2025

CIBER inteligencia

ANÁLISIS Y TENDENCIAS

Guardia Civil

LA AMENAZA TECNOLÓGICA

Actualización de métodos y tendencias detectados durante el año 2025

GRUPO DE CIBERINTELIGENCIA CRIMINAL
UNIDAD TÉCNICA DE POLICÍA JUDICIAL

Marzo 2026
Unidad Técnica de Policía Judicial
Jefatura de Policía Judicial

Príncipe de Vergara, 246
28016 Madrid
(+34) 91 514 69 40

CONTENIDOS

PRESENTACIÓN

La socialización de las nuevas tecnologías, derivada de la expansión acelerada de la transformación digital, ha venido acompañada de un crecimiento sostenido y cada vez más sofisticado de la ciberdelincuencia.

Las organizaciones criminales explotan la dependencia estructural de la tecnología para articular esquemas delictivos cada vez más complejos, impactando directamente, no solo en la actividad económica o la confianza en los servicios digitales, sino también en el ejercicio efectivo de los derechos de la ciudadanía.

Informes recientes de evaluación de la amenaza, nacionales e internacionales, sitúan al malware –especialmente el ransomware– y al fraude online como vectores de ataque predominantes, sin olvidarse como principal manifestación de esa amenaza las sinergias entre el cibercrimen y el crimen organizado transnacional, todo ello en un ecosistema crecientemente industrializado y potenciado por el modelo de crimen como servicio (CaaS-*Crime as a Service*).

En este contexto, la Guardia Civil se consolida como un actor pionero, referente y vertebrador en la respuesta frente al cibercrimen, ejerciendo su función como policía integral con competencias preventivas e investigadoras en todo el territorio nacional.

Esta respuesta de lucha contra el crimen organizado y la delincuencia grave en la red se articula de forma coordinada y complementaria desde la Policía Judicial, combinando capacidades operativas y de inteligencia criminal. A nivel operativo, el Departamento contra el Cibercrimen de la Unidad Central Operativa (UCO) asume la investigación de las formas más graves y complejas de criminalidad en el ciberespacio. En el plano estratégico y de inteligencia, el Grupo de Ciberinteligencia Criminal de la Unidad Técnica de Policía Judicial (UTPJ) aporta una visión integrada del panorama de amenazas, identifica tendencias, apoya la toma de decisiones y facilita la orientación de las investigaciones.

"La Guardia Civil reafirma su compromiso firme y permanente para proteger el ciberespacio y garantizar la seguridad de toda la ciudadanía"

Esta estructura no se circunscribe a nivel central. El auténtico músculo investigador en la Guardia Civil descansa en los EDITEs de las distintas Unidades Orgánicas de Policía Judicial, que actúan sobre el terreno como primera línea especializada de respuesta frente al cibercrimen. Por último, no se debe olvidar que la proximidad al ciudadano es clave en este ámbito, desempeñando un papel fundamental la red de Equipos @.

Estas unidades, diseminadas por todo el territorio nacional, son el pilar sobre el que se sustenta la atención a la víctima, la sensibilización y la canalización ágil de denuncias favoreciendo una cobertura homogénea y eficaz en el conjunto del territorio.

Ante un escenario en el que la convergencia entre el crimen organizado y la explotación sistemática del ciberespacio seguirá intensificándose, la Jefatura de Policía Judicial reafirma su compromiso irrevocable con la prevención, detección y neutralización de las amenazas relacionadas con el cibercrimen. Este compromiso se sustenta en la mejora continua de las capacidades tecnológicas, la especialización permanente de sus unidades y la participación en marcos de cooperación internacional, sin olvidarse el necesario impulso de la colaboración público privada como elemento imprescindible para incrementar la resiliencia del tejido institucional, empresarial y social.

Para finalizar, me gustaría resaltar que este documento pretende reflejar las principales tendencias delictivas observadas por nuestras unidades de investigación, ilustrándolas con casos de éxito. Con su ejemplo, se pone de manifiesto la voluntad de la Guardia Civil de contribuir con su trabajo, como ha hecho desde su fundación, a salvaguardar el ciberespacio como pilar esencial de la soberanía nacional y de la seguridad de toda la ciudadanía.

Alberto Redondo
Comandante Jefe del Grupo de Ciberinteligencia
Unidad Técnica de Policía Judicial
GUARDIA CIVIL

01.- INTRODUCCIÓN

A la par que la sociedad prospera en el ámbito de las tecnologías de la información, con una adopción tecnológica incremental en cada nueva generación, lo hacen las organizaciones criminales beneficiándose para sus fines lucrativos de los avances técnicos.

El ecosistema del cibercrimen ha experimentado una evolución a lo largo de los últimos diez años que se refleja en la eclosión de nuevas figuras delictivas. Los nuevos métodos facilitadores del delito han puesto a la tecnología como base de cualquier actividad criminal, desde el tráfico de estupefacientes a los delitos contra el patrimonio. Esta incidencia transversal llega a borrar en algunas ocasiones la línea que separa el delito "ciber" del que ha empleado la tecnología como medio.

Dentro de la esfera que componen los delitos tecnológicos e igualmente de forma coherente con las tendencias sociales y empresariales, los delincuentes han optado por la especialización, creando así verdaderas redes de intercambio de bienes y servicios, al estilo de subcontrata tradicional, en la figura que comúnmente se conoce como *Crime As A Service*. El crimen como servicio, además de proporcionar a los hechos delictivos una complejidad y profesionalidad mayor, ha generado mercados *underground* u ocultos, en los que se opera con el dinero fruto de la actividad criminal.

El presente informe pretende presentar, a grandes rasgos, las tendencias más importantes observadas desde el Grupo de Ciberinteligencia de la Unidad Técnica de Policía Judicial, el cual ostenta una posición privilegiada en cuanto a visibilidad del panorama tanto nacional como internacional por su carácter de unidad central especializada. La lucha contra el crimen organizado, y en este caso altamente especializado, requiere, además de las herramientas necesarias, los conocimientos exactos y precisos sobre la amenaza.

Esta información es la que se pretende aportar al lector con este documento.

02.- ROBO DE CREDENCIALES

ROBO DE CREDENCIALES BANCARIAS: "LA PRIORIDAD DE LOS ATACANTES"

Durante el último año, el robo de credenciales de todo tipo se ha consolidado como una de las actividades delictivas más frecuentes dentro del ecosistema del cibercrimen.

Aunque este apartado abarca múltiples técnicas -incluyendo *keyloggers*, *infostealers*, ataques de fuerza bruta y explotación de brechas en servicios online-, el robo de credenciales bancarias continúa destacando de forma clara como la amenaza más relevante y persistente, priorizando el engaño directo al usuario como mecanismo para obtener acceso a cuentas financieras.

“MAYOR **SOFISTICACIÓN:**
… MENOS **CONOCIMIENTOS**”

El 2025 nos ha dejado una paradoja llamativa en el ámbito del *phishing*: las campañas son cada vez más sofisticadas desde el punto de vista técnico, pero los actores que las ejecutan requieren menos conocimientos especializados que nunca. Esta tendencia se explica por la proliferación y madurez de los **kits de *phishing* avanzados**, herramientas empaquetadas que automatizan gran parte del proceso delictivo.

Estos kits incorporan funcionalidades que antes solo estaban al alcance de grupos con capacidades técnicas elevadas, como:

- **Clonación precisa** de portales legítimos, con plantillas actualizadas y listas para desplegar.
- **Captura en tiempo real** de credenciales, códigos de autenticación y OTPs, facilitando ataques más eficaces.
- **Integración con servicios ilícitos complementarios**, como paneles de control, sistemas de distribución de campañas o herramientas de evasión.
- **Actualizaciones continuas**, que permiten adaptarse rápidamente a nuevas medidas defensivas.

El resultado es un ecosistema donde la **barrera de entrada** se ha **reducido** drásticamente. Muchos ciberdelincuentes ya no necesitan comprender en profundidad cómo funcionan los protocolos web, las técnicas de suplantación o los mecanismos de seguridad. Basta con **adquirir** o alquilar un **kit,** configurarlo mínimamente y **ponerlo en marcha**. La **sofisticación proviene del software,** no del operador.

Esta dinámica ha contribuido a un **aumento** del **volumen y** la **calidad** de las campañas de **phishing**, al tiempo que ha ampliado el número de actores capaces de ejecutarlas. En consecuencia, el **riesgo** para usuarios y organizaciones se **incrementa**, no por la pericia individual de los atacantes, sino por la **industrialización del fraude digital** y la disponibilidad de herramientas **cada vez más potentes.**

DETENCIÓN de "GoogleXCoder": Se acabó "robarle todo a las abuelas"

La Guardia Civil desarticuló una de las **redes de *phishing* más activas del ámbito hispanohablante** tras detener en Cantabria a un joven brasileño de 25 años, identificado como el desarrollador **"GoogleXCoder"**.

Este individuo era considerado el principal proveedor de herramientas para el robo masivo de credenciales, operando bajo un modelo de ***Crime as a Service*** que facilitaba a numerosos grupos delictivos kits de *phishing* capaces de clonar páginas de bancos y organismos públicos. Sus servicios incluían personalización, soporte y actualizaciones, lo que profesionalizó y amplificó el impacto de las campañas fraudulentas iniciadas en 2023.

La investigación, reveló que los "*phishers*" contrataban estos servicios a través de **Telegram** por cientos de euros al día, **llegando a suplantar decenas de entidades** y estafar a miles de víctimas en una sola jornada. La sensación de impunidad era tal que algunos grupos operativos utilizaban canales con nombres tan explícitos como "Robarle todo a las abuelas".

El desarrollador se movía constantemente entre distintas provincias, usando identidades suplantadas y manteniendo un estilo de vida de "nómada digital" para evitar su localización.

Tras un año de investigación, la operación culminó con registros en seis provincias y la identificación de seis personas vinculadas directamente al uso de estos servicios ilícitos, todo ello con la colaboración la Policía Federal de Brasil y la empresa de ciberseguridad Group-IB.

“EL CIBERDELINCUENTE TRASPASA LA BARRERA DIGITAL”

La creciente facilidad para ejecutar este tipo de delitos, unida a la incorporación de actores con un perfil técnico muy limitado, ha generado entre muchos de ellos una **sensación de impunidad** que reduce su preocupación por ocultar rastros o aplicar medidas básicas de autoprotección.

Esta falta de disciplina operativa se traduce en errores frecuentes, tanto técnicos como operativos que, en conjunto, **abren oportunidades valiosas para la investigación** y permiten a las Unidades establecer líneas de investigación fructíferas.

En 2025 se ha observado como los delincuentes, **tras obtener** acceso a la banca online y **establecer un primer contacto telefónico** con la víctima, donde llevan a cabo diversas transferencias fraudulentas, van más allá y convencen a la víctima de que sus tarjetas bancarias están comprometidas y alguien va a ir a recogerlas a su domicilio, llegando el ciberdelincuente a traspasar a barrera digital y trasladarse físicamente al domicilio a retirar las tarjetas.

INFOSTEALERS Y VENTA DE CREDENCIALES DE **SERVICIOS**

En el último año se ha detectado una expansión significativa de **plataformas alojadas** en la ***surface web*** que ponen a la venta credenciales y accesos ilícitos, no solo a servicios digitales, sino también a **productos de consumo cotidiano**, como puntos en empresas de comida rápida, combustible, tarjetas descuento en supermercados o suscripciones comerciales. Este fenómeno marca un cambio relevante: aunque los pagos continúan realizándose mayoritariamente mediante criptomonedas, **la oferta ya no está restringida a compradores experimentados en la *darknet*.**

Por el contrario, estas plataformas adoptan interfaces simples, modelos de compra directa y una **apariencia casi comercial,** lo que abre el acceso a un público mucho más amplio y reduce la barrera de entrada para usuarios sin conocimientos técnicos ni vínculos previos con mercados clandestinos.

INFOSTEALERS Y GAMING

Se ha identificado una clara conexión entre la **distribución de *infostealers*** y **plataformas que ofrecen parches, modificadores y trucos para videojuegos**. Estos espacios, que suelen atraer a usuarios jóvenes en busca de ventajas competitivas o mejoras gratuitas, se han convertido en un canal ideal para la propagación de malware diseñado para **robar credenciales y datos sensibles**.

Los operadores de *infostealers* aprovechan la confianza que generan estas comunidades y la alta demanda de contenido "gratuito" para **camuflar código malicioso dentro de instaladores**, supuestos parches o herramientas de modificación. Como resultado, muchos usuarios descargan estos archivos sin sospechar que, en segundo plano, el software recopila credenciales de servicios, entre otra información.

OPERACIÓN MOSENIK

La **Guardia Civil**, en el marco de la **Operación MOSENIK**, ha desmantelado una red de infraestructura tecnológica que recopilaba datos para ponerlos a disposición de los ciberdelincuentes. Empleaban una **sofisticada infraestructura de SIMBOX industriales** albergando cientos de módems GSM, que permitía **explotar miles de tarjetas SIM a la vez**, enviando millones de mensajes y llamadas de forma simultánea.

Esta red era controlada por una única persona mediante una decena de ordenadores. **En total se han intervenido** 35 SIMBOX equipadas con 865 módems; más de 60.000 tarjetas SIM nacionales para su uso inmediato; una gran cantidad de dispositivos informáticos, así como dinero en efectivo y en criptomonedas.

03.- BUSINESS EMAIL COMPROMISE

“LA GRAN **AMENAZA** DE NUESTRAS EMPRESAS”

Durante el último año, los incidentes de ***Business Email Compromise*** (BEC) han experimentado **un crecimiento sostenido**, consolidándose como una de las **amenazas más perjudiciales** para el tejido **empresarial nacional.**

Este tipo de fraude, basado en la manipulación de comunicaciones corporativas legítimas, ha demostrado una **capacidad significativa para generar pérdidas económicas y operativas,** afectando de manera especialmente severa a las pequeñas y medianas empresas.

“CIBERSEGURIDAD **LIMITADA**”

La **limitada disponibilidad** de recursos dedicados a la ciberseguridad en este segmento incrementa su exposición y **dificulta la detección temprana** de estas actividades maliciosas.

> “La pronta actuación de la Guardia Civil ha conseguido paralizar millones de euros en transferencias fraudulentas relacionadas con casos BEC”

En este contexto, la Guardia Civil ha puesto **especial énfasis** en trasladar a sus unidades operativas la **importancia** de una **actuación temprana**, subrayando que la rapidez en las **primeras actuaciones** puede resultar determinante para la **recuperación** de fondos comprometidos.

Gracias a este esfuerzo y a la colaboración con diferentes Agencias como INTERPOL, la Guardia Civil ha logrado la paralización de transferencias monetarias fraudulentas por valor de varios millones de Euros, así como la recuperación de importantes sumas.

La **GUARDIA CIVIL** distribuye **DOCUMENTO** de **ANÁLISIS** de **RIESGOS** entre empresas e investigadores como medida de **MITIGACIÓN**

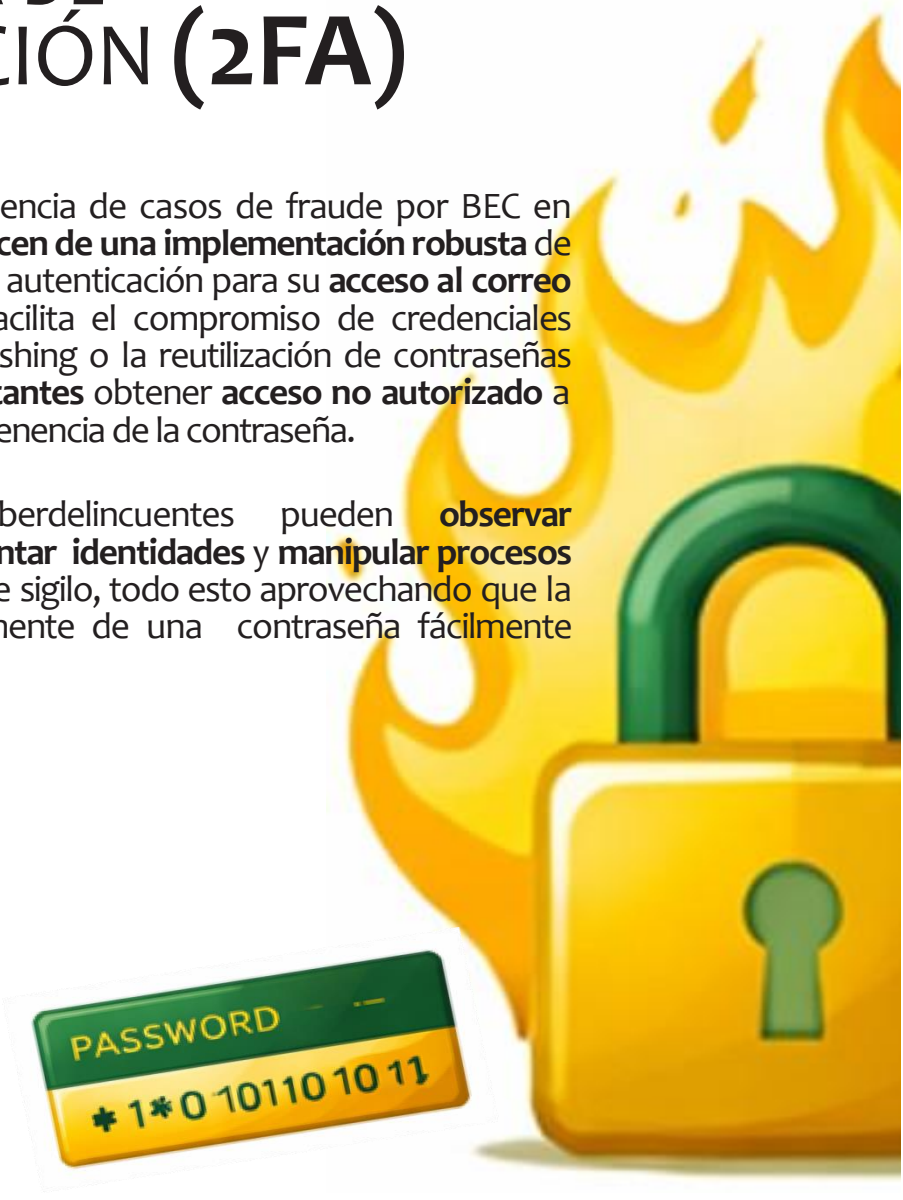
Además, en el marco de la estrecha colaboración que la Guardia Civil mantiene con el sector privado a través del programa Coopera, la UTPJ elaboró y distribuyó un documento de **análisis de riesgos** que expone de manera detallada como operan los BEC.

El informe ofrece a las empresas una serie de **recomendaciones preventivas**, así como **pautas de actuación** en caso de verse afectadas por una estafa de este tipo. Asimismo, en el **ámbito interno**, dicho documento sirve como **guía de referencia** para las Unidades de Investigación, facilitando las primeras actuaciones y el desarrollo de las labores investigativas.

ABUSO DE SERVICIOS DE CORREO ELECTRÓNICO CON **ESCASA** IMPLANTACIÓN DE SISTEMAS DE DOBLE FACTOR DE AUTENTICACIÓN **(2FA)**

Se ha observado una alta incidencia de casos de fraude por BEC en entornos **corporativos que carecen de una implementación robusta** de mecanismos de doble factor de autenticación para su **acceso al correo electrónico**. Esta deficiencia facilita el compromiso de credenciales mediante técnicas como el phishing o la reutilización de contraseñas filtradas, permitiendo a los **atacantes** obtener **acceso no autorizado** a buzones internos, con la simple tenencia de la contraseña.

Una vez dentro, los ciberdelincuentes pueden **observar comunicaciones** legítimas**, suplantar identidades** y **manipular procesos financieros** con un alto grado de sigilo, todo esto aprovechando que la protección depende exclusivamente de una contraseña fácilmente vulnerable.



ORGANIZACIONES TRANSNACIONALES: "LAS DUEÑAS DEL BEC"

En los últimos años, las estafas tipo BEC han dejado de ser un fenómeno exclusivo de grupos especializados en cibercrimen para atraer también la participación de redes criminales tradicionales, que ven en este método una vía eficaz y de bajo riesgo para obtener beneficios económicos significativos. Estas organizaciones encuentran en el BEC una oportunidad para diversificar sus operaciones, aprovechando su infraestructura preexistente para mover fondos robados y reclutar intermediarios.

Un claro ejemplo es la detección de la organización criminal nigeriana conocida como **Neo Black Movement Of Africa / BLACK AXE**, la cual se ha comprobado posee un papel activo en la ejecución de estafas de tipo *Business Email Compromise* (BEC) en nuestro país. Su actividad ha sido objeto de operaciones policiales internacionales, entre ellas la Operación Jackal **[1]**, en la que catorce países de cuatro continentes participaron en un dispositivo coordinado por INTERPOL, contra Black Axe y otros grupos de delincuencia organizada de África Occidental y conllevaron la detención de más de 70 personas.

"La combinación de **conocimientos técnicos** aportados por los ciberdelincuentes y la **logística consolidada** de grupos criminales clásicos…

…incrementa la **sofisticación** y el **impacto.**"

OTF HEARTBREAKER

Desde 2025, la Guardia Civil se encuentra coliderando la **Operational Task Force** (OTF) **"Heartbreaker" de EUROPOL**, bajo el auspicio del AP *High Risk* de EUROPOL, junto con 9 países miembros, así como con el *United States Secret Service* (USSS) de los Estados Unidos. Todo ello con el **fin de combatir la organización** criminal **"Black Axe"**, considerada como ***High Value Target*** en el ámbito policial. Los **principales crímenes investigados** son las estafas de tipo *Business Email Compromise*, *Romance Scam*, así como la falsedad documental, el blanqueo de capitales, el tráfico de drogas y trata de seres humanos con fines de explotación sexual.

Neo Black Movement Of Africa / BLACK AXE

Esta organización tuvo su origen en los años 70 en el entorno estudiantil de la Universidad de Benin (Nigeria). Parte de sus integrantes evolucionó hacia estructuras criminales transnacionales, conservando elementos simbólicos internos como la representación de un "hacha negra".

El grupo criminal ha diversificado sus ámbitos de actuación, combinando ciberdelincuencia - incluyendo fraudes BEC y romance scams - con actividades tradicionales del crimen organizado, como el blanqueo de capitales mediante empresas pantalla y mulas financieras, la trata de seres humanos y la explotación sexual de mujeres trasladadas a Europa y el uso de violencia para garantizar el control interno.

Operan bajo un modelo jerárquico, con un liderazgo central o regional ("*Chairman*") que coordina células autónomas distribuidas en distintos territorios. Se han identificado otros roles diferenciados, como la figura del "*Priest*" encargado de liderar actividades rituales, "*Eyes*" a cargo de la vigilancia, "*Criers*" de la propaganda o el reclutamiento o los "*butchers*", encargados de la parte coercitiva y violenta de la organización.

Aunque su núcleo original se sitúa en Nigeria, la red ha consolidado presencia en varias zonas de Europa, con actividad destacada en Italia, Irlanda, Alemania, Reino Unido y España. Asimismo, se han detectado operaciones financieras ilícitas vinculadas al grupo en América y otros continentes, lo que confirma su alcance transnacional y su capacidad para operar en múltiples jurisdicciones. El modus operandi del grupo combina técnicas de captación en entornos universitarios, redes migratorias y plataformas sociales con la creación de células especializadas en fraude online, explotación de víctimas y blanqueo de capitales.

HIGH VALUE TARGET

EUROPOL, entre otras agencias policiales, utiliza el término ***High Value Target (HVT) -Objetivo de Alto Valor-*** para referirse a individuos de alta prioridad dentro del crimen organizado, cuya actividad delictiva, posición jerárquica o capacidad operativa los convierte en objetivos estratégicos.

Se trata de personas cuya detención o neutralización tiene un impacto significativo en la desarticulación de redes criminales transnacionales, especialmente en ámbitos como el tráfico de drogas, la violencia organizada, los homicidios y otras formas graves de delincuencia.

0 4.- FALSAS INVERSIONES EN CRIPTOMONEDAS

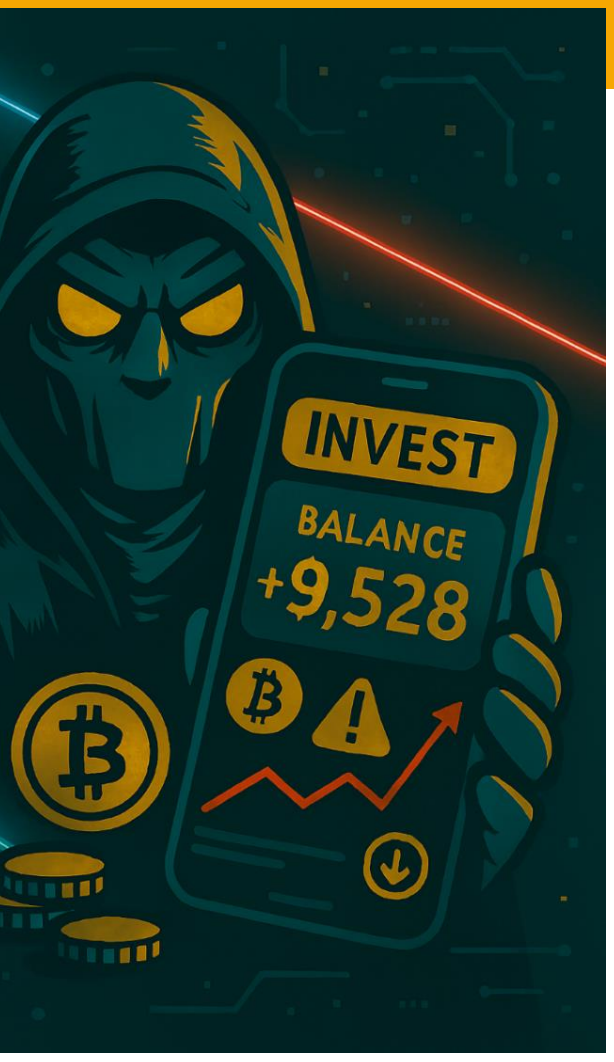
CRIPTO... ARGUCIAS

Durante el último año, las estafas vinculadas a falsas inversiones en criptoactivos han consolidado un **patrón operativo** cada vez más **sofisticado** y **difícil de detectar**. Los análisis realizados muestran dos vectores de evolución de especial interés:

- Por un lado, se observa un incremento notable en el uso de **aplicaciones móviles fraudulentas**, diseñadas para imitar plataformas legítimas de *trading* o gestión de criptoactivos. Estas apps aprovechan la confianza del usuario en el ecosistema móvil para simular inversiones inexistentes y dar credibilidad a la estafa.

- Por otro lado, los **ciberdelincuentes** han **perfeccionado** sus estrategias de **captación y retención de las víctimas**, **trasladándolas** rápidamente desde **canales públicos** -como redes sociales, anuncios o plataformas de citas- **hacia entornos cerrados** como grupos de *WhatsApp* o *Telegram*. En estos espacios privados, los delincuentes aplican técnicas de ingeniería social como la existencia de figuras de **mentores o profesores que dan instrucciones** a la hora de hacer las hipotéticas inversiones.

USO de aplicaciones móviles

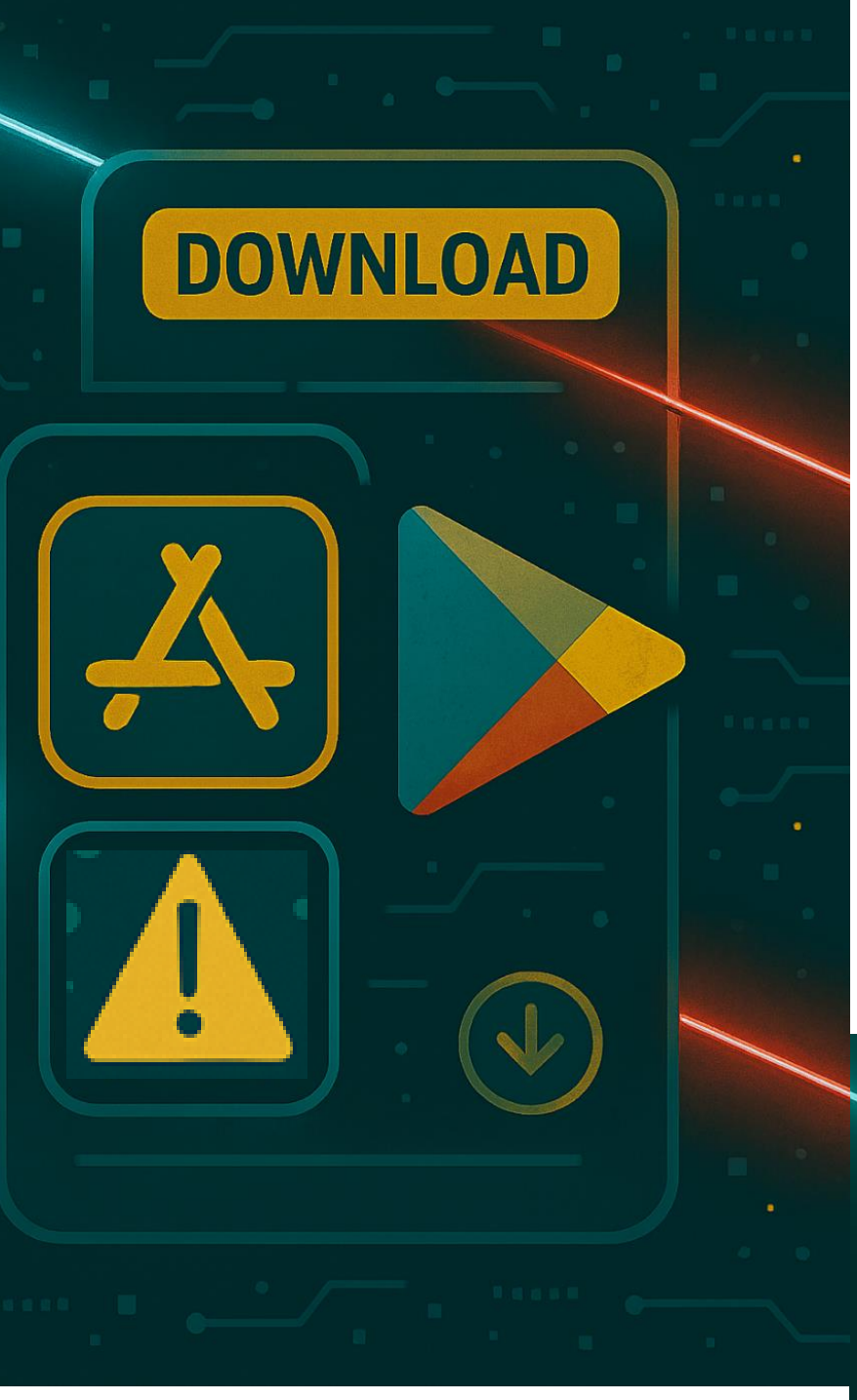


Se ha observado cómo los grupos criminales están desarrollando apps móviles fraudulentas que imitan aplicaciones legítimas de inversión, mostrando **balances con ganancias ficticias** para convencer a las víctimas de que sus fondos están generando altos rendimientos.

A diferencia de las páginas web fraudulentas convencionales, estas **aplicaciones** operan **desde los teléfonos de las víctimas, dejando un menor rastro digital** de su actividad, dificultando la labor forense y de seguimiento (por ejemplo, no quedan históricos web accesibles ni dominios que monitorizar una vez que la app es retirada).

Las aplicaciones identificadas **comparten descripciones genéricas sobre herramientas financieras** y utilizan nombres que simulan productos de inversión, pero en realidad son **interfaces falsas** controladas por los estafadores.

La Comisión Nacional del Mercado de Valores (CNMV) incluyó a varias de ellas en sus **listas de entidades no autorizadas,** advirtiendo de forma expresa que se trataba de **apps** promovidas en grupos de WhatsApp **para defraudar** a inversores.



Algunas de estas aplicaciones lograron incluso publicarse en las **tiendas oficiales de *Android* o *iOS***, otorgándoles una fachada de legitimidad, estando disponibles durante semanas antes de ser eliminadas por incumplir las normas. Durante este periodo **acumularon cientos de descargas**.

Las aplicaciones presentaban en la tienda descripciones y capturas de pantalla profesionales, sin reseñas negativas iniciales, lo que facilitó que víctimas desprevenidas las descargaran confiando en su **aparente legitimidad.**

El **engaño** se ve **potenciado** por la atención personalizada de los **falsos *"brokers"*,** que mantienen **contacto frecuente con la víctima** (vía chat o teléfono), guiándola en el uso de la aplicación y animándola a invertir más dinero.

Grupos de WhatsApp y Telegram

La segunda tendencia identificada se basa en la creación de **grupos cerrados** de ***WhatsApp* y/o *Telegram*** de tipo **"VIP"**, en los que las víctimas son incluidas junto a **miembros** de la **organización criminal** que se hacen pasar por otros inversores exitosos. Los estafadores presentan estos grupos como exclusivos, donde se comparten **"oportunidades de inversión" supuestamente únicas** y consejos financieros de alta calidad.

Desde el primer momento, generan una atmósfera de confianza y éxito: los perfiles falsos publican capturas de ganancias, mensajes celebrando retiros de fondos, o testimonios de cómo "**la estrategia del grupo**" les está enriqueciendo. Esta **dinámica** de "prueba social" sirve para **legitimar** la estafa ante los ojos de **nuevos integrantes**.

Cabe destacar que los administradores de estos grupos utilizan **números de teléfono anónimos**, obtenidos con **identidades falsas** (a menudo se utilizan documentaciones de ciudadanos extranjeros) y contratados a través de operadoras de escasa colaboración policial. De este modo, cada número de *WhatsApp* / *Telegram* aparece registrado a nombre de personas ficticias, dificultando la atribución y el rastreo.

Además, los ciberdelincuentes **suelen cambiar con frecuencia** de **terminal o línea** telefónica para evitar su seguimiento una vez que perciben riesgo de ser descubiertos.

La victimología asociada...

...a este esquema revela que los estafadores suelen dirigirse a **inversores sin experiencia** previa o pequeños ahorradores atraídos por la promesa de ganancias rápidas y fáciles. Estas personas, con **menor conocimiento financiero**, resultan más **vulnerables** a las tácticas de manipulación empleadas.

Una vez **integradas en el grupo "VIP",** la **presión social** ejercida por los falsos inversores, crea un clima de **confianza artificial** que refuerza el engaño. Bajo esta influencia, las víctimas se sienten instadas a invertir sumas cada vez mayores, temiendo perder la oportunidad exclusiva o quedarse atrás respecto al resto del grupo.

La presencia aparente de pares que ya están ganando dinero actúa como incentivo psicológico para minimizar las dudas y continuar aportando capital.

OPERACIÓN "HUMO... DIGITAL"

La Guardia Civil, junto a la Policía Nacional y los Mossos d'Esquadra, y con el apoyo operativo de EUROPOL, ha desmantelado una sofisticada organización criminal dedicada a la comisión de estafas online a gran escala y al posterior blanqueo de capitales.

La estructura delictiva operaba mediante un **ecosistema digital avanzado**, diseñado para generar confianza en las víctimas y facilitar la captación de fondos. El grupo mantenía **numerosas páginas web fraudulentas** que simulaban plataformas de inversión en criptomonedas y empresas de reconocido prestigio, además de difundir **anuncios falsos** que prometían rentabilidades extraordinarias.

Paralelamente, disponían de ***call centers* temporales** equipados con medidas de seguridad extremas, incluyendo un *"botón del pánico"* capaz de desconectar de inmediato los sistemas informáticos ante una posible intervención policial.

En estos centros se realizaba la **gestión personalizada de las víctimas**, estableciendo vínculos de confianza que permitían asegurar el desvío de fondos. Una vez obtenidas las inversiones fraudulentas, la organización activaba una **compleja red financiera** compuesta por empresas pantalla y falsos asesores, diseñada para canalizar y ocultar el origen ilícito del dinero.

Esta infraestructura permitió a los responsables **estafar más de 10 millones de euros a más de 300 víctimas**, enviando la mayor parte de los fondos al extranjero para dificultar su rastreo.

La operación culminó con la **detención de 21 personas** y la recuperación de **más de 1.300.000 euros** en efectivo y criptomonedas. Además, se intervinieron vehículos de lujo, relojes de alta gama y un amplio conjunto de equipos informáticos utilizados para la actividad criminal.

05.- MALWARE

Durante 2025, los *infostealers* y el *ransomware* se consolidan como las **variantes de malware de mayor impacto** dentro del panorama global de ciberamenazas desde un enfoque cualitativo.

Los ***infostealers*** destacan por su capacidad para robar credenciales, datos financieros y accesos corporativos a gran escala, alimentando otros delitos como la estafa informática y el acceso ilícito a redes empresariales.

Paralelamente, el ***ransomware*** mantiene su posición como una de las amenazas más disruptivas, combinando cifrado de sistemas, robo de información y extorsión múltiple para maximizar el daño económico y operativo.

Destaca la consolidación del **ransomware de cuádruple extorsión** como una de las tácticas más agresivas y lucrativas empleadas por los grupos criminales. Este modelo amplía las fases tradicionales del ransomware y **combina múltiples capas de presión para forzar el pago**.

La primera consiste en el **cifrado de los sistemas,** paralizando la actividad operativa de la víctima.

En la segunda los atacantes aplican la **exfiltración y amenaza de publicación de datos,** incrementando el riesgo reputacional y legal.

UN PASO MÁS EN EL *RANSOMWARE:* EXTORSIÓN CUÁDRUPLE

La tercera capa se dirige a los **clientes, socios o empleados** de la organización afectada, quienes reciben amenazas directas para generar un impacto adicional.

Finalmente, la cuarta fase implica ataques de **denegación de servicio (DDoS)** contra la infraestructura de la víctima, aumentando la interrupción y dificultando cualquier intento de recuperación.

Operación Aether

Durante 2025, la **Guardia Civil** ha participado activamente en la **operación internacional Aether**, coordinada por EUROPOL en la que se permitió la detención de cuatro líderes del grupo de ***ransomware 8Base***, todos ciudadanos **rusos**, acusados de usar una variante de *Phobos* para extorsionar a víctimas en Europa y otros países, además de intervenir 27 servidores vinculados a la red criminal.

Esta acción se suma a arrestos previos relacionados con *Phobos*, incluido un administrador detenido en Corea del Sur en 2024 y un afiliado en Italia en 2023, lo que debilitó aún más la infraestructura del *ransomware*.

En total, en la operación participaron **fuerzas de seguridad de 14 países** con el apoyo de EUROPOL y EUROJUST, cuya labor de integración de **inteligencia** fue **clave** para golpear simultáneamente a ambos grupos de ransomware.

"Gracias a la operación, **más de 400 empresas fueron alertadas** de ataques en curso o inminentes..."

Continúan las técnicas ***Ransomware as a Service* (RaaS)**

El ecosistema de ***Ransomware as a Service (RaaS)*** ha alcanzado en 2025 un nivel de madurez que lo acerca cada vez más a la estructura de una empresa formal, pero operando en la clandestinidad.

Los grupos que desarrollan el malware funcionan como proveedores de servicios: crean el *ransomware*, mantienen la infraestructura, actualizan las variantes y ofrecen paneles de control intuitivos para que sus afiliados gestionen ataques sin necesidad de conocimientos técnicos avanzados.

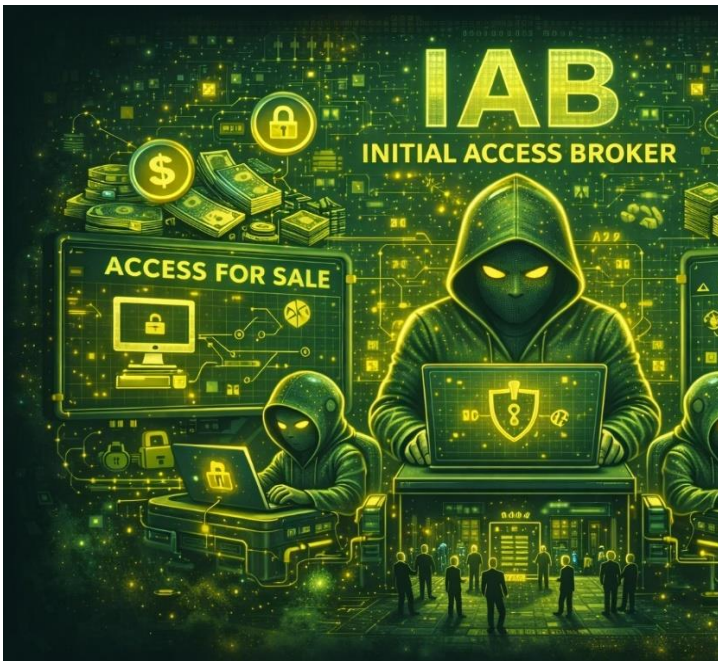
Este modelo ha permitido que actores con poca experiencia -e incluso sin habilidades técnicas- puedan ejecutar campañas complejas mediante suscripciones, comisiones o pagos por uso. Los operadores del *ransomware* proporcionan manuales, soporte técnico, herramientas de evasión, cifrado optimizado y sistemas automatizados para la filtración y publicación de datos robados. Además, muchos programas RaaS incluyen funciones de *customer support* para los propios delincuentes, así como mecanismos de reputación interna que premian a los afiliados más "eficientes".

La consecuencia directa es un **aumento significativo del volumen y la sofisticación de los ataques**, ya que el modelo *RaaS* reduce las barreras de entrada y multiplica la capacidad operativa de los grupos criminales.

31

Uso de credenciales obtenidas por *infostealers* para el acceso inicial a sistemas

En 2025, los ***infostealers*** se han convertido en una de las principales fuentes de acceso inicial para los grupos de *ransomware*, transformando por completo la fase de intrusión.



Estas familias de malware, diseñadas para robar credenciales, *cookies* de sesión, *tokens* de autenticación y datos sensibles del navegador, operan de forma **silenciosa y masiva**. Una vez recopilada la información, los **datos robados se venden** en mercados clandestinos o se distribuyen a través **de *Initial Access Brokers* (IAB)**, actores especializados en comercializar accesos a redes corporativas comprometidas.

Este modelo permite a los operadores de *ransomware* adquirir accesos legítimos y listos para usar, evitando técnicas más ruidosas como la explotación de vulnerabilidades o el phishing directo.

"Operación TALENT"

En 2025, en el marco de la **operación Talent** y como consecuencia de un macrooperativo liderado por EUROPOL en varios paises, **Guardia Civil detuvo en Valencia** a dos ciberdelincuentes implicados en la administración de los **foros internacionales de cibercrimen *Cracked* y *Nulled***. Estos foros, que reunían a más de diez millones de usuarios, facilitaban la compraventa de datos personales robados, credenciales de acceso, manuales de técnicas delictivas y servicios criminales, además de herramientas basadas en inteligencia artificial para detectar vulnerabilidades y optimizar ataques informáticos.

Los detenidos actuaban como administradores e intermediarios en transacciones ilícitas realizadas con criptomonedas, obteniendo importantes beneficios económicos sin actividad laboral conocida.

La operación permitió desmantelar ambos foros y realizar un registro domiciliario en el que se intervino abundante material informático, dinero en efectivo y criptoactivos valorados en más de 234.000 euros.

06.- USO CRIMINAL DE CRIPTOMONEDAS

“LA EXPLOSIÓN DE LAS ***STABLECOINS***”

Durante 2025 las *stablecoins* han jugado un papel fundamental en una parte importante de los delitos que involucran criptomonedas, siendo su empleo de utilidad para los criminales al tener por diseño un precio fijo, normalmente de 1 dólar estadounidense.

Las dos stablecoins de mayor uso han sido el **USDT (Tether) y el USDC (Circle).**

Operación IFADE-YUZUK

Durante el pasado año, en el marco de la operación IFADE-YUZUK **Guardia Civil logró la desarticulación de una organización criminal dedicada al blanqueo de capitales a gran escala** mediante un sistema de compensación en criptomonedas.

El grupo recibía millones de euros en efectivo de forma clandestina en España, procedentes principalmente del comercio opaco de mercancía importada desde China y de la venta de productos falsificados, desviándolos de los cauces legales y compensándolos por su equivalente en criptoactivos a cambio de comisiones del 2 al 3 %.

La red realizaba entre cuatro y seis operaciones semanales, moviendo alrededor de tres millones de euros por semana, y operaba en múltiples provincias españolas y países como Chipre, Francia y Portugal.

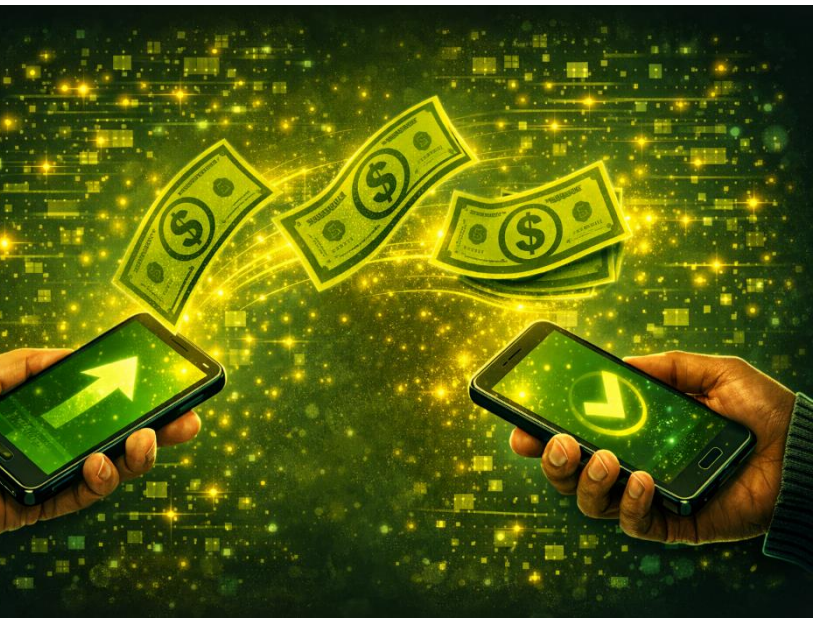
El operativo permitió intervenir más de **27 millones de euros en criptomonedas,** más de ocho millones en efectivo y el **bloqueo de 26,4 millones de USDT.** En total, se practicaron 90 registros, con 23 detenidos y 17 investigados, desmantelando una estructura compuesta por al menos 52 miembros y una amplia cartera de clientes.

PERFECCIONANDO LOS MÉTODOS DE OFUSCACIÓN

En el caso de estafas con criptomonedas, aunque se sigue utilizando con bastante frecuencia **en el inicio de la estafa Bitcoin o Ethereum**, debido a su mayor facilidad de obtención, tras realizar una primera trazabilidad se suelen detectar cambios de estas criptomonedas a stablecoins, como el USDT o USDC.

Esta modificación se pueden realizar dentro de una cuenta de un *Exchange* o utilizando alguna plataforma de tipo *swap*. Igualmente, se ha observado la utilización de puentes *(bridges)*, plataformas que introducen saltos entre diferentes *blockchains* y que, aun no estando diseñados para ello, aportan dificultades a la hora de llevar a cabo una trazabilidad forense de los fondos.

"¡TRASPASO URGENTE DE LOS FONDOS!"



En la última parte del año se ha observado un ligero cambio de tendencia en el uso de USDT, debido probablemente al aumento de los bloqueos de este tipo de criptoactivo por parte de cuerpos policiales a nivel mundial. Esto ha hecho que los **movimientos de los fondos** en USDT sean **más rápidos** por parte de las organizaciones criminales, evitando que estos se acumulen en una dirección que pudiera facilitar la acción policial.

Este hecho ha conllevado un **aumento** del **uso de USDC** en comparación con el USDT al no estar tan extendido su bloqueo actualmente.

“ACUMULANDO EL DINERO SUCIO”

Igualmente, y muy especialmente en lo relacionado con estafas con criptomonedas, se ha detectado durante las trazabilidades que en una parte importante de casos, los fondos robados acaban en **redes de blanqueo de criptomonedas.** Aquí se acumulan fondos **de diversa procedencia**, dificultando su investigación y bloqueo.

Esto complica notablemente la actividad investigadora al coexistir diferentes ilícitos penales que usan la misma red de blanqueo.

Igualmente, se sigue observando el uso de **plataformas de juego (*gambling*)** para el blanqueo de fondos ilícitos.

TIPOLOGÍAS DELICTIVAS EN **ALZA**

> "... se puede intuir que el actor principal de estos robos de fondos sea algún tipo de ***malware*** o ***infostealer*** ..."

En lo relativo a tipologías delictivas, los análisis practicados revelan un aumento de fondos robados contenidos en billeteras hardware, especialmente aquellos relacionados con ***Ledger***.

Las investigaciones intuyen que la causa principal de estos robos de fondos sean por infección de ***malware o infostealer*** en el dispositivos a los cuales se conectan los monederos hardware (llegando los fondos en muchas ocasiones a redes de mulas o *exchanges* no colaborativos). Tampoco se puede descartar la posibilidad de que los dispositivos se hubieran vulnerado incluso antes de su compra, en casos en los que la billetera hardware no hubiera sido adquirida en establecimientos de confianza.

Los análisis revelan la continuidad de estafas a través de **criptomonedas no reguladas** y no respaldadas en el mercado general.

Esta técnica consiste en la creación de una **página web que simula un proyecto de criptomoneda real,** con un *roadmap* (hoja de ruta) para dar veracidad, llegando incluso a la creación de algún **puente en la *blockchain***, todo ello añadido a la creación de perfiles en redes sociales y grupos de *Telegram* para dar más credibilidad al proyecto, ejerciendo así una potente ingeniería social incluso para usuarios con algunos conocimientos.

Estas estafas se materializan realizando una **preventa** de la **criptomoneda a precios generalmente altos**, que el mismo día de su salida oficial pierden valor al no estar respaldadas con suficiente liquidez.

En lo relativo a técnicas que faciliten la investigación por parte de los cuerpos policiales, destaca la creación de sistemas que permiten **etiquetar** direcciones de **criptomoneda** y **monitorizar su comportamiento.**

“MEDIDAS DISRUPTIVAS”

Gracias a estas capacidades, cuando los fondos asociados a una dirección previamente etiquetada acceden a un *Exchange*, estos pueden ser bloqueados de forma inmediata, lo que facilita una medida disruptiva en este tipo de contextos.

REFERENCIAS

Detención de GoogleXCoder PÁG. 9
https://web.guardiacivil.es/en/destacados/noticias/La-Guardia-Civil-desmantela-una-red-de-phishing-bancario-y-detiene-al-principal-desarrollador-de-kits-de-robo-de-credenciales-en-Espana/

https://www.eldiario.es/tecnologia/cayo-googlexcoder-hacker-kits-estafa-revelan-funciona-nuevo-cibercrimen-espana_1_12711285.html

https://www.cope.es/programas/la-linterna/audios/asi-googlexcoder-joven-25-anos-robo-numero-tarjeta-sms-tenia-35-entidades-bancarias-suplantadas-20251014_3232052.html

Operación MOSENIK PÁG. 12
https://web.guardiacivil.es/es/destacados/noticias/Desmantelada-una-red-de-infraestructura-tecnologica-que-recopilaban-datos-para-ponerlos-a-disposicion-de-ciberdelincuentes/

https://elpais.com/espana/2025-11-28/desmantelada-en-barcelona-una-red-tecnologica-que-recopilaba-datos-para-estafas-masivas.html

https://www.eleconomista.es/tecnologia/noticias/13714696/01/26/la-guardia-civil-detecta-un-nuevo-metodo-para-vaciar-cuentas-por-mensajes-suplantando-la-identidad-de-cientos-de-personas.html

Operación JACKAL PÁG. 18
https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Operacion-internacional-contra-las-redes-de-delincuencia-financiera-de-Africa-Occidental

Operación AETHER PÁG. 29
https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown

Operación TALENT PÁG. 32
https://web.guardiacivil.es/eu/destacados/noticias/Detenidos-dos-ciberdelincuentes-en-Valencia-dentro-de-un-macrooperativo-policial-de-Europol/

https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world

Operación IFADE-YUZUK PÁG. 34
https://web.guardiacivil.es/es/destacados/noticias/Intervenidos-mas-de-27-millones-de-euros-en-criptomonedas-y-mas-de-ocho-millones-en-efectivo-a-una-organizacion-criminal/

(+34) 914 538 183

dg-utecnicapj-4ctecnologico@guardiacivil.org

Guardia Civil