 2 Market
To You Team Market	Topcc
UnderMarket	Unicc
Vendetta.cc	Wall Street Market
Yellow Brick Market	cvv.me

Proprietary and Confidential

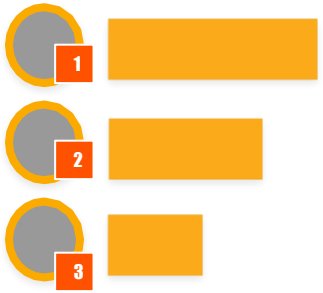
Genere pistas a partir de millones de direcciones IP

Ejemplo: agencias de LE/Intel/equipo de investigación cibernética que buscan identificar direcciones IP que podrían estar involucradas en actividades ilícitas, dentro de un conjunto de datos de millones de direcciones IP

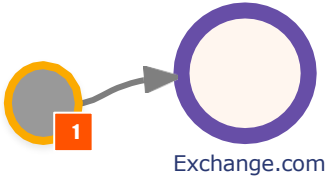


Busque IP e identifique los clústeres asociados dentro de los datos de Chainalysis

Obtenga más IP de los clústeres identificados y amplíe el conjunto de IP



Priorizar clústeres en función del volumen y la exposición a entidades ilícitas



Identifique intercambios conformes dentro de las contrapartes o inicie una investigación

Descubrimiento de IP: enfoque basado en la investigación

MONERO

En colaboración con USG, los pagos directos a la billetera de proveedor/administrador de DNM (Mercado de la web oscura) revelan un descubrimiento de IP que conduce tanto a la ubicación del servidor de DNM como al posible sospechoso.

IP del centro de datos del servidor DNM

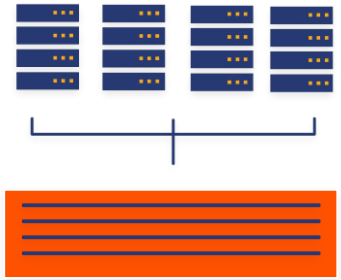
31.13.xxx.xxx

IP móvil de Monero Wallet

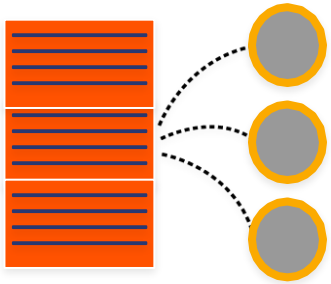
181.140.xxx.xxx

Genere nuevas pistas potenciales a través de direcciones/hash txn

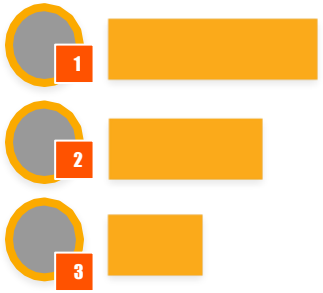
Ejemplo: priorizar los datos incautados de un mercado de darknet (o un dispositivo)



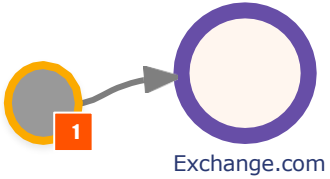
Obtenga todas las entradas/salidas y las cantidades para todos los hash txn en el servidor del mercado darknet



Clasifique todas las transacciones entrantes/salientes por tamaño para identificar proveedores/administradores



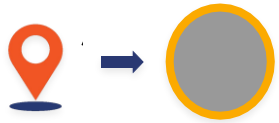
Priorizar entradas/salidas en función del volumen y la exposición a entidades ilícitas



Identifique los intercambios compatibles dentro de las contrapartes para los grupos de clasificación superior

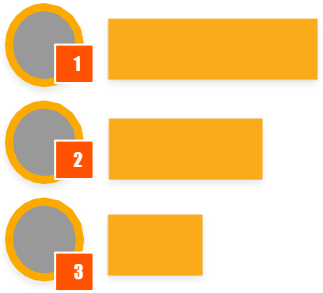
Genere pistas a partir de millones de direcciones IP

Ejemplo: agencias de LE/Intel/equipo de investigación cibernética que buscan identificar direcciones IP que podrían estar involucradas en actividades ilícitas, dentro de un conjunto de datos de millones de direcciones IP

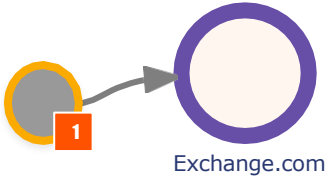


Busque IP e identifique los clústeres asociados dentro de los datos de Chainalysis

Obtenga más IP de los clústeres identificados y amplíe el conjunto de IP



Priorizar clústeres en función del volumen y la exposición a entidades ilícitas



Identifique intercambios conformes dentro de las contrapartes o inicie una investigación

Inteligencia de Criptomonedas para los Cuerpos Policiales

T E & I
telecom|energia|infotec

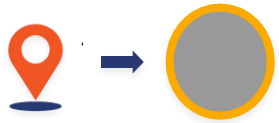
Siga el dinero para exponer a las entidades del mundo real

Los delincuentes a menudo eligen criptomonedas para realizar fraudes, lavado de dinero y otras actividades ilícitas, a fin de evadir la detección por parte de las fuerzas del orden. Sin las herramientas adecuadas, es difícil para los investigadores identificar y detener esta actividad criminal.

Chainalysis Reactor impulsa las investigaciones con inteligencia de criptomonedas en tiempo real, rastreando transacciones a servicios nombrados y detectando actividades ilícitas a medida que suceden. Con la confianza de las agencias de cuerpos policiales público a nivel mundial, Reactor se utiliza todos los días para vincular entidades del mundo real a sus contrapartes digitales y combatir los delitos en todas las misiones.

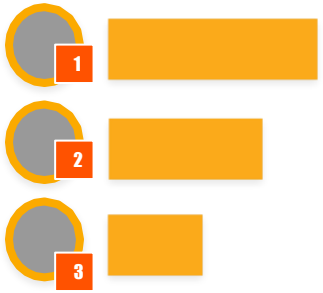
Genere pistas a partir de millones de direcciones IP

Ejemplo: agencias de LE/Intel/equipo de investigación cibernética que buscan identificar direcciones IP que podrían estar involucradas en actividades ilícitas, dentro de un conjunto de datos de millones de direcciones IP

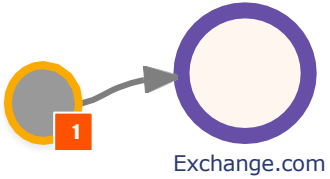


Busque IP e identifique los clústeres asociados dentro de los datos de Chainalysis

Obtenga más IP de los clústeres identificados y amplíe el conjunto de IP



Priorizar clústeres en función del volumen y la exposición a entidades ilícitas



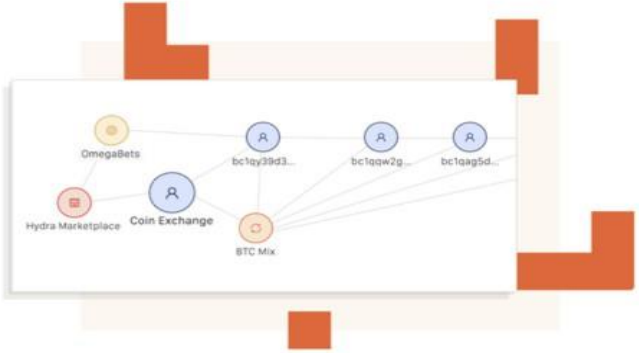
Identifique intercambios conformes dentro de las contrapartes o inicie una investigación

Datos que son válidos en los tribunales

A diferencia de las herramientas manuales con altas tasas de falsos positivos, Chainalysis le ofrece el conjunto de datos más confiable, enriquecido con conocimientos basados en nuestra metodología patentada. La datos ofrecida por Chainalysis es totalmente auditable, basándose en pruebas fundamentadas que conservan su validez ante los tribunales.

Desanonimizar los servicios Blockchain

Chainalysis proporciona atribución automática en servicios conocidos, como las casas de cambio, para revelar las principales contrapartes y la exposición al riesgo asociada con cada transacción.



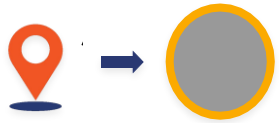
Seguimiento claro de la actividad ilícita

Rastree el flujo de criptomonedas para identificar la fuente o el destino de los fondos. Cree un registro claro de sus hallazgos con herramientas de visualización flexibles y búsqueda automatizada de rutas.

> *“ La cooperación funcional entre las fuerzas del orden y la industria es la única manera de hacer frente con éxito a la amenaza significativa de la ciberdelincuencia. Chainalysis aporta un nivel de experiencia que será de gran beneficio para nuestras investigaciones en toda Europa.”*

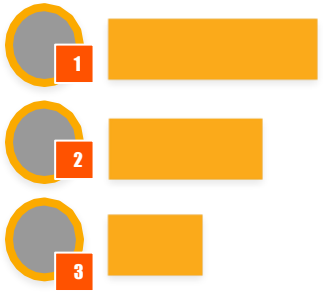
Genere pistas a partir de millones de direcciones IP

Ejemplo: agencias de LE/Intel/equipo de investigación cibernética que buscan identificar direcciones IP que podrían estar involucradas en actividades ilícitas, dentro de un conjunto de datos de millones de direcciones IP

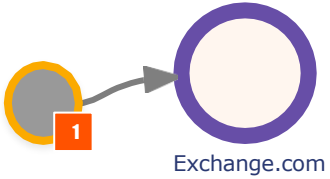


Busque IP e identifique los clústeres asociados dentro de los datos de Chainalysis

Obtenga más IP de los clústeres identificados y amplíe el conjunto de IP



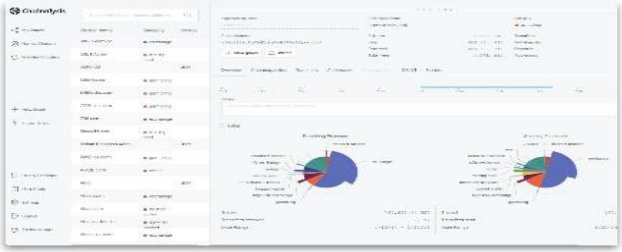
Priorizar clústeres en función del volumen y la exposición a entidades ilícitas



Identifique intercambios conformes dentro de las contrapartes o inicie una investigación

Identificar sospechosos y malos actores que usan criptomonedas

Identifique sospechosos y demuestre cómo se benefician de la actividad ilícita a través de las criptomonedas.



Software de investigación integral en el que confía la seguridad nacional global

Como el software más confiable, Chainalysis es utilizado todos los días por analistas de todo el mundo para extraer inteligencia financiera relacionada con las transacciones de criptomonedas en programas de interés como:

- **Sanciones**
- **Anti lavado de dinero**
- **Antinarcóticos**
- **Contraterrorismo**
- **Contraespionaje**
- **La seguridad cibernética**
- **Contraproliferación**
- **Crimen organizado transnacional**
- **Explotación infantil**
- **Trata de personas**

Professional Services

Soporte de casos de investigación

Professional Services

Enfoque multiple para el analisis de tendencias

El mejor patrón y monitoreo de actividades ilícitas de su clase

desmezclar, Monero, & Análisis de red

Expertos en la materia, desarrollo de casos y apoyo a la investigación

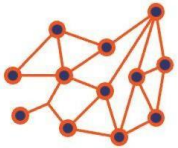
Asistencia a los fiscales y preparación para juicio / audiencia

Servicios profesionales - Soporte de casos

Expertos en la materia

Construcción de conocimiento

Juicio/Audiencia Testimonio de Testigo



Trazado y Reconstrucción Paralela

Explotación de datos

Investigación y monitoreo de Deep/Dark Web

Educación y Capacitación

Cursos de Certificación

Educación y Capacitación: estrategia empresarial

Capacitación integrada de especialistas en todas las áreas de la misión

Chainalysis Reactor Certification (CRC)

Educación de Conciencia Amplia

Chainalysis Cryptocurrency Fundamentals Certification (CCFC)

Paquete de Software y Servicios diseñados para La Policia Nacional de Colombia – Medellin – ESU.

Resumen de inversión – Licenciamiento a 12 meses

Línea de productos/servicios	Oferta de productos/servicios	Inversión total
Servicios profesionales	*Un investigador dedicado por 125* ***horas*** *durante el primer año de nuestro compromiso* Acceso directo a expertos en la materia de Chainalysis para obtener ayuda en el análisis de datos – Incluido.	**Incluido**
Educación y Capacitación	Incluye 10 sillas en sitio CCFC (Fundamentales) Incluye 10 sillas en sitio de CRC (Reactor)	**Incluido**
Atención al cliente	Acceso directo a soporte al cliente 24/7 Gerente de Éxito del Cliente Dedicado. 12 meses.	**Incluído**
Chainalysis Reactor Platinum, IP Observations, Reactor Demixing, búsqueda avanzada.	1 licencia con capacidades avanzadas de observación de IP. Licencia de la nube. Servicio Platinum, Demixing, API. 12 meses.	**Incluido**
		COP$880,000,000.00

Exención de IVA; El ESTATUTO TRIBUTARIO, en su artículo 476, exeptua de la obligación del pago de IVA en su numeral 21 el servicio de computación en la nube (CLOUD COMPUTING), por lo tanto el valor expresado no incluye esta imposición tributaria

Contact Information

Pedro E. Mejia Ochoa
Gerente General
TE&I Consultores SAS
+504-9990-7990
Pedro.mejia@tei-consultores.com

Definiciones

- Reactor: interfaz principal de Chainalysis para investigadores
- Observaciones: función dentro de Reactor que permite presentar la ubicación de IP para ciertos tipos de billetera
- Nodos: función dentro de Reactor que permite identificar la ubicación IP de los servidores/servicios
- BTC-Bitcoin
- Usuario "nombrado": una estructura de licencia primaria para identificar la cantidad de licencias asignadas a usuarios individuales; generalmente coincide con la dirección de correo electrónico única de un usuario individual.
- En las instalaciones: no se propone, pero se señaló en diapositivas anteriores que Reactor tiene la capacidad de ejecutarse en una infraestructura dedicada alojada o a la que accede la UIF; generalmente utilizada por organizaciones que requieren acceso a la capacidad pero que no tienen acceso a Internet (lado alto)
- DNM - Mercados DarkNet
- OSINT - Inteligencia de código abierto
- ACS - Advanced Case Support: acceso basado en consultoría a los servicios profesionales de Chainalysis, el personal científico principal y los investigadores