



Delincuencia
organizada en línea:
**cómo Europol desarticula
la ciberdelincuencia**





Europol, con sede en La Haya (Países Bajos), ayuda a los Estados miembros a prevenir y combatir todas las formas graves de delincuencia organizada e internacional, el terrorismo y la ciberdelincuencia.

La lucha contra la ciberdelincuencia es una de las máximas prioridades de la Agencia, tal como se pone de relieve en la última Evaluación de la amenaza de la delincuencia grave y organizada de la Unión Europea (SOCTA UE). En el contexto de la SOCTA UE, los siguientes ciberdelitos se consideran amenazas graves en la UE: ciberataques, tramas de fraude en línea y explotación sexual de menores (en línea).

| Europol, Delincuencia organizada en línea: cómo Europol desarticula la ciberdelincuencia.

PDF Web | ISBN 978-92-9414-072-2 | DOI-10.2813/4291295 | QL-01-25-021-ES-N

© Agencia de la Unión Europea para la Cooperación Policial, 2025


Este resumen ejecutivo se ha traducido por motivos de comodidad.
Tenga en cuenta que la versión en inglés es la referencia oficial.

Se autoriza la reproducción siempre y cuando se mencione la fuente.

Cualquier uso o reproducción de fotografías u otro material que no esté sujeto a los derechos de autor de la Agencia de la Unión Europea para la Cooperación Policial requerirá la autorización de sus titulares.

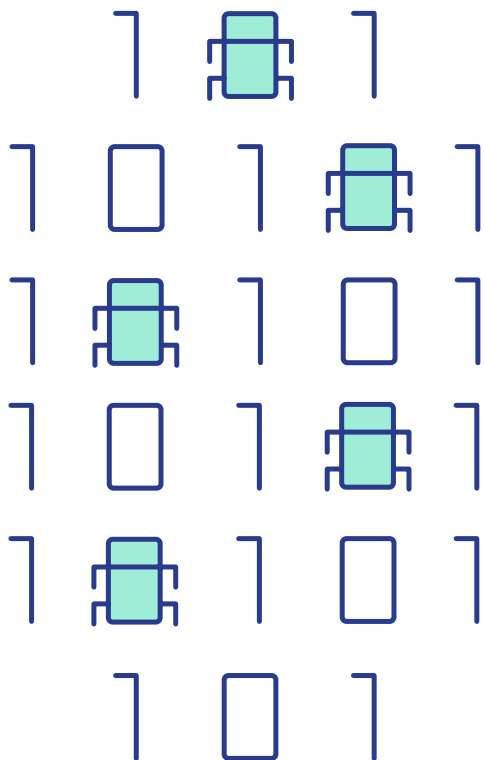
Cómo citar esta publicación: Europol, Delincuencia organizada en línea: cómo Europol desarticula la ciberdelincuencia, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2025.

El informe completo puede consultarse en el sitio web de Europol
www.europol.europa.eu

 Los **ciberataques** son delitos en línea en los que los ciberdelincuentes atacan infraestructuras críticas, administraciones, empresas y particulares. A menudo se perpetran en nombre de autores de amenazas externos, cada vez más alineados con un Estado concreto y con motivaciones ideológicas.

Tendencias principales de los ciberataques:

- **Los datos son un elemento fundamental en el panorama de las amenazas de los programas maliciosos**, porque se utilizan para consumir ataques —que sería el objetivo— y como resultado de los ataques.
- **Estos delitos los propicia la economía del delito como servicio**, que incluye foros de mercado en la web oscura en los que se venden datos robados, servicios de intrusión, y prestadores de servicios delictivos de representación y de alojamiento de datos.
- **El panorama de la ciberdelincuencia se ha fragmentado aún más**, con duraciones más cortas y la fragmentación de los mercados y los grupos dedicados a los programas de secuestro (ransomware), por lo que resulta más complicado identificar a los autores de las amenazas.



Las redes de ciberdelincuencia en el punto de mira

La operación «Eastwood» se centró en la red de ciberdelincuencia «NoName057(16)». Esta operación interna conjunta con Eurojust se llevó a cabo entre el 14 y el 17 de julio de 2025.


Las personas que actúan en nombre de NoName057(16) son principalmente simpatizantes de habla rusa que utilizan herramientas automatizadas para perpetrar ataques distribuidos de denegación de servicio (DDoS). Operan sin liderazgo formal ni habilidades técnicas sofisticadas, y sus motivaciones son la ideología y las recompensas.

Las autoridades nacionales se han puesto en contacto con varios cientos de personas que consideran simpatizantes de esta red de ciberdelincuencia. En los mensajes, enviados a través de una popular aplicación de mensajería, se informa a los destinatarios de las medidas oficiales y se hace hincapié en la responsabilidad penal que entrañan los actos que han cometido en virtud de la legislación nacional.

Hasta ahora, esta operación ha permitido desarticular una infraestructura de ataque compuesta por cien sistemas informáticos repartidos por todo el mundo, así como desconectar una parte importante de la infraestructura central de servidores del grupo.

Se puede acceder al informe íntegro de la IOCTA aquí

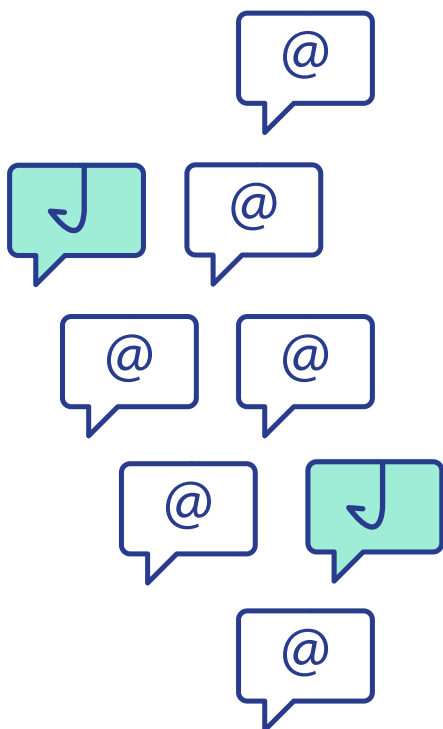


 Las **tramas de fraude en línea** constituyen uno de los sectores de más rápida expansión de la delincuencia organizada, cuyo blanco de ataque es un amplio espectro de víctimas. La magnitud del fraude en línea ha alcanzado niveles sin precedentes y se prevé que siga en auge, sobre todo debido a los avances en automatización e inteligencia artificial.

Principales tendencias de las tramas de fraude en línea:

- Las **tramas de fraude en línea** son cada vez más difíciles de detectar, ya que tienden a ser duraderas, personalizadas y muy sofisticadas.
- El **robo de datos personales de los sistemas de pago es motivo de gran preocupación**. Los datos se explotan directamente o se venden a otros delincuentes, lo que se traduce en una victimización reiterada de los objetivos.
- **Algunos defraudadores demuestran una gran destreza y desarrollan continuamente sus técnicas**, lo que amplifica los futuros riesgos debido a la capacidad de adaptación de los atacantes.

El panorama de la amenaza del fraude en línea cuenta con una industria delictiva bien organizada y sofisticada que no solo apunta a las víctimas, sino que también ofrece servicios profesionales a los delincuentes. Los defraudadores se aprovechan de las tecnologías avanzadas, de los despistes humanos y de las lagunas en la legislación.



Investigación de plataformas de phishing como servicio


Europol desempeñó un papel clave en el desmantelamiento de «LabHost», una de las mayores plataformas de phishing como servicio del mundo. Como parte de la operación, que duró un año, entre el 14 y el 17 de abril de 2024 se detectaron setenta direcciones a escala mundial, lo que resultó en la detención de treinta y siete personas sospechosas.

La plataforma «LabHost» ofrecía, por una suscripción mensual, un servicio personalizable que abarcaba desde paquetes de phishing hasta páginas de alojamiento de infraestructuras. En función de la suscripción, los delincuentes podían ampliar el alcance de sus actividades para llegar a instituciones financieras, servicios postales y proveedores de servicios de telecomunicaciones, entre otras. Esta suscripción también incluía una herramienta de campaña denominada «LabRat», que permitía a los delincuentes no cualificados supervisar y controlar los ataques en tiempo real.

Hasta ahora, esta operación ha permitido descubrir 40 000 dominios de phishing y localizar a más de 10 000 usuarios en todo el mundo. Los datos obtenidos de LabHost y LabRat se utilizarán para las actividades operativas internacionales en curso.

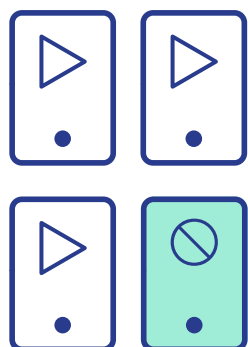
Escucha nuestro episodio de podcast sobre cómo se fomenta el crimen en línea



 La explotación sexual de menores en línea se refiere al abuso sexual de una persona menor de dieciocho años, así como a la producción y el intercambio en línea de imágenes de dicho abuso. Se trata de un delito atroz y grave, ya que implica violencia física y psicológica contra menores, algo que repercute gravemente en su salud y desarrollo.

Principales tendencias de la explotación sexual de menores:

- **La aceleración digital ha provocado una rápida evolución en la explotación sexual de menores en línea.** Ha habilitado plataformas cifradas de extremo a extremo que no conocen de fronteras para que los delincuentes creen, almacenen e intercambien material de abuso sexual de menores, así como para ponerse en contacto con las víctimas y ganarse su confianza.
- **La accesibilidad a las herramientas de IA ha transformado el panorama de la explotación sexual de menores.** Estas herramientas pueden utilizarse para editar material existente o crear nuevos contenidos, por ejemplo, haciendo que los adultos parezcan más jóvenes en imágenes explícitas o transformando las imágenes no explícitas en imágenes de desnudos.
- **Diversos grupos sacan provecho de las plataformas digitales.** Se utilizan para reclutar a delincuentes y atraer a víctimas de todo el mundo, normalizar actos de extrema crueldad, extorsionar a las víctimas, compartir material de abuso sexual de menores e incluso radicalizar a personas hacia el extremismo violento.



Lucha contra la explotación sexual de menores

La operación «Stream» (también denominada «operación Kidflix») es una de las mayores operaciones de la historia de Europol contra la explotación sexual de menores. La investigación comenzó en 2022 y culminó con semanas de trabajo, desde el 10 hasta el 23 de marzo de 2025.

Kidflix se creó en 2021 y no tardó en convertirse en una plataforma popular entre los pederastas. Según las autoridades, se subieron y compartieron 91 000 vídeos exclusivos, con una duración total de 6 288 horas. A diferencia de otras plataformas de este tipo, Kidflix permitió a los usuarios descargar material de abuso sexual de menores, pero también visualizar archivos de vídeo mediante transmisión continua. Los usuarios efectuaron pagos con criptomonedas.

Hasta la fecha, esta operación ha permitido identificar a 1 393 personas sospechosas, detener a otras 79 personas sospechosas, incautar más de 3 000 dispositivos electrónicos y proteger a 39 menores.

Para obtener más información sobre los ciberataques, las tramas de fraude en línea y la explotación sexual de menores, puede acceder a la SOCTA-UE aquí



Cambios en el panorama de la ciberdelincuencia: explotación de datos

Durante los últimos doce meses, Europol ha seguido investigando las amenazas y tendencias cambiantes en el contexto de la ciberdelincuencia. Un tema general que surgió fue el uso indebido de los datos como fuerza motriz del ecosistema delictivo, que abarca desde el fraude en línea y los programas de secuestro (ransomware) hasta la explotación sexual de menores. Este fue el tema central de la Evaluación de la amenaza de la delincuencia organizada en internet (IOCTA) de este año titulada **Steal, deal, and repeat: How cybercriminals trade and exploit your data (Robar, negociar y repetir: cómo los ciberdelincuentes venden y explotan tus datos)**.

« No se puede defender lo que no se entiende. El informe IOCTA 2025 de Europol arroja luz sobre la economía oculta de los datos robados que alimenta las ciberamenazas más peligrosas de hoy en día, proporcionando a la policía, los responsables políticos y la industria la información necesaria para actuar con determinación.»

Edvardas Šileris, jefe del Centro Europeo de Ciberdelincuencia de Europol.

Los resultados de este año revelan las siguientes tendencias principales que ilustran el modo en que los ciberdelincuentes están adaptando sus métodos y ampliando sus operaciones:

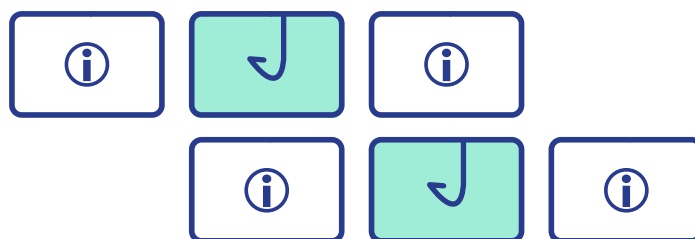
➤ **Los datos comprometidos son muy valiosos para un amplio abanico de delincuentes**, que los explotan como una mercancía por derecho propio, pero también como un objetivo que conseguir para otros fines, incluida la perpetración de nuevas actividades delictivas.

➤ **Los ciberdelincuentes utilizan diversas técnicas para acceder a los datos personales y robarlos**, para lo que se aprovechan tanto de las vulnerabilidades del sistema como de los descuidos humanos. La ingeniería social destaca como una técnica especialmente frecuente.

➤ **Los grandes modelos de lenguaje (LLM) y otras formas de inteligencia artificial generativa están mejorando la eficacia de las técnicas de ingeniería social** mediante la personalización de la comunicación con las víctimas y la automatización de los procesos delictivos.

➤ **Una parte próspera del ecosistema delictivo gira en torno a la venta del acceso a sistemas y cuentas comprometidos**. Los intermediarios de acceso inicial (IAB) anuncian cada vez más estos servicios, junto con productos relacionados, en plataformas delictivas especializadas utilizadas por un amplio espectro de ciberdelincuentes.

➤ **Los intermediarios de datos están expandiendo sus actividades a múltiples plataformas con el fin de diversificar sus operaciones y aumentar su resiliencia frente a las operaciones policiales**. Las aplicaciones de comunicación cifrada de extremo a extremo (E2EE) se utilizan cada vez más para anunciar, negociar y efectuar transacciones de venta que impliquen datos robados, así como para compartir los datos personales de las víctimas, incluidos los menores.



En el punto de mira: vectores utilizados para robar datos

Los ciberdelincuentes utilizan diversas técnicas que se aprovechan de las vulnerabilidades del sistema o de los descuidos humanos para acceder a los datos personales y robarlos. El uso de técnicas de ingeniería social es cada vez más frecuente para acceder a los datos; estos son algunos ejemplos:



Captación ilegítima de datos confidenciales (phishing)

Tipo de ataque que consiste en infectar a las víctimas con programas informáticos maliciosos o engañarlas para que introduzcan sus credenciales en sitios web fraudulentos creados mediante paquetes de phishing.



Ladrón de información (infostealer)

Categoría de programa informático malintencionado diseñado específicamente para extraer de forma ilícita información delicada de dispositivos comprometidos, que recaba credenciales de inicio de sesión, tokens de aplicaciones y cookies de sesión. Los delincuentes utilizan correos electrónicos, SMS o mensajes en redes sociales con archivos adjuntos o URL malintencionados para introducir programas informáticos malintencionados en el sistema de la víctima.



Phishing de voz (vishing)

Llamadas telefónicas fraudulentas que engañan a las víctimas para que proporcionen información delicada mediante servicios de spoofing¹, que permiten a los delincuentes hacerse pasar por entidades locales y de confianza.

Desmantelación de redes infectadas (botnets)

La operación «Endgame» forma parte de una serie de operaciones dedicadas a desarticular redes infectadas, lo que la convierte en una de las más importantes de su tipo. Comenzó en mayo de 2024 y aún está en curso.

Las botnets son redes de dispositivos infectados con programas informáticos maliciosos que permiten a los atacantes hacerse con el control remoto de los aparatos sin que los propietarios se den cuenta. Estas infecciones con programas informáticos maliciosos suelen comenzar con el uso de droppers, un tipo de software malicioso diseñado para instalar programas informáticos maliciosos adicionales en un sistema que sea el objetivo del ataque.

Durante toda la operación, Europol y el Grupo Conjunto sobre Ciberdelincuencia (J-CAT) han seguido apoyando las investigaciones facilitando el intercambio de información entre las autoridades implicadas y prestando apoyo analítico y forense a los investigadores.

La última operación «Endgame» se llevó a cabo desde el 19 hasta el 22 de mayo de 2025. Durante este período, las autoridades cerraron unos trescientos servidores en todo el mundo, neutralizaron 650 dominios y emitieron órdenes internacionales de detención contra veinte objetivos, asestando un golpe directo a la cadena de ataque basada en programas de secuestro.

1. Un servicio que permite a los usuarios hacer llamadas telefónicas con números de teléfono falsos o que cambian constantemente o enviar correos electrónicos que parecen proceder de una fuente fiable.



www.europol.europa.eu