CENTRO DE CAPACITACION
DEL MINISTERIO DEL INTERIOR
DE LA FEDERACION DE RUSIA EN NICARAGUA

Curso:

Formas y métodos modernos de lucha contra la legitimación (lavado) de fondos ilícito, obtenidos por medio de sistemas de pagos electrónicos y criptomonedas

Tema:

Particularidades de la lucha contra legitimación (lavado) de dinero y activos obtenidos de forma ilícita en Uruguay

Elaborado por:

- **Capitán:** Alda Dersis Delgado
- **Teniente:** Jorvil de Jesús Galeano.
- **Teniente :** Yisenia Danelia Pérez Martínez.
- **Inspectora :** Magaly del Carmen Torrez Pineda.

Docentes:

- **Teniente coronel:** Seleznev Pavel Bladimirovich.
- **Coronel de Policía :** Grachiov Sergey Alexandrovich

УЧЕБНЫЙ ЦЕНТР МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В НИКАРАГУА

Тема:

Особенности борьбы с легализацией (отмыванием) незаконно полученных доходов в Уругвае

Участники группы 5:
Капитан: Альда Дерсис Дельгадо
Лейтенант: Йорвиль Хесуса Галеано.
Лейтенант: Йисения Даниэла Перес Мартинес.
Инспектор: Магали из Кармен Торрес Пинеда.

Учителя:
Подполковник полиции: Селезнев Павел Владимирович.
Полковник полиции: Грачев Сергей Александрович

INTRODUCCIÓN

Dado el rápido desarrollo de los instrumentos conocidos como “activos virtuales” y su creciente operativa tanto a nivel global como doméstico, se considera necesario dar mayor certidumbre y claridad sobre este fenómeno y sus consideraciones normativas, con el objetivo de que su desarrollo en el mercado local, así como su utilización en los distintos servicios financieros sean seguros.

En este sentido, el Banco Central del Uruguay en cumplimiento de sus finalidades, debe garantizar la protección a los consumidores e inversores, el buen funcionamiento de los mercados y mitigar los riesgos para la estabilidad financiera y de política monetaria que puedan derivarse del uso de activos virtuales.

Según el Marco Conceptual para el tratamiento regulatorio de activos virtuales, esta orientado a la comprensión y categorización de los distintos instrumentos y sus operativas con el objetivo de contribuir al análisis de un enfoque regulatorio para los Activos Virtuales(AV) en el país de URUGUAY.

ВВЕДЕНИЕ

Учитывая быстрое развитие инструментов, известных как «виртуальные активы», и расширение их операций как на глобальном, так и на национальном уровне, считается необходимым обеспечить большую определенность и ясность в отношении этого явления и связанных с ним регулятивных соображений, с тем чтобы его развитие на локальном рынке , а также его использование в различных финансовых сервисах являются безопасными.

В этом смысле Центральный банк Уругвая в соответствии со своими целями должен гарантировать защиту потребителей и инвесторов, надлежащее функционирование рынков и снижать риски для финансовой стабильности и денежно-кредитной политики, которые могут возникнуть в результате использования виртуальных активов. .

Согласно Концептуальным основам регулирования виртуальных активов, он направлен на понимание и классификацию различных инструментов и их операций с целью содействия анализу подхода к регулированию виртуальных активов (АВ) в стране УРУГВАЙ.

MARCO LEGAL

LEY ASUNTO: 152583
EL BANCO CENTRAL DEL URUGUAY PODRÁ REGULAR LOS CRIPTOACTIVOS EN SUS DIVERSAS FORMAS, INCLUIDAS LAS CRIPTOMONEDAS Y LOS CRIPTOTOKENS, SIEMPRE RESPETANDO LOS PRINCIPIOS PREVISTOS EN LA PRESENTE LEY.

Ley Nº 18.494
CONTROL Y PREVENCIÓN DE LAVADOS DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISM**O**

Decreto N° 147/018
APROBACION LA ESTRATEGIA NACIONAL PARA LA LUCHA CONTRA EL LAVADO DE ACTIVOS EL FINANCIMIENTO DEL TERRORISMO Y LA PROLIFERACION DE ARMAS DE DESTRUCCION MASIVA BASADA EN RIESGOS Y SU PLAN DE ACCION

Resolución N° 16/017
SANCIONES POR INCUMPLIMIENTO DE NORMATIVA CONTRA EL LAVADO DE ACTIVOS Y EL FINANCIAMIENTO DEL TERRORISMO.

ПРАВОВЫЕ РАМКИ

Закон 152583
ЦЕНТРАЛЬНЫЙ БАНК УРУГВАЯ МОЖЕТ РЕГУЛИРОВАТЬ КРИПТОАКТИВЫ В ИХ РАЗЛИЧНЫХ ФОРМАХ, ВКЛЮЧАЯ КРИПТОВАЛЮТЫ И КРИПТОТОКЕНЫ, ВСЕГДА СОБЛЮДАЯ ПРИНЦИПЫ, ПРЕДУСМОТРЕННЫЕ НАСТОЯЩИМ ЗАКОНОМ.

Закон № 18,494
КОНТРОЛЬ И ПРЕДОТВРАЩЕНИЕ ОТМЫВАНИЯ ДЕНЕГ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

Указ № 147/018
УТВЕРЖДЕНИЕ НАЦИОНАЛЬНОЙ СТРАТЕГИИ БОРЬБЫ С ОТМЫВАНИЕМ ДЕНЕГ, ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА И РАСПРОСТРАНЕНИЕМ ОРУЖИЯ МАССОВОГО УНИЧТОЖЕНИЯ НА ОСНОВЕ РИСКОВ И ПЛАНА ЕЕ ДЕЙСТВИЙ

Постановление № 16/017
САНКЦИИ ЗА НАРУШЕНИЕ ПОЛОЖЕНИЙ О БОРЬБЕ С ОТМЫВАНИЕМ ДЕНЕГ И ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА.

Organismos para la prevención del LA/FT

Grupo de Acción Financiera de Latinoamérica (GAFILAT)

Unidades de Inteligencia Financiera (UIF)

EGMONT GROUP

La Unidad de Información y Análisis Financiero fue creada por Resolución del Directorio del Banco Central del Uruguay de fecha 20/12/2000, comunicada mediante la Circular No. 1722 de 21 de diciembre de 2000 y desde esa fecha desempeña las funciones de Unidad de Inteligencia Financiera de Uruguay.

Организации по предотвращению ОД/ФТ

Латиноамериканская группа финансовых действий (GAFILAT)

Подразделения финансовой разведки (ПФР)

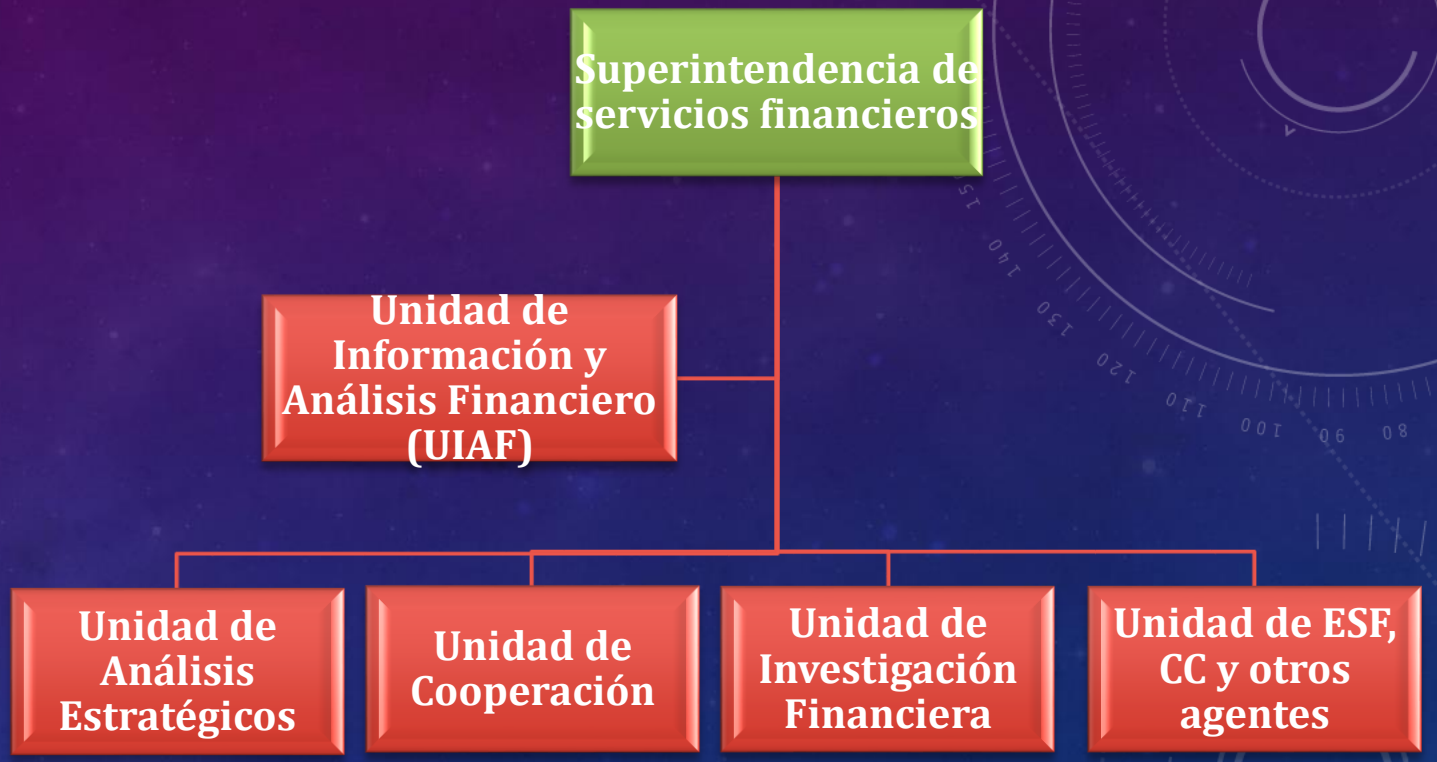
ЭГМОНТ ГРУП

Группа финансовой информации и анализа была создана Постановлением Совета директоров Центрального банка Уругвая от 20.12.2000 г., сообщенная Циркуляром № 1722 от 21 декабря 2000 г., и с этой даты выполняет функции Подразделения финансовой разведки Уругвая..

Estructura organizativa de UIAF y su integración en la Superintendencia de Servicios Financieros

La Ley 18.401 de 24 de octubre de 2008 -modificativa de la Carta Orgánica del Banco Central del Uruguay- establece que la Unidad de Información y Análisis Financiero funciona en el ámbito de la Superintendencia de Servicios Financieros (SSF).

Esta Superintendencia es un órgano del Banco Central que actúa en forma desconcentrada y con autonomía técnica y operativa y tiene como cometido el desarrollo de la regulación y fiscalización de las entidades que integran el sistema financiero nacional



lo que incluye, entre otras instituciones, a los intermediarios financieros, las empresas de servicios financieros, casas de cambio, las bolsas y los intermediarios de valores, las empresas de transferencias de fondos, las empresas de seguros y reaseguros, las administradoras de fondos de inversión, las administradoras de fondos de ahorro previsional, las empresas administradoras de crédito, etc.

Организационная структура UIAF и ее интеграция в Управление финансовых услуг

Закон 18 401 от 24 октября 2008 г., вносящий изменения в Органический устав Центрального банка Уругвая, устанавливает, что Группа финансовой информации и анализа действует в рамках Управления финансовых услуг (SSF).

Это управление является органом Центрального банка, который действует децентрализованно и с технической и оперативной автономией, и его задача заключается в разработке регулирования и надзора за субъектами, которые составляют национальную финансовую систему,

которая включает, среди прочих учреждений, финансовых посредников, компании по оказанию финансовых услуг, бюро по обмену валюты, фондовые биржи и посредников по ценным бумагам, компании по переводу средств, страховые и перестраховочные компании, управляющие инвестиционными фондами, управляющие пенсионными накопительными фондами, компании по управлению кредитами и т.д.

Funciones de la UIAF

Unidad de Análisis Estratégico apoya la función de inteligencia a partir de: a) el análisis de las operaciones (identificación de tipologías y patrones de comportamiento en relación al lavado de activos y el financiamiento del terrorismo), b) el apoyo para el diseño de políticas y metas

Unidad de Cooperación tiene a su cargo la función de cooperación nacional e internacional para la investigación del LA/FT, tarea en la que debe interactuar con las autoridades judiciales y otros organismos públicos competentes a nivel nacional, además de intercambiar información con unidades de inteligencia financiera del exterior.

Unidad de Investigación Financiera: es la responsable de la recepción y análisis de los Reportes de Operaciones Sospechosas, estudios sobre el funcionamiento del sistema, tipologías de lavado o financiamiento del terrorismo.

Unidad de Supervisión de Empresas de Servicios Financieros, Casas de Cambio y Otros Agentes tiene a su cargo la función de supervisión sobre aquellas entidades cuyo objetivo principal de supervisión es la prevención del lavado de activos y el financiamiento del terrorismo, de acuerdo al Marco Estratégico de la Superintendencia de Servicios Financieros

Функции УИАФ

Группа Стратегического Анализа поддерживает функцию разведки на основе: а) анализа операций (выявление типов и моделей поведения в отношении отмывания денег и финансирования терроризма), б) разработки политики и целей

Отдел сотрудничества отвечает за национальное и международное сотрудничество в расследовании ОД/ФТ, где он должен взаимодействовать с судебными органами и другими компетентными государственными органами на национальном уровне, в дополнение к обмену информацией с иностранной финансовой разведкой

Группа финансовых расследований отвечает за получение и анализ отчетов о подозрительных операциях, исследований работы системы, типологий отмывания денег или финансирования терроризма

Группа по надзору за компаниями, оказывающими финансовые услуги, обменными пунктами и другими агентами отвечает за функцию надзора за теми организациями, основной целью которых является предотвращение отмывания активов и финансирования терроризма, в соответствии со Стратегическими рамками Управления финансового надзора

CRIPTOMONEDAS Y CRIPTOBILLETERAS MAS USADAS

El entorno de los criptoactivos presenta un crecimiento que, al menos por los momentos, parece imparable. Nuevos proyectos e iniciativas interesantes y muy innovadoras surgen con bastante frecuencia, brindando mayores oportunidades tanto para los usuarios principiantes como para los más experimentados.

Criptomonedas uruguayas podríamos mencionar:

Farret Token
Ñeripeso
Urbit
MateCoin

Se trata de tokens diseñados y lanzados en Uruguay con la finalidad de proporcionar una alternativa de ahorros, un medio de pago confiable y una herramienta para familiarizarse con el mundo de las monedas virtuales.

Ferret Token

Desarrollo a cargo de la empresa financiera inBierto.com, Ferret Token se presenta como una criptomoneda implementada y verificada en Binance Smart Chain.

НАИБОЛЕЕ ИСПОЛЬЗУЕМЫЕ КРИПТОВАЛЮТЫ И КРИПТОВАЛЮТНЫЕ КОШЕЛЬКИ

Среда криптоактивов демонстрирует рост, который, по крайней мере на данный момент, кажется неостановимым. Новые интересные и инновационные проекты и инициативы появляются довольно часто, предоставляя больше возможностей как новичкам, так и более опытным пользователям.

Уругвайские криптовалюты, которые мы могли бы упомянуть:

Farret Token
Ñeripeso
Urbit
MateCoin

Это токены, разработанные и запущенные в Уругвае с целью предоставить альтернативу сбережениям, надежное средство платежа и инструмент для знакомства с миром виртуальных валют.

Farret Token, разработанный финансовой компанией inBierto.com, представлен как криптовалюта, внедренная и протестированная в Binance Smart Chain.

¿Qué es una wallet para Criptomonedas?

Es para sus activos de criptomonedas lo mismo que una cuenta corriente bancaria para su dinero en efectivo.

Son dispositivos de hardware, programas o apps para móvil diseñados específicamente con el fin de proteger sus activos de Criptomonedas de las múltiples ciberamenazas a las que se enfrenta la Industria de las criptomonedas.

La única diferencia con la tradicional cuenta de seguridad bancaria es que, mientras la caja fuerte guarda el dinero en efectivo, el wallet de criptomonedas guarda las claves privadas que se usan para acceder a su criptomonedas, la prueba de que es usted el verdadero dueño de los criptomonedas.

Las claves, en este caso, son un complejo código alfanumérico generado tras cada transacción de criptomonedas.

¿Что такое криптовалютный кошелек?

Для ваших криптовалютных активов это то же самое, что текущий счет для ваших наличных.

Это аппаратные устройства, программы или мобильные приложения, специально разработанные для защиты ваших криптовалютных активов от многочисленных кибер-угроз, с которыми сталкивается криптовалютная индустрия.

Единственная разница с традиционной банковской учетной записью заключается в том, что в то время как в сейфе хранятся деньги наличными, криптовалютный кошелек хранит закрытые ключи, которые используются для доступа к вашим криптовалютам, как доказательство того, что вы являетесь истинным владельцем этой криптовалюты.

Ключи в данном случае представляют собой сложный буквенно-цифровой код, генерируемый после каждой криптовалютной транзакции.

Tipos de wallet para Criptomonedas

- Dispone de pantalla táctil en color
- Puede realizar todas las transacciones directamente en el dispositivo
- Puede ver las transacciones en la pantalla
- Puede albergar cientos de criptomonedas y tokens ERC20
- Opciones de copia de seguridad seguras

La principal ventaja es que tiene bluetooth, lo que la convierte en la primera cartera de hardware que se conecta con los dispositivos. Es más seguro que usar sólo una aplicación, porque todas las transacciones se firman con el Nano X

- Pantalla monocromática y dos botones físicos
- Debe estar conectado a un dispositivo para introducir el PIN y la frase de contraseña
- Se pueden ver las transacciones en la pantalla
- Permite almacenar cientos de criptomonedas y tokens ERC20
- Opciones de copia de seguridad seguras

Типы wallet для Криптоденег

- Имеет цветной сенсорный экран
- Можно совершать все транзакции прямо на устройстве
- Можно видеть транзакции на экране
- Может хранить сотни криптовалют и токенов ERC20
- Безопасные варианты резервного копирования

Основным преимуществом является наличие Bluetooth, что делает его первым аппаратным кошельком, который подключается к устройствам. Это более безопасно, чем использование только одного приложения, поскольку все транзакции подписываются с помощью Nano X.

- Монохромный экран и две физические кнопки
- Вы должны быть подключены к устройству, чтобы ввести PIN-код и кодовую фразу.
- Транзакции можно увидеть на экране
- Позволяет хранить сотни криптовалют и токенов ERC20
- Безопасные варианты резервного копирования

Instalación del primer cajero automático (terminal)

La inauguración del cajero, que quedó instalado en un céntrico lugar de Punta del Este epicentro de la actividad social en el verano austral, contó con el apoyo de Binance Uruguay - plataforma de compraventa de criptomonedas y la presencia de Carlos Enciso, embajador de Uruguay en Argentina.

Los creadores del cajero, desarrollado íntegramente en Uruguay, buscan ampliar la red en Maldonado (departamento del sureste uruguayo donde está Punta del Este) y posteriormente, llevarla a Montevideo y Colonia (suroeste), otro de los puntos más turísticos del país, como próximos objetivos.

Установка первого банкомата (терминала)

Открытие банкомата, установленного в центре города Пунта-дель-Эсте, эпицентра социальной активности в периоды южного лета, произошло при поддержке Binance Uruguay — платформы для торговли криптовалютой и в присутствии Карлоса Энсисо, посла Уругвая в Аргентине.

Создатели банкомата, полностью разработанного в Уругвае, стремятся расширить сеть в Мальдонадо (юго-восточный уругвайский департамент, где находится Пунта-дель-Эсте), а затем перенести ее в Монтевидео и Колонию (юго-запад), еще одно из самых туристических мест в стране.

Fake Coins

El programa de la Unión Europea **"EL PAcCTO"** y la red de cooperación **CibEL@,** presentaron la campaña de comunicación "FakeCoins: Estafas con criptomonedas" con el objetivo de concienciar a la ciudadanía sobre las estafas con criptomonedas más comunes detectadas en 17 países de América Latina y la Unión Europea.

El objetivo es que la ciudadanía pueda informarse sobre los casos de delito más habituales para poder identificarlos, saber qué hacer y cómo consultar los canales de denuncia de cada país participante.

Las criptomonedas se han popularizado como fenómeno mediático y como un nuevo instrumento de inversión. Como tal, son una herramienta financiera legal y útil si se sabe hacer uso de ellas. Sin embargo, a raíz de su fama, han aparecido una serie de estafas que, utilizando las criptomonedas como gancho, confunden a los inversores con el fin de sustraer su dinero.

Fake Coins/
Фальшивые монеты

Программа Европейского Союза «EL PAcCTO» и сеть сотрудничества CibEL@ представили информационную кампанию «FakeCoins: Мошенничество с криптовалютами» с целью повышения осведомленности общественности о наиболее распространенных мошенничествах с криптовалютой, обнаруженных в 17 странах Латинской Америки и Европейского Союза.

Цель кампании состоит в том, чтобы граждане могли узнать о наиболее распространенных преступлениях, чтобы их идентифицировать, знать, какие каналы существуют и как к ним обращаться для заявлений в каждой участвующей стране.

Криптовалюты стали популярны как медийное явление и как новый инвестиционный инструмент. Как таковые, они являются законным и полезным финансовым инструментом, если вы знаете, как их использовать. Однако на волне их известности появилось множество мошенников, которые, используя криптовалюты в качестве приманки, вводят инвесторов в заблуждение, чтобы украсть их деньги.

Delitos más habituales

- **Estafas mediante la simulación o suplantación:**

“WebCoin"- Во время мошенничества обычно используются веб-сайты, имитирующие инвестиционные портфели. В некоторых случаях они могут выдавать себя за сайт, где пользователь зарегистрирован и хочет получить свои учетные данные для доступа к своему счету. В других случаях они будут представлять себя как новый сайт, где потерпевший будет думать, что совершает реальные операции по покупке и продаже криптовалюты.

“AppCoin” - Igual que con las Webs existen aplicaciones que suplantan las carteras de inversión real o, en otros casos, que son aplicaciones que parecen ser carteras de inversión en criptomonedas, pero que realmente simulan ser reales para obtener los datos bancarios de la víctima.

- **Estafas utilizando la imagen de un famoso:**

“CelebriCoin” - Cómo decir que no a ese personaje tan famoso que admiras que te dice que, si inviertes, te harás rico en pocos días y de forma extrema.

- **Estafas mediante la seducción:**

“BesuCoin” - También conocida como “DonjuanCoin” o KissCoin. Esta estafa se caracteriza porque el estafador seduce a la víctima, a veces usando aplicaciones de contactos tipo Tinder para convencerla más adelante en que invierta en Bitcoins o en otras criptomonedas, pero realmente lo único que estarán haciendo es engañarlos para conseguir su dinero.

Самые распространенные преступления

Мошенничество путем имитации или выдачи себя за другое лицо:

«WebCoin» — Во время мошенничества обычно используются веб-сайты, имитирующие инвестиционные проекты. В некоторых случаях они могут выдавать себя за сайт, где пользователь зарегистрирован и хочет получить свои учетные данные для доступа к своему счету. В других случаях они представляются как новый сайт, где потерпевший будет думать, что совершает реальные операции по покупке и продаже криптовалюты.

«"AppCoin" - Как и с веб-сайт, существуют приложения, которые выдают себя за настоящие инвестиционные кошельки или, в других случаях, это приложения, которые выглядят как криптовалютные инвестиционные кошельки, но на самом деле делают вид, что они настоящие, чтобы получить банковские данные пострадавшего.

Мошенничество с использованием знаменитостей :

“CelebriCoin» - Как сказать «нет» известному человеку, которым вы восхищаетесь, который говорит вам, что если вы инвестируете, то разбогатеете через несколько дней.

Мошенничество через соблазнение :

“BesuCoin» — также известен как «DonjuanCoin» или KissCoin. Эта афера характеризуется тем, что мошенник соблазняет потерпевшего, иногда используя приложения для знакомств, похожие на Tinder, чтобы позже убедить его/её инвестировать в биткойны или другие криптовалюты, но на самом деле все, что они делают, это получение денег обманным путем.

Delitos más habituales

- **Estafas de captación piramidal:**

  “PiramiCoin” - !Cuánta más gente logres convencer para que invierta en la Web mayor será tu beneficio en Criptomonedas! O tal vez, ¿te llegó la invitación personal de un amigo para recibir una oferta súper especial? En cualquiera de los dos casos es posible que estés ante una estafa piramidal que utilice algún tipo de Criptomonedas como gancho.

- **Falsas promociones en el e-mail:**

  “MailCoin” - Esta estafa aparecerá en la bandeja de entrada de tu correo electrónico, acompañada de testimonios de famosos, promesas de multiplicar rápidamente tu inversión o, incluso, ofreciendo las primeras Criptomonedas gratuitas. Te pedirá que te registres en un portal que resultará ser falso, o te notificará con un mail de pérdida de contraseña.

Самые распространенные преступления

Схема Пирамиды :

“PiramiCoin» - !Чем больше людей вам удастся убедить инвестировать в Сеть, тем больше будет ваша прибыль в криптовалютах! Или, может быть, ¿Вы получили личное приглашение от друга, с супер специальным предложением для приобретения чего либо? В любом случае, возможно, вы столкнулись с мошеннической пирамидой, которая использует какой-то тип криптовалюты в качестве крючка.

Ложные рекламные объявления по электронной почте:

«MailCoin» — эта афера появится в вашем электронном почтовом ящике в сопровождении с отзывами знаменитостей, обещаний быстро приумножить ваши инвестиции или даже предложить первые бесплатные криптовалюты. У вас попросят зарегистрироваться на портале, который окажется ложным, или вас уведомят по электронной почте о потерянном пароле.

Operación "Bitcoins"

La Policía detuvo a un Hacker uruguayo que robó información importante de una institución y extorsionó a cambio de dinero. La operación llevó 7 meses de investigación y en las últimas horas un hombre de 41 años fue procesado con prisión por la Justicia.

La denuncia fue radicada por parte de los representantes de una mutualista de asistencia médica privada de Uruguay , ante la Sección Delitos Tecnológicos de la Dirección General de Lucha Contra el Crimen Organizado e INTERPOL (D.G.L.C.C.O. e I.).

En la misma, expusieron que el sistema Informático de la misma recibió un ciberataque contra su base de datos, desde dónde se robó información sensible de la empresa. Posteriormente esa entidad recibió una solicitud de dinero a cambio de liberar dicha información, a través de un correo electrónico.

Según informaron desde la (D.G.L.C.C.O. e I.), "el autor solicitó 15 bitcoins (moneda virtual que asciende a unos 4000 dólares la unidad, en el mercado) y a partir del pedido, cada 24 horas que pasaran, se incrementaría en 5 bitcoins".

Операция «Bitcoins "

Полиция арестовала уругвайского хакера, который похитил важную информацию из учреждения и вымогал деньги. Следствие длилось 7 месяцев, 41-летний мужчина был привлечен к уголовной ответственности и приговорен к тюремному заключению.

Заявление было подано представителями частного общества взаимной медицинской помощи в Уругвае в отдел по борьбе с технологическими преступлениями Главного управления по борьбе с организованной преступностью и Интерпола (D.G.L.L.C.C.O. e I.).

Они указали в нем, что их компьютерная система подверглась кибер-атаке на базу данных, откуда была похищена конфиденциальная информация компании. Впоследствии компания получила по электронной почте требование денег в качестве компенсации за не разглашение этой информации. По словам (D.G.L.L.C.C.O. и И.), «преступник запросил 15 биткоинов (виртуальная валюта, стоимость которой на рынке составляет около 4000 долларов за единицу) и после запроса, каждые 24 часа, которые прошли, она увеличивалась на 5 биткоинов".

Operación "Bitcoins"

La investigación Personal de la Sección Delitos Tecnológicos (SDT), en conjunto con Presidencia de la República a través de la Agencia de Seguridad del Gobierno (AGESIC) siguieron los rastros de las direcciones IP que fueron utilizadas para enviar los correos, en una operación que duró varios meses.

La misma estuvo a cargo del Juzgado Letrado Penal de 11er. Turno y la Fiscalía de 20mo. Turno, que dispuso las actuaciones inmediatas.

En los últimos días, los investigadores identificaron la procedencia de este ataque cibernético, así como la identidad de quién lo realizó. Esto determinó un allanamiento en la capital del país donde ubicaron a un uruguayo de 41 años, de profesión ingeniero informático a quien se le incautó una importante cantidad de material informático y otros efectos.

Del domicilio del autor, la Policía incautó 6 computadoras notebook, 5 teléfonos celulares; un lector/grabador de tarjetas (dispositivo que se utiliza para clonar tarjetas magnéticas); un lector/grabador de discos duros; un router; 13 discos duros de computadora; 125 plásticos de tarjetas magnéticas originales, 1 post de tarjetas magnéticas; 16 pendrives; 2 impresoras a color y una guillotina.

Операция «Bitcoins "

Следственный персонал из Отдела по технологическим преступлениям (SDT) вместе с Президентом Республики через Агентство государственной безопасности (AGESIC) проследил следы IP-адресов, которые использовались для отправки электронных писем, в ходе операции, которая длилась несколько месяцев.

Эта операция находилась в ведении 11-го уголовного суда и 20-го отделения прокуратуры, которые отдали приказ о немедленных действиях.

Исследователи установили происхождение этой кибератаки, а также личность того, кто ее осуществил. Был подписан приказ об обыске его дома, в столице страны, где был обнаружен 41-летний уругваец, инженер-компьютерщик по профессии, у которого было изъято значительное количество компьютерных материалов и других вещей.

В доме исполнителя преступления полиция изъяла 6 ноутбуков, 5 сотовых телефонов; устройство чтения/записи карт (устройство, используемое для клонирования магнитных карт); устройство чтения/записи жесткого диска; маршрутизатор; 13 жестких дисков компьютеров; 125 пластиков оригинальных магнитных карт; 16 флешек; 2 цветных принтера и гильотина.

Otros delitos

La Policía ubicó en el apartamento de esta persona una importante cantidad de dinero, de dudosa procedencia, la cual por mandato de la Justicia fue enviada para su análisis a la Dirección Nacional de Policía Científica, para determinar si se trata de dinero falso. En este caso, se incautaron de $1.460 dólares, $8.320 euros, $157 reales y $3.180 pesos uruguayos.

Desde la Sección de Delitos Tecnológicos (SDT) indicaron a UNICOM que "este es el primer caso registrado en Uruguay de una persona que comete este tipo de delitos y que tiene un cabal conocimiento de transacciones con bitcoins".

La Justicia dispuso el procesamiento con prisión de A.D.H.A. como autor responsable de un delito de conocimiento fraudulento de documentos secretos, en concurrencia, fuera de la reiteración real, con un delito de extorsión en grado de tentativa.

Asimismo, dispuso que profesionales de esa Unidad realizaran las pericias pertinentes a los equipos informáticos incautados para determinar otros posibles ataques por parte del autor.

Por otra parte, esta operación continúa en curso "a fin de determinar si el responsable cometió otros delitos similares que aún no hayan sido denunciados" indicaron desde la SDT.
Fuente: (D.G.L.C.C.O. e I.)

Другие преступления

Полиция обнаружила в квартире этого лица крупную сумму денег сомнительного происхождения, которая по распоряжению судьи была направлена на анализ в Национальное управление научной полиции, чтобы определить, являются ли деньги фальшивыми. В данном случае было изъято 1460 долларов США, 8320 евро, 157 реалов и 3180 уругвайских песо.

В Секции технологических преступлений (SDT) UNICOM указали, что «это первый случай, зарегистрированный в Уругвае, в отношении лица, которое совершает этот вид преступления и полностью осведомлено о транзакциях с биткойнами».

Суд постановил привлечь к ответственности с лишением свободы A.D.H.A. как исполнителя преступления “мошеннического ознакомления с секретными документами”, в совокупности, с преступлением, связанным с попыткой вымогательства.

Он также поручил специалистам этого подразделения провести соответствующие экспертизы изъятого компьютерного оборудования, чтобы определить другие возможные атаки преступника.

С другой стороны, эта операция продолжается до сих пор, "чтобы установить, не совершал ли виновный других подобных преступлений, о которых еще не сообщалось", указали в ГДТ.
Источник: (D.G.L.C.C.O. и I.)

Evidencias
Доказательства

Código Penal N° 9155

APROBADO POR LEY N° 9.155

Artículo 300 (Conocimiento fraudulento de documentos secretos)

El que, por medios fraudulentos, se enterare del contenido de documentos públicos o privados, que por su propia naturaleza debieran permanecer secretos, y que no constituyeran correspondencia, será castigado siempre que del hecho resultaren perjuicios, con 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables) de multa.

Artículo 345 (Extorsión)

El que, con violencias o amenazas, obligare a alguno a hacer, tolerar o dejar de hacer algo contra su propio derecho, para procurarse a sí mismo o para procurar a otro un provecho injusto, en daño del agredido o de un tercero, será castigado con cuatro a diez años de penitenciaría.

Уголовный кодекс № 9155

УТВЕРЖДЕНО ЗАКОНОМ № 9.155

Статья 300 (Мошенническое ознакомление с секретными документами)Тот, кто обманным путем узнает содержание государственных или частных документов, которые по своей природе должны оставаться секретными и которые не являются перепиской, наказывается, если это повлекло за собой ущерб, штрафом в размере от 20 R.U. (двадцати единиц гибкого курса) до 400 R.U. (четырехсот единиц гибкого курса).

Статья 345 (Вымогательство)
Тот, кто с применением насилия или угроз принуждает кого-либо делать, терпеть или прекращать делать что-либо вопреки собственному праву, с целью получения несправедливой выгоды для себя или другого лица, во вред потерпевшему или третьему лицу, подлежит наказанию в виде лишения свободы от четырех до десяти лет.

Referencias
Ссылки

https://kpmg.com/uy/es/home/insights/2022/04/cajeros-automaticos-de-criptomonedas-en-uruguay-tienen-regularidad-juridica.html

https://www.gub.uy/secretaria-nacional-lucha-contra-lavado-activos-financiamiento-terrorismo/institucional/normativa/resolucion-n-16017-sanciones-incumplimiento-normativa-contra-lavado-activos

https://www.minterior.gub.uy/index.php/unicom/noticias/4971-operacion-bitcoins#:~:text=La%20Polic%C3%ADa%20detuvo%20a%20un,con%20prisi%C3%B3n%20por%20la%20Justicia.

https://fakecoins.org/

Gracias por su atención….

Спасибо за ваше внимание….