INTERPOL

INFORME DE INTERPOL DE EVALUACIÓN DE LAS CIBERAMENAZAS EN ÁFRICA - 2024

PREPARADO POR LA OFICINA DE OPERACIONES CONTRA LA CIBERDELINCUENCIA EN ÁFRICA

3º Edición

ABRIL DE 2024

ÍNDICE

PRÓLOGO DE INTERPOL 3
PRÓLOGO DE AFRIPOL 5
ABREVIATURAS Y ACRÓNIMOS 7
AGRADECIMIENTOS 8
RESUMEN 9
1 Introducción 10
2 Tendencias en el panorama africano de las ciberamenazas: 2023 11
3 Ransomware y extorsión en línea 13
4. Estafas en línea 16
5. Estafas a empresas por e-mail mediante suplantación de identidad (estafas BEC) 22
6. Ciberresiliencia y capacidades policiales en el continente africano 26
7. Próximas medidas 30
ACERCA DE INTERPOL 33

PRÓLOGO DE INTERPOL

En el mundo actual, la tecnología no es solo una comodidad, sino la base de nuestra vida cotidiana. Internet, piedra angular de esta era tecnológica, es vital para gestionar infraestructuras críticas, llevar a cabo transacciones financieras seguras, mantener la comunicación con los seres queridos, disfrutar comprando en línea y acceder a una gran cantidad de información y entretenimiento. Su capacidad para salvar grandes distancias y facilitar el acceso inmediato a datos y experiencias virtuales hace que resulte indispensable para todos nosotros.

No obstante, la era digital plantea sus propios retos, principalmente la amenaza creciente de la ciberdelincuencia. A medida que avanza la tecnología, también lo hacen las tácticas utilizadas por los ciberdelincuentes, que recurren a métodos cada vez más sofisticados para aprovecharse de vulnerabilidades, lo que supone un riesgo importante, tanto para las personas como para las organizaciones. Las víctimas suelen quedar en la indigencia económica, psicológica y emocional. Al mismo tiempo, el panorama de las amenazas se ve exacerbado por acontecimientos sociales, económicos y políticos más amplios, como la creciente desigualdad entre la capacidad de ciberresiliencia de países, organizaciones y personas. Todas estas circunstancias son aprovechadas por los ciberdelincuentes a escala nacional, regional y mundial, dejando tras de sí una lista interminable de víctimas.

A medida que nos adentramos en 2024, resulta más evidente la importancia de aplicar estrategias integrales de ciberseguridad. Las entidades grandes y pequeñas deben protegerse contra una amplia gama de ciberamenazas, desde los ataques convencionales hasta las nuevas amenazas más sofisticadas.

Durante los últimos nueve años, INTERPOL ha dirigido un programa internacional cohesionado y coherente en materia de ciberdelincuencia, respaldado por su Estrategia Mundial contra la Ciberdelincuencia, cuyo objetivo es reducir la repercusión mundial de la ciberdelincuencia y proteger a las comunidades para lograr un mundo más seguro. INTERPOL coordina y apoya a sus 196 países miembros mediante actividades que previenen, detectan, investigan o neutralizan los ciberdelitos que causan grandes daños y tienen una gran repercusión, o bien que son muy frecuentes o de gran interés en las comunidades que ayudamos a proteger. Es algo que se lleva a cabo a través de un marco tripartito que proporciona apoyo a los países miembros en los ámbitos del intercambio de información, la coordinación operativa y desarrollo estratégico y de capacidades.

En este contexto, INTERPOL ha introducido un enfoque regional de apoyo a través de las Oficinas Regionales de Operaciones contra la Ciberdelincuencia. La Oficina de Operaciones Conjuntas contra la Ciberdelincuencia en África (AFJOC), financiada por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido, es un ejemplo de este tipo de iniciativas. Está especializada en la recopilación y el análisis de información sobre actividades de ciberdelincuencia; en la realización de actuaciones policiales coordinadas basadas en datos de información policial y, en general, en el fomento de la cooperación y las buenas prácticas entre los países miembros africanos, así como en la creación de acuerdos de cooperación con otras partes interesadas, tanto públicas como privadas.

Teniendo todo esto en cuenta, tengo el privilegio de presentar la última edición del informe de evaluación de las ciberamenazas en África. Esta evaluación proporciona un análisis exhaustivo del panorama de las ciberamenazas en el continente africano y examina más en detalle el ransomware, las estafas a empresas por e-mail mediante suplantación de identidad (BEC) y otras formas de estafas en línea. No se limita a destacar estas ciberamenazas, sino que también examina los esfuerzos nacionales constantes para mejorar la ciberresiliencia. El informe concluye con recomendaciones estratégicas para allanar el camino hacia el futuro.

A lo largo de este análisis se muestra la necesidad imperiosa de cooperación internacional y regional entre los organismos encargados de la aplicación de la ley frente a las actividades de los ciberdelincuentes. Un enfoque unificado mejora la capacidad de hacer frente a las amenazas con eficacia, permitiendo el intercambio de información policial, compartiendo prácticas de investigación y haciendo uso de tecnologías avanzadas.

Las intervenciones policiales siempre tendrán un nivel local y siempre serán parte integral de nuestras comunidades. No obstante, delitos como los cibernéticos tienen una repercusión mundial e implican un volumen, una escala y una complejidad que pueden suponer un reto para todos. Tenemos la responsabilidad colectiva de prevenir, detectar, investigar y neutralizar a los delincuentes y grupos que están detrás de estos delitos. Los particulares y las empresas que se conectan a Internet deben hacerlo con mayor seguridad.

En este panorama tan complejo, ningún actor puede por sí solo garantizar nuestra seguridad colectiva. Consciente de ello, INTERPOL actúa como interlocutor neutral y de confianza, fomentando la colaboración entre los organismos encargados de la aplicación de la ley y los sectores público y privado. Mediante la combinación de esfuerzos y el intercambio de conocimientos especializados, INTERPOL pretende reforzar nuestras defensas colectivas contra las ciberamenazas, haciendo hincapié en la responsabilidad que compartimos para proteger nuestro mundo digital.

Para concluir, me gustaría expresar mi gratitud a nuestros países miembros de la región africana y a nuestros socios, por su apoyo inquebrantable y su dedicación a esta causa, así como por su contribución en la elaboración de esta evaluación. Sus esfuerzos incesantes y su compromiso son fundamentales para avanzar en nuestro objetivo común de un entorno digital más seguro para todos.

Craig Jones
Dirección de Ciberdelincuencia
INTERPOL

PRÓLOGO DE AFRIPOL

Mientras reflexionamos sobre el año pasado y miramos hacia el futuro, el panorama de las ciberamenazas en África (y, de hecho, en todo el mundo) sigue evolucionando para hacerse cada vez más complejo. El camino recorrido desde finales de los años 1990, cuando el acceso a Internet en África era un lujo que pocos se podían permitir, hasta la fecha, con el gran auge de la conectividad, ilustra una trayectoria notable de avances tecnológicos. Sin embargo, esta evolución no deja de plantear retos. La proliferación de ciberamenazas se ha intensificado, llegando a todos los rincones de nuestro continente y afectando por igual a particulares, gobiernos e industria.

El año 2023 ha sido fundamental para dar forma a nuestra respuesta ante nuevas amenazas. Partiendo de las conquistas de años anteriores, la lucha contra la ciberdelincuencia ha avanzado considerablemente. Nuestra colaboración con INTERPOL nunca ha sido tan estrecha y está marcada por iniciativas innovadoras y el despliegue de tecnologías avanzadas destinadas a reforzar nuestras ciberdefensas. La creación del centro de datos y las bases de datos policiales de AFRIPOL, así como la inauguración de la unidad de Análisis de la Información Policial son hitos fundamentales en nuestro proceso hacia un entorno cibernético más seguro en África.

La puesta en marcha del curso de formación de AFRIPOL sobre investigación de la ciberdelincuencia es una prueba de nuestro compromiso en el desarrollo de capacidades en el continente. La expansión de estos programas para incluir módulos avanzados sobre amenazas contra la ciberseguridad y estrategias de respuesta han enriquecido el arsenal que podemos utilizar contra los ciberdelincuentes. El compromiso de los Estados miembros ha sido abrumadoramente positivo, con un aumento vertiginoso de las cifras de participación y una notable mejora de las competencias de nuestro personal de ciberseguridad.

En 2023, nuestras alianzas se han desarrollado más allá de nuestros aliados tradicionales, para incluir gigantes tecnológicos e instituciones académicas. Esta colaboración nos ha permitido aprovechar la investigación y la tecnología más avanzadas, mejorando nuestra capacidad de adaptación al cambiante panorama tecnológico. Nuestro enfoque también se ha ampliado para abordar el impacto socioeconómico de las ciberamenazas, conscientes de que la ciberseguridad no es un mero reto técnico, sino la piedra angular de nuestra estabilidad y nuestro crecimiento económicos. África tiene una economía digital floreciente y proteger este sector vital es primordial para nuestro desarrollo sostenible.

De cara a 2024, AFRIPOL se ha comprometido a multiplicar sus esfuerzos en cuatro frentes estratégicos:
1. Conscientes de la naturaleza transfronteriza de las ciberamenazas, nos proponemos reforzar nuestra red de cooperación en todo el continente y con nuestros socios mundiales. Para ello, deseamos compartir información policial, operaciones conjuntas y armonizar los marcos jurídicos para garantizar un frente unificado contra la ciberdelincuencia. También estamos reforzando la colaboración con el sector privado a fin de armonizar y normalizar los procedimientos y las tecnologías, a través de recopilación de información policial por todo el continente.

A comienzos de 2024, AFRIPOL firmó un memorando de entendimiento con Group IB, líder mundial en ciberseguridad. Este acuerdo mejorará el intercambio de información policial y dotará a los Estados miembros de la Unión Africana de tecnología punta y de conocimientos especializados en áreas críticas como ciberinvestigaciones, ingeniería inversa y gestión de incidentes. Gracias a estas herramientas y conocimientos avanzados, AFRIPOL reforzará su capacidad de protección contra las ciberamenazas en el continente. Además, AFRIPOL tiene previsto firmar un acuerdo con Kaspersky, un socio privado estratégico.
2. Un elemento clave de nuestra estrategia consiste en formar un grupo operativo para compartir información sobre incidentes de ciberdelincuencia y prestar el apoyo necesario a la investigación. Nos dedicamos a suministrar a nuestros Estados miembros los equipos y el software esenciales para la investigación de la ciberdelincuencia, junto con formación especializada sobre estas herramientas. Algunos ejemplos de nuestras iniciativas son la 3ª Operación Conjunta INTERPOL-AFRIPOL contra la Ciberdelincuencia, conocida como Africa Cyber Surge 3, nuestra formación especializada sobre activos virtuales, y el suministro de herramientas de investigación cruciales conjuntamente con INTERPOL, todo lo cual pone de relieve nuestro compromiso inquebrantable de reforzar nuestras capacidades de ciberdefensa en todo el continente.

3. Seguiremos explorando e integrando tecnologías emergentes como la inteligencia artificial y el blockchain para mejorar nuestras capacidades de ciberdefensa. Estas tecnologías ofrecen vías prometedoras para el análisis predictivo de amenazas, la gestión segura de los datos y la asignación eficiente de recursos. Además, estamos adoptando tecnologías de código abierto a través de nuestros programas de formación, lo que demuestra nuestro compromiso de superar los retos financieros asociados a los costosos derechos de licencia.
4. Nos centramos cada vez más en la implicación de la comunidad y tenemos previsto lanzar campañas globales de ciberconcienciación dirigidas a grupos de población vulnerables, como los jóvenes y las pymes. Educar a estos grupos demográficos clave en prácticas de ciberhigiene es un elemento fundamental para mitigar el riesgo de ciberamenazas a nivel básico.

El camino que tenemos por delante está plagado de retos, pero mantenemos una determinación inquebrantable. A medida que avanzamos hacia 2024, nuestra perspectiva es cada vez más clara: crear un continente africano seguro y resiliente en el que la tecnología sirva de faro de progreso, no de vector de vulnerabilidad. Todos juntos, con el apoyo inquebrantable de nuestros socios y los esfuerzos colectivos de nuestros Estados miembros, estamos preparados para hacer realidad esta perspectiva. Acojamos este viaje con determinación y optimismo, ya que la seguridad de nuestro ciberespacio es la piedra angular de nuestra prosperidad compartida.
.

Embajador Jalel CHELBA
Director ejecutivo en funciones, AFRIPOL

ABREVIATURAS Y ACRÓNIMOS

AFJOC	African Joint Operation against Cybercrime (Operaciones Conjuntas contra la Ciberdelincuencia en África)
IA	Inteligencia artificial
BEC	Estafa "business e-mail compromise" o BEC (estafa a empresas por e-mail mediante suplantación de la identidad).
BPH	Bulletproof Hosting (servicios de alojamiento blindado frente a las denuncias por actividades ilícitas)
CaaS	Crime-as-a-Service (ciberdelincuencia como servicio)
CCP - Operation	Plataforma Colaborativa sobre Ciberdelincuencia- Operaciones
CERT	Computer Emergency Response Teams (equipos de respuesta a emergencias informáticas)
CSIRT	Equipo de respuesta a incidentes de seguridad informáticos
CKE	Intercambio de Conocimientos sobre la Ciberdelincuencia
DDoS	Distributed Denial-of-Service (denegación de servicio distribuida)
GLACY+	Acción mundial ampliada contra la ciberdelincuencia (actualmente GLACY-e)
IP	Internet Protocol (protocolo de Internet)
ISPA	Programa de INTERPOL de apoyo a la Unión Africana en relación con AFRIPOL,
LLM	Large Language Models (grandes modelos de lenguaje)
MFA	Autenticación multifactor
PII	Información personal identificable
RAT	Remote Access Trojan (troyano de acceso remoto)
RD	Remote Desktop Protocol (protocolo de escritorio remoto)
PYMES	Pequeñas y medianas empresas

AGRADECIMIENTOS

El presente informe de evaluación ha sido redactado por la Oficina de Operaciones contra la Ciberdelincuencia en África, bajo la égida de Operaciones Conjuntas contra la Ciberdelincuencia en África (AFJOC), y financiado por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido. El Programa de apoyo de Interpol a la Unión Africana (ISPA) también ha contribuido a la elaboración de este informe, con el apoyo del Ministerio Federal de Asuntos Exteriores de Alemania.

Este informe se fundamenta en evaluaciones de información proporcionadas a INTERPOL por los países miembros pertinentes y por socios privados de INTERPOL como Bi.Zone, Fortinet, Group-IB, Kaspersky Lab y Trend Micro.

RESUMEN

En este informe se presenta el análisis de INTERPOL sobre las principales ciberamenazas que afectan al continente africano, sobre la base de información interna, reflexiones operativas, resultados de encuestas y contribuciones de socios del sector privado.

Las principales conclusiones del informe subrayan la escalada de la ciberdelincuencia en todo el continente, con el ransomware, las estafas a empresas por e-mail y otras formas de estafas en línea que se van imponiendo como las amenazas de más rápida expansión en 2023. En particular, el ransomware se ha identificado como una amenaza emergente crítica que se dirige con frecuencia contra infraestructuras esenciales, mientras que las estafas en línea siguen siendo la forma más común de delincuencia digital contra particulares y empresas, con volúmenes e implicaciones financieras de gran envergadura. El informe también señala la rápida evolución de los actores de las amenazas y de su modus operandi, incluida la creciente explotación de las redes sociales, el uso de inteligencia artificial y las técnicas avanzadas en ingeniería social.

El documento arroja luz sobre los esfuerzos nacionales africanos para hacer frente a la ciberdelincuencia, centrándose en el desarrollo legislativo, la mejora de la capacidad policial, el fomento de la cooperación y el compromiso de los poderes públicos. Aunque los países miembros han dado pasos importantes para reforzar sus ciberdefensas y mejorar la respuesta de las fuerzas del orden, todavía quedan diversos obstáculos para lograr un enfoque global, coordinado y sostenible de la lucha contra la ciberdelincuencia en todo el continente.

El compromiso de INTERPOL con África en materia de lucha contra la ciberdelincuencia, así como la ayuda que presta en este ámbito, son patentes en todo el informe. Es algo que se lleva a cabo principalmente a través de un enfoque regional especializado dirigido por la Oficina de Operaciones contra la Ciberdelincuencia en África y ejecutado a través del proyecto de Operaciones Conjuntas contra la Ciberdelincuencia en África, financiado por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido. Esta iniciativa se complementa con otras actividades importantes, entre ellas las llevadas a cabo por el programa de apoyo de INTERPOL a la Unión Africana y la acción mundial ampliada contra la ciberdelincuencia.

El informe concluye con recomendaciones estratégicas de INTERPOL, sobre todo, cómo moverse en el panorama africano de las ciberamenazas y cómo reforzar la ciberseguridad en todo el continente. Entre las recomendaciones figuran la adopción o mejora de medidas de ciberseguridad globales, la inversión en cibercapacidades policiales (personas, procesos y tecnologías), la creación de sinergias dentro del ecosistema de la ciberseguridad, la sensibilización de la ciudadanía y el refuerzo de la cooperación internacional y regional.

INTRODUCCIÓN

Los países africanos están experimentando una notable transformación digital. A pesar de los constantes retos en cobertura, acceso y calidad de las infraestructuras, el número de usuarios de Internet sigue aumentando en todo el continente, con más de 160 millones de personas que accedieron regularmente al ciberespacio entre 2019 y 2022[1]. El impacto de la digitalización es evidente en numerosos sectores, desde las infraestructuras críticas hasta la banca y el comercio electrónico. Esta tendencia también se incorpora a numerosos aspectos de la vida cotidiana de los ciudadanos africanos, desde el rápido aumento del número de pagos digitales hasta la creciente cantidad de tiempo en línea, especialmente en las plataformas de las redes sociales. A nivel individual, el acceso creciente a Internet se ve facilitado en particular por la adopción generalizada de teléfonos móviles, con más de 650 millones de africanos que utilizan estos dispositivos como principal medio de acceso a Internet.

La revolución digital está afectando especialmente a los jóvenes africanos, que representan más del 60 % de la población del continente[2]. El recurso a Internet es cada vez mayor, a menudo a través del teléfono móvil, para comunicarse, trabajar, transferir dinero, comprar y expresar la creatividad. A medida que los jóvenes africanos adoptan rápidamente las tecnologías digitales, contribuyen al desarrollo de una sociedad joven y cibernética. Los países ganan así increíbles oportunidades de crecimiento constante e innovación, pero también deben hacer frente a nuevos retos y vulnerabilidades en materia de ciberseguridad.

El aumento del número de africanos que se conectan a Internet, la creciente dependencia tecnológica de las economías y las sociedades y la llegada de los llamados "nativos digitales" están ampliando de forma inevitable la superficie de ataque para los ciberdelincuentes. Como consecuencia, la ciberdelincuencia está aumentando en toda África y es una de las amenazas emergentes más rápidas en todo el continente. El primer Informe de INTERPOL de Evaluación de las Ciberamenazas en África (2021) estimaba que el impacto financiero de la ciberdelincuencia en la región superaba los 4 000 millones de dólares estadounidenses, lo que equivale aproximadamente al 10 % del producto interior bruto total de África[3]. Desde entonces, el reto al que se enfrentan los 54 países africanos miembros de INTERPOL no ha hecho más que aumentar en volumen, repercusiones y complejidad.

Cada vez es más urgente abordar la escasa alfabetización digital, la inadecuada preparación cibernética y la falta general de buenas prácticas de ciberhigiene. Afortunadamente, los países africanos han dado pasos importantes en 2023 para construir economías digitales más seguras y proteger a sus comunidades en línea. INTERPOL se ha comprometido a ayudar a sus países miembros a cumplir estos objetivos. Reconociendo la increíble diversidad del continente africano, que incluye una gran variedad de culturas, idiomas y condiciones económicas, los proyectos y programas clave como la Operación Conjunta contra la Ciberdelincuencia en África (AFJOC) y el Programa de INTERPOL de apoyo a la Unión Africana en relación con AFRIPOL (ISPA) llevan a cabo actividades fundamentales adaptadas a las necesidades de los diferentes organismos encargados de la aplicación de la ley.

1 Banco Mundial (2024): https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

2 Foro Económico Mundial (2023): https://www.weforum.org/agenda/2022/09/why-africa-youth-key-development-potential

3 Investigación de una empresa keniana de ciberseguridad informática. Serianu: https://phys.org/news/2021- 05-rights-group-tool-stem-cybercrime.html

TENDENCIAS EN EL PANORAMA AFRICANO DE LAS CIBERAMENAZAS: 2023

En 2023, el panorama africano de las ciberamenazas seguía siendo muy dinámico, con ataques que evolucionaban rápidamente en términos de sofisticación y escala. Sobre la base de la información policial y los datos operativos procedentes de las actividades regionales de INTERPOL, complementados con los resultados de un cuestionario distribuido a los países miembros africanos y la información facilitada por los socios del sector privado, INTERPOL ha identificado las siguientes amenazas y tendencias clave:

El volumen y el impacto de la ciberdelincuencia siguen aumentando en África

- El número de ciberataques sigue aumentando en todo el continente africano, como han puesto de relieve los países miembros de INTERPOL[4].
- Más de dos tercios de los encuestados consideraron que los delitos dependientes y facilitados por Internet representaban un riesgo de medio a alto en su jurisdicción. En particular, los países señalaron un aumento del impacto financiero y social de estos delitos.
- En una ilustración más del rápido crecimiento de la ciberdelincuencia, se estima que en 2023 se produjo un aumento interanual del 23 % en el número medio de ciberataques por organización en África. Se trata de la media más alta del mundo[5].

El ransomware, la estafa a empresas por e-mail y otras estafas en línea fueron las ciberamenazas que más crecieron en 2023

- En ediciones anteriores del Informe de INTERPOL de Evaluación de las Ciberamenazas en África se señalaron las siguientes ciberamenazas más destacadas: ataques con malware, incluido el ransomware, troyanos bancarios y robos; phishing y estafas en línea, como la estafa BEC, así como el crimeware como servicio, por ejemplo programas espía y kits de phishing. Estas amenazas siguen repercutiendo en el panorama cibernético africano, causando importantes perjuicios a comunidades de todo el continente.
- En 2023, las principales ciberamenazas identificadas por los países miembros africanos fueron el ransomware, las estafas BEC y otras estafas en línea.
- El ransomware se destacó como una de las amenazas emergentes más graves en el continente, a menudo dirigida contra infraestructuras críticas, mientras que las estafas en línea siguen siendo la principal forma de delincuencia digital que afecta a los particulares y organizaciones, en términos de volumen y de impacto financiero.

Los actores de las amenazas y sus modus operandi evolucionan rápidamente: desde técnicas de ingeniería social más sofisticadas hasta el uso creciente de las redes sociales y la inteligencia artificial

- Los ciberdelincuentes que operan en y desde África siguen explotando vulnerabilidades humanas como principal método de ataque. Utilizan técnicas de ingeniería social cada vez más sofisticadas para atacar a organizaciones y particulares.
- El phishing por correo electrónico sigue siendo uno de los principales vectores de ataque inicial en una gran variedad de ciberdelitos, incluido el ransomware y muchas formas de estafa en línea. Además, los delincuentes explotan cada vez más los distintos canales de comunicación, incluidas las redes sociales y las aplicaciones de mensajería instantánea, en consonancia con las tendencias tecnológicas y sociales de la región.
- Los agresores incorporan a su modus operandi los avances tecnológicos. Algunos ejemplos destacados son el creciente uso del robo de datos como forma de extorsión, así como el creciente uso indebido de la inteligencia artificial.

4 Esta información se basa en la autodeclaración de los países miembros africanos. Cabe señalar que las definiciones de los ciberdelitos pueden variar según las jurisdicciones.

5 Checkpoint (2023): https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

En respuesta a la amenaza cada vez mayor que representa la ciberdelincuencia, los países miembros africanos han tomado medidas importantes para mejorar su capacidad de reacción y de aplicación ley en este ámbito

- Han aumentado las detenciones, actuaciones e investigaciones, a lo que ha contribuido la ampliación de los recursos contra la ciberdelincuencia. Por ejemplo, 19 países miembros destacaron un total acumulado de 10 490 detenciones relacionadas con la ciberdelincuencia de enero a diciembre de 2023. Teniendo en cuenta que estos países representan solo el 35 % del continente, el número total de detenciones por ciberdelitos será probablemente mucho mayor.
- En los últimos dos años, una docena de países africanos han adoptado o están en proceso de adoptar nueva legislación relacionada con la ciberdelincuencia. Esto supone un paso proactivo hacia el fortalecimiento de los marcos jurídicos de lucha contra la ciberdelincuencia.
- También se ha registrado un aumento sustancial de la inversión en la lucha contra la ciberdelincuencia en el continente, tanto por parte de los países miembros africanos como de las partes interesadas de fuera de la región. En 2023, más países crearon unidades especializadas en ciberdelincuencia, casi la mitad aumentaron su dotación de personal y más del 60 % informaron de que estaban participando en iniciativas de desarrollo de capacidades. Además, se dieron más de 130 iniciativas de formación, así como más de 40 campañas de concienciación pública en el continente.

Sin embargo, se siguen dando importantes retos en materia de prevención, detección, investigación y desarticulación de la ciberdelincuencia en toda África

- Las carencias persistentes en la denuncia de ciberdelitos dificulta la capacidad de actuación de las fuerzas del orden. En algunos países, este reto se ve agravado por la ausencia de plataformas de información y registro especializadas o fáciles de usar.
- A pesar de algunos avances, la colaboración entre las fuerzas del orden y otras partes interesadas fundamentales (lo que incluye el sector privado y los organismos que se ocupan de la ciberseguridad) sigue siendo un reto en algunas jurisdicciones.
- Una ciberhigiene insuficiente sigue socavando la ciberresiliencia en todo el continente, ya que muchas organizaciones e individuos africanos siguen teniendo bajos niveles de preparación contra los ciberataques.

En las siguientes secciones se ofrece un análisis más detallado de las tendencias relativas a las principales ciberamenazas identificadas por los países miembros de INTERPOL en África: ransomware, estafas en línea y estafa a empresas por e-mail mediante suplantación de identidad

RANSOMWARE Y EXTORSIÓN EN LÍNEA

Puntos clave:

- El ransomware y la extorsión en línea van en aumento: más de la mitad de los países africanos miembros de INTERPOL han informado de ataques contra sus infraestructuras críticas.
- Los correos electrónicos de phishing siguen siendo el vector más común para los ataques de ransomware en África, mientras que los métodos de extorsión y los modelos de negocio utilizados por los ciberdelincuentes siguen evolucionando.
- En general, los países miembros africanos han tomado medidas positivas para mejorar su resiliencia frente a los ataques de ransomware, pero persisten los problemas, sobre todo en lo que se refiere a la denuncia de los ataques y el pago de los rescates.

El ransomware y la extorsión en línea aumentan en África

Los países miembros de INTERPOL han señalado que el ransomware y la extorsión en línea son una de las amenazas más graves a las que se enfrenta el continente africano. Estos ataques son especialmente preocupantes debido a su elevado impacto financiero, su capacidad para perturbar gravemente las infraestructuras críticas y los servicios esenciales y el daño que pueden causar a las organizaciones y personas afectadas. La magnitud del reto es evidente: según la empresa de ciberseguridad Chainalysis, los pagos de rescates por ransomware superaron los mil millones de dólares estadounidenses en 2023[6].

El volumen, la frecuencia y el impacto de los ataques de ransomware siguen creciendo en África. Una investigación de la empresa de ciberseguridad Check Point sugiere que, de media, una de cada quince organizaciones en África sufrió un intento de ransomware cada semana durante el primer trimestre de 2023. Esta cifra es incluso superior a la media semanal mundial, que se situaba en torno a una de cada 31 organizaciones[7]. Según los informes, durante una sola semana de febrero de 2023, el socio privado de INTERPOL Kaspersky detectó más de 300 casos de ransomware en Sudáfrica, cifra que ilustra la frecuencia creciente de los ataques[8]. El impacto financiero de los ataques también parece ir en aumento: según IBM, el coste medio de un ataque de ransomware en 2023 fue de 5,13 millones de dólares, lo que supone un aumento del 13 % respecto a 2022[9].

Ataque a las infraestructuras críticas africanas

Es preocupante que cerca de la mitad de los países africanos encuestados hayan informado de ataques de ransomware contra sus infraestructuras críticas entre enero de 2023 y diciembre de 2023. Se incluyen ataques dirigidos contra infraestructuras gubernamentales, hospitales, instituciones financieras y proveedores de servicios de Internet. Por citar algunos ejemplos, en los últimos años han sufrido ataques de ransomware la mayor comercializadora de electricidad de Ghana, la Electricity Company of Ghana (ECG), los bancos nacionales de Zambia y Sudán del Sur, instituciones gubernamentales de Etiopía, Senegal y Zimbabue y el proveedor sudafricano de servicios de Internet RSAWEB. Incluso la Unión Africana se ha enfrentado a un ataque paralizante del grupo BlackCat (conocido también como ALPHV) contra su intranet en 2023, que INTERPOL y sus socios fueron capaces de mitigar[10]. El ataque contra infraestructuras críticas es especialmente alarmante, ya que la transformación digital se sigue acelerando en todo el continente y los sistemas esenciales están cada vez más interconectados.

Además de las infraestructuras críticas, los países miembros africanos también han denunciado ataques de ransomware en diversos sectores. Por ejemplo, se ha denunciado un número significativo de ataques contra empresas de los sectores financiero, manufacturero y minorista. Según la empresa de seguridad informática Sophos, el 78 % de las empresas de Sudáfrica sufrieron ataques de ransomware en 2023[11]. Entre los ataques que más repercusión han tenido figuran los perpetrados contra la sede de Porsche South Africa en Johannesburgo y contra la división sudafricana de la agencia de crédito internacional TransUnion. Estas tendencias son acordes con la evolución mundial. Según los datos agregados proporcionados por los socios de INTERPOL del sector privado, aunque la banca, la administración pública, el comercio minorista y los sectores tecnológico y sanitario fueron objetivo preferente a escala mundial, ningún sector, institución u organización es inmune a los ataques de ransomware.

6 Chainalysis (2024) : https://www.chainalysis.com/blog/ransomware-2024/

7 Checkpoint (2023): https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

8 News24 (2023): https://www.news24.com/fin24/companies/rsaweb-victim-of-cyberattack-as-wave-of-ransomware-attempts-hits-sa-in-past-week-20230206

9 IBM (2023) : https://www.ibm.com/reports/data-breach

10 Le Monde (2023): https://www.lemonde.fr/afrique/article/2023/04/25/vent-de-panique-a-l-union-africaine-apres-une-nouvelle-cyberattaque_6170976_3212.html

11 Sophos (2023): https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

Explotación persistente del factor humano

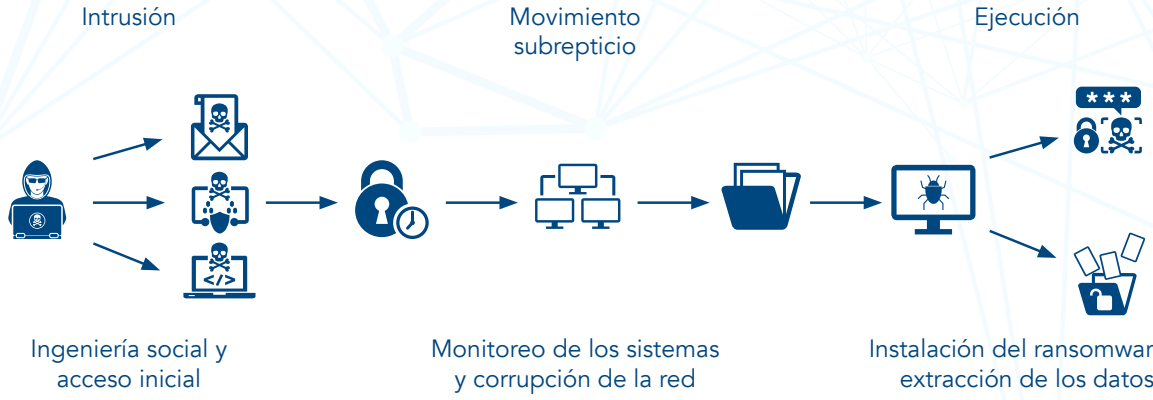
En términos de modus operandi, **los correos electrónicos de phishing parecen ser el vector de cebo más común** para los ataques de ransomware en África, **de modo que cerca de la mitad de los países africanos miembros de INTERPOL han notificado casos de phishing en este tipo de ataques.** Estos correos electrónicos suelen contener un archivo o URL maligno, diseñados para facilitar el acceso a un sistema por parte de un ciberdelincuente o para instalar de forma inmediata el malware en el momento de hacer clic en ellos. Otros métodos comunes de infección utilizados por los grupos de ransomware en la región africana incluyen el recurso a conexiones de protocolo de escritorio remoto (RDP) no seguras o a otras vulnerabilidades. Estas tendencias regionales coinciden con las conclusiones a escala mundial de Trend Micro, socio privado de INTERPOL[12]. Según la empresa de ciberseguridad, los vectores de ataque iniciales más utilizados por los grupos de ransomware en todo el mundo son el correo electrónico, la web y las aplicaciones web, los programas malignos como falsas aplicaciones móviles y la explotación de vulnerabilidades del sistema, como conexiones RDP no seguras.

Para mejorar la prevención, la detección y la mitigación, es fundamental comprender cómo los autores de las amenazas obtienen el acceso inicial para instalar el ransomware. En particular, la mayor parte de los vectores de ataque explotan fallos humanos, ya sea un usuario que hace clic en una URL maligna o un informático que no actualiza o parchea regularmente sus sistemas. De hecho, las investigaciones de la empresa de ciberseguridad Fortinet, colaboradora de INTERPOL Gateway, indican que muchos grupos de ransomware dedican más tiempo a seleccionar e investigar sus objetivos[13]. Aprovechan la información de cuentas personales en redes sociales, sitios web de empresas, páginas web de conferencias y filtraciones previas de datos para llevar a cabo ataques de ingeniería social más eficaces y para obtener un acceso inicial a los sistemas que les permita instalar el ransomware.

Evolución de las tácticas de extorsión digital

Una vez que los autores de las amenazas de ransomware han obtenido el acceso inicial, lo primero suele ser trazar un mapa de la infraestructura de red de su objetivo y desplazarse subrepticiamente por el sistema aprovechando vulnerabilidades y aumentando sus privilegios. A continuación, instalan un malware que cifra los datos de su objetivo y exigen un rescate a sus víctimas a cambio de devolverles los archivos. Para aumentar la presión sobre los objetivos, muchos grupos utilizan scareware o tácticas de extorsión adicionales. Por ejemplo, los atacantes pueden extraer datos antes de cifrarlos para amenazar con filtrar información sensible (doble extorsión), utilizar ataques de interrupción de servicio para bloquear a los objetivos que se resisten a pagar (triple extorsión) e incluso amenazar a terceros asociados de su víctima principal para aumentar la presión (cuádruple extorsión).

Sin embargo, en los últimos años, INTERPOL ha detectado el uso creciente de la extracción de datos con fines de extorsión digital. Tras la intrusión inicial en el sistema de su víctima, algunos grupos de ransomware prefieren ahora prescindir de la fase de cifrado y simplemente extraer los datos sensibles. Luego amenazan con filtrar esa información a menos que sus víctimas paguen un rescate. Debido a los posibles daños financieros, reputacionales y psicológicos que puede causar esa filtración, muchas organizaciones parecen más dispuestas a pagar. Los rescates pueden alcanzar varios millones de dólares, a pesar de que no hay garantías de que los atacantes eliminen realmente los datos robados. A causa de su potencial lucrativo, la extracción de datos está emergiendo rápidamente como un modo de actuación fundamental, tanto sustituyendo a la encriptación como en asociación con ella, lo que transforma el ransomware y la extorsión digital.



Esquema general de un ataque típico de ransomware y extracción de datos

12 Trend Micro (2023): https://newsroom.trendmicro.com/2022-08-31-Trend-Micro-Warns-of-75-Surge-in-Ransomware-Attacks-on-Linux-as-Systems-Adoptions-Soared

13 Fortinet (2023): https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

Programas de afiliación y crecimiento del ecosistema de servicios de ciberdelincuencia

Además de la evolución del modus operandi, el creciente impacto del ransomware puede atribuirse en parte al auge de los nuevos modelos organizativos que emplean los ciberdelincuentes. INTERPOL y sus socios han detectado que muchos grupos de ransomware gestionan actualmente elaborados programas de afiliación que incluyen plataformas que ofrecen ransomware como servicio a terceros delincuentes, conocidos como "afiliados". Los afiliados pueden utilizar las plataformas proporcionadas por el grupo principal de ransomware para instalar malware, publicar datos extraídos y blanquear los beneficios de sus delitos. A cambio de utilizar la plataforma, los afiliados pagan una cuota al grupo central de ransomware, que puede ser una suscripción mensual o un porcentaje de los importes recibidos en concepto de rescates recibidos a través de la plataforma.

A medida que van madurando, estas operaciones de ransomware como servicio permiten a los ciberdelincuentes agilizar los procesos y ampliar sus actividades. También están contribuyendo a la aparición de nuevas variantes más sofisticadas y agresivas. Fortinet detectó más de 10 600 nuevas variantes de ransomware en el primer semestre de 2022, el doble que en los seis meses anteriores[14]. Fundamentalmente, los programas de afiliación y otras operaciones de ransomware como servicio se basan en el desarrollo y especialización constantes del ecosistema de servicios de los ciberdelincuentes. Los miembros principales de los grupos de ransomware reclutan a diversos especialistas para dirigir los programas de afiliación: desarrolladores, pen-testers, administradores de sistemas, gestores de datos, negociadores, reclutadores, expertos jurídicos y contables[15]. También recurren a proveedores de servicios externos, como intermediarios de acceso inicial y servicios de blanqueo de capitales y alojamiento blindado (BPH). Por ejemplo, el año pasado, Br0k3r, uno de los intermediarios de acceso inicial más activos especializados en África y Oriente Próximo, tenía a la venta en su tienda en línea más de 60 ofertas de acceso a redes corporativas con privilegios de administrador de dominios[16]. Como miembros principales, los afiliados y proveedores de servicios pueden formar parte de varios grupos y es importante desarticular el ecosistema de servicios en su conjunto para poner coto al ciberdelito.

Source: Northwave-Cybersecurity.com

Esquema general del ecosistema de servicios ciberdelictivos que permite el ransomware

14 Fortinet (2023): https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

15 Europol (2023): https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf

16 Group-IB (2024): https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/

OPERACIÓN LANDSLIDE

A principios de 2023, INTERPOL puso en marcha una operación denominada "Landslide" dirigida contra la infraestructura que permite la comisión de ciberdelitos como el ransomware. El objetivo específico de la operación Landslide era acabar con un factor de delincuencia que ha estado durante demasiado tiempo fuera del alcance de las fuerzas del orden: el alojamiento blindado (BPH). En colaboración con las autoridades de las Seychelles y el socio privado Trend Micro, INTERPOL descubrió una serie de proveedores de alojamiento blindado implicados en la facilitación de actividades ilícitas. Sobre la base de los resultados de actividades operativas anteriores, INTERPOL logró limpiar y desmantelar infraestructuras malignas. La operación todavía está en marcha.

Resiliencia frente al ransomware en África: avances significativos y retos pendientes

Los países africanos miembros de INTERPOL han tomado medidas importantes para hacer frente a la amenaza persistente del ransomware. Por ejemplo, más del 60 % ha introducido un mecanismo de notificación de delitos cibernéticos para apoyar la detección, mitigación e investigación de ataques. Los Estados también están aumentando la colaboración con el sector privado y casi dos tercios de los países miembros africanos se han asociado con terceros del sector privado para combatir el ransomware. Además, los países africanos han informado de mayores esfuerzos para concienciar a las empresas de la amenaza de la ciberextorsión. A escala regional, otro avance positivo es la creación de grupos de trabajo conjuntos en los que participan organismos encargados de la aplicación de la ley de toda África, con el fin de responder mejor a los ataques de ransomware y concienciar sobre su impacto.

A pesar de estos logros significativos, los países miembros también informan de los retos pendientes. El nivel de las denuncias por parte de las víctimas de ataques de ransomware sigue siendo un problema y afecta a la capacidad de las fuerzas del orden para poner en marcha investigaciones. Además, los países miembros informaron de que el 16 % de las víctimas acabaron pagando el rescate en caso de ataques de ransomware. Por desgracia, el pago del rescate no garantiza el fin del ataque, ni que el software maligno vaya a ser eliminado de los sistemas. En algunos casos, es posible que la víctima ni siquiera recupere sus datos o que tenga que hacer frente además al coste de la recuperación[17]. Además, el pago del rescate no evita nuevos ataques. Es más, puede suponer un incentivo y nuevos recursos para que los autores del ransomware sigan ampliando sus actividades. Consciente de este reto, INTERPOL, junto con cincuenta países miembros de la iniciativa internacional contra el ransomware (Counter Ransomware Initiative), publicó en noviembre de 2023 una declaración conjunta en la que desaconsejaba enérgicamente a las organizaciones el pago de los rescates por ransomware[18].

ESTAFAS EN LÍNEA

Puntos clave:

- Las estafas en línea y los modus operandi relacionados evolucionan constantemente y los autores se dirigen a víctimas de todos los grupos demográficos y sectores.
- La suplantación de identidad por correo electrónico y en las redes sociales explota el elemento humano y actúa como una importante puerta de entrada para otros ciberdelitos.
- La inteligencia artificial está proporcionando nuevas vías a los delincuentes que se dedican a la estafa denominada pig butchering (despiece del cerdo) y a las estafas sentimentales por Internet.
- En un reflejo de las tendencias sociales, los teléfonos inteligentes son cada vez más el blanco de los estafadores a través de los troyanos bancarios.

17 Sophos (2023) : https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

18 La declaración está disponible en el sitio web oficial de la Counter Ransomware Initiative: https://counter-ransomware.org/briefingroom/8ed7d1de-1a74-4a36-a2df-d5950624ebd8

Las estafas en línea, una grave crisis socioeconómica en África

Además del ransomware, una de las principales amenazas cibernéticas identificadas por los países miembros africanos en 2023 fueron las estafas en línea, en términos de volumen y de impacto financiero general. Una estafa en línea es una operación fraudulenta llevada a cabo mediante el uso de tecnología informática y a través de Internet, con la intención de robar dinero o información personal de particulares u organizaciones. Para lograr sus objetivos, los delincuentes suelen utilizar una combinación de elementos técnicos, como el phishing y el malware, asociados a técnicas de ingeniería social[19].

El crecimiento exponencial de las estafas en línea está relacionado con la transformación digital que se está produciendo en el continente africano[20]. A medida que los africanos pasan más tiempo en el ciberespacio, por ejemplo, comunicándose a través de las redes sociales, o pagando a través de la banca móvil, la superficie de ataque se va ampliando para los delincuentes que buscan cometer estafas a través de medios digitales. Es difícil cuantificar las pérdidas causadas por las estafas en línea en todo el continente africano, pero los países miembros de INTERPOL han indicado que se pueden encontrar víctimas individuales en todos los grupos de edad, sexos y profesiones. Aunque algunos grupos pueden ser más vulnerables a formas específicas de estafas en línea, en última instancia cualquier ciudadano puede convertirse en víctima. Asimismo, las organizaciones objetivo de las estafas en línea pueden ir de pequeñas y medianas empresas a organizaciones muy grandes y se distribuyen por todos los sectores e industrias. En resumen, la prevalencia de las estafas en línea en África representa una crisis socioeconómica importante que afecta a países de la región y de fuera de ella.

Entre la amplia gama de estafas en línea, los países africanos miembros de INTERPOL informaron de cinco tipos de estafa fraudulentas especialmente destacadas en 2023. Se trata, en el orden de su presentación de: estafas a empresas por e-mail mediante suplantación de identidad (estafa BEC), **estafas de phishing, estafas sentimentales, despieces del cerdo y estafas relacionadas con la telefonía móvil.** A continuación analizamos estas diferentes formas de estafas en línea, con excepción de las estafas BEC, que se examinan en una sección independiente debido a su prevalencia particularmente alta en África.

La suplantación de identidad por correo electrónico y en redes sociales es la puerta de entrada a otros ciberdelitos

Los países miembros africanos identificaron el phishing como la amenaza de estafa en línea predominante, tanto por el número de casos como por su impacto socioeconómico en todo el continente. Las estafas por phishing son un tipo de estafa en línea en las que los atacantes se hacen pasar por organizaciones o entidades legítimas a través del correo electrónico, las plataformas de mensajería o sitios web falsos, con el fin de engañar a las personas para que faciliten información personal sensible[21]. Esta información suele incluir credenciales de inicio de sesión, detalles financieros (como números de tarjetas de crédito), números de la seguridad social y otros datos que se pueden utilizar para obtener acceso no autorizado a cuentas o para llevar a cabo robos de identidad o robos financieros. Los intentos de phishing suelen consistir en comunicaciones urgentes o alarmantes cuyo objetivo es provocar en el destinatario una acción inmediata, como hacer clic en un enlace maligno, descargar un archivo adjunto infectado con malware o facilitar directamente información confidencial. Aunque el objetivo principal del phishing es explotar la psicología humana para acceder a datos o activos valiosos, **en la práctica, los ataques de phishing suelen servir de puerta de entrada a otros ciberdelitos, como el ransomware y diversos tipos de estafas en línea.**

En toda África se ha `podido determinar dos formas distintas de phishing sobre la base de los resultados de la encuesta y de acuerdo con los datos internos de INTERPOL: el phishing tradicional y el phishing social. En este contexto, los países miembros africanos han identificado el phishing tradicional como la amenaza más importante de la ciberdelincuencia en la región. Las campañas de phishing tradicionales, ejecutadas principalmente a través del correo electrónico, suelen consistir en mensajes procedentes de direcciones que parecen legítimas, pero que en realidad son falsas. El objetivo es manipular a los destinatarios para que visiten sitios web fraudulentos o hagan clic en enlaces malintencionados, donde la información de carácter personal que se escriba será robada por los delincuentes. Una forma frecuente de ataque de phishing por correo electrónico es la suplantación de identidad, que se analiza con más detalle en la siguiente sección de este informe.

19 Para contrarrestar el aumento de las estafas en línea, la Dirección de Ciberdelincuencia de INTERPOL colabora estrechamente con el Centro de INTERPOL contra la Delincuencia Financiera y la Corrupción (IFCACC). Para más información sobre el IFCACC: https://www.interpol.int/en/Crimes/Financial-crime

20 IJSSRR (2023): https://www.ijssrr.com/journal/article/view/1360

21 CSCR (2023): https://csrc.nist.gov/projects/human-centered-cybersecurity/research-areas/phishing

A pesar de la importancia que sigue teniendo el phishing tradicional, los países miembros africanos informan de un aumento del uso de **las redes sociales y la mensajería instantánea para cometer ataques de phishing.** El modus operandi es similar al del phishing tradicional, pero se pone en práctica en plataformas diferentes: los autores utilizan cuentas falsas en redes sociales y mensajes engañosos como señuelo para obtener los datos financieros y la información personal identificable (IPI) de las víctimas. Según los datos facilitados por los países miembros de INTERPOL, las plataformas más utilizadas para estafas por phishing en África fueron Meta (antes Facebook), Messenger y WhatsApp. La adaptación de las técnicas de phishing para incluir las redes sociales y los servicios de mensajería es una forma de incorporar los modos de comunicación predominantes en la región e ilustra la capacidad de los estafadores para explotar las tendencias tecnológicas y sociales con fines malintencionados.

Ambas formas de phishing se basan en la ingeniería social. A este respecto, es preocupante que los países miembros de INTERPOL informen del empleo por parte de los autores de los delitos de tácticas de ingeniería social cada vez más sofisticadas en el marco de las modernas campañas de phishing. Por ejemplo, durante la operación Echoes, dirigida por Marruecos con el apoyo de INTERPOL y sus socios privados, se descubrió que el delincuente conocido como "Ex-Robotos", famoso por haber desarrollado un kit de phishing con el mismo nombre, seleccionaba meticulosamente a sus víctimas mediante investigación en línea, con preferencia por los directores generales y otros directivos. En otros casos, los estafadores han recurrido a servicios legítimos y a la apropiación de dominios y cuentas de correo electrónico para mejorar la tasa de éxito de sus campañas de phishing. Por último, los datos procedentes de los países miembros de INTERPOL y de los socios de Gateway sugieren que la inteligencia artificial es el último avance tecnológico explotado por los delincuentes, por ejemplo para minimizar las señales de advertencia tradicionales del phishing.

OPERACIÓN ECHOES :

En mayo de 2023, las autoridades marroquíes, en estrecha colaboración con INTERPOL, Microsoft y Group-IB, desmantelaron las actividades de unos ciberdelincuentes sospechosos de utilizar un kit de phishing de Microsoft 365 para atacar a miles de víctimas. El kit había permitido a los delincuentes robar los datos de las víctimas, que luego podían monetizar o vender en la web oscura. La acción conjunta, denominada operación Echoes, se basa en anteriores colaboraciones con las autoridades marroquíes, como la operación Lyrebird, y demuestra la determinación del país a la hora de hacer frente a las ciberamenazas.

El catfishing y la extorsión sexual alimentan una epidemia de estafas sentimentales por Internet

Los datos facilitados por los países africanos miembros de INTERPOL también ponen de relieve el creciente volumen, la repercusión y la sofisticación de las estafas sentimentales que se producirán en o procederán de África en 2023. Las estafas sentimentales por Internet pueden adoptar diversas formas, pero todas giran en torno a delincuentes que fingen una relación romántica o una amistad íntima para obtener beneficios económicos. En general, los estafadores se ponen en contacto con sus víctimas con el pretexto de una relación sentimental, a menudo, utilizando una identidad falsa en Internet. Según los datos facilitados por los países miembros de INTERPOL, los delincuentes de toda África abordan con mayor frecuencia a sus víctimas a través de las redes sociales, los servicios de mensajería y las aplicaciones de citas en línea. A continuación, intentan entablar una relación personal con la víctima, aprovechándose de sus vulnerabilidades y debilidades. Esta etapa puede terminar muy rápidamente o durar varios años. Una vez que han logrado crear la ilusión de una relación de confianza, los agresores proceden a manipular o a robar a sus víctimas.

En África, los países miembros de INTERPOL destacaron dos tendencias de especial importancia en lo que se refiere a las estafas sentimentales: el **catfishing** y la **extorsión sexual.** En el contexto de las estafas sentimentales, el catfishing se produce cuando los estafadores crean una identidad falsa en Internet para engañar a sus víctimas[22]. Lo hacen robando información e imágenes de otras personas para crearse identidades falsas. El engaño puede consistir en utilizar una foto de perfil robada para parecer más atractivo o incluso apropiarse por completo de la identidad de otra persona, incluidos su nombre, imagen, sexo, fecha de nacimiento y ubicación geográfica. **Según han informado los países africanos miembros de INTERPOL, las tramas de catfishing tienden a dirigirse contra objetivos seleccionados y se producen a lo largo de periodos de tiempo prolongados.** Tras elegir a sus víctimas,

22 La práctica del catfishing existe desde hace muchos años, especialmente en foros y sitios web de citas en línea. Las personas pueden caer en una estafa de catfishing por diferentes motivos. Algunas personas están motivadas por la inseguridad, mientras que otras personas tienen intenciones delictivas, por ejemplo acosar por Internet o estafar a sus víctimas.

los estafadores utilizan un guion cuidadosamente elaborado para entablar una relación de confianza, antes de intentar manipularlas emocionalmente para que les transfieran una cantidad de dinero. Por ejemplo, un estafador puede afirmar que él o alguien cercano está enfermo, herido o en la cárcel, o pedir ayuda económica para reunirse en persona o planificar un futuro en común[23]. Una vez transferidos los fondos, desaparecen, dejando a la víctima no solo en la miseria económica, sino también emocional y psicológica. Además de utilizar tácticas de ingeniería social cada vez más sofisticadas, **algunos estafadores también aprovechan los avances de la tecnología de inteligencia artificial (IA).** Además de crear imágenes falsas para enganchar a sus víctimas, utilizan chatbots de inteligencia artificial como LoveGPT para crear perfiles falsos, redactar textos y, en última instancia, atrapar a sus víctimas en aplicaciones de citas[24].

La segunda tendencia en estafas sentimentales señalada por los países miembros africanos es el aumento de los casos de extorsión sexual. La extorsión sexual tiene cierta similitud con otras formas de estafa sentimental. Los delincuentes suelen utilizar una identidad falsa para ponerse en contacto con sus víctimas (a menudo jóvenes) a través de aplicaciones de citas, redes sociales y otras plataformas en línea. Sin embargo, tras ganarse su confianza, los estafadores convencen a su víctima de que envíe información íntima o sexualmente explícita y luego amenazan con publicar este contenido en Internet o compartirlo con familiares y amigos como forma de chantaje. Para presionar más todavía a sus víctimas, los delincuentes empiezan divulgando información íntima de su objetivo en Internet y luego exigen un pago a cambio de retirar el contenido. Aunque la extorsión sexual suele asociarse a mensajes, fotos o videos de carácter explícito, es importante señalar que, dependiendo de las particularidades de la comunidad de la víctima, puede bastar con que un estafador amenace con hacer públicos chats de contenido sentimental para extorsionar a sus víctimas.

El modus operandi de la extorsión sexual parece ser muy dinámico. Por ejemplo, algunos países han informado de casos de extorsión sexual en los que se utilizaron métodos de phishing para acceder al contenido privado (no publicado) de las víctimas en sus cuentas de Facebook e Instagram. En estos casos, el agresor accede ilegalmente a los perfiles de las víctimas en las redes sociales para buscar y extraer sistemáticamente contenido íntimo. El aspecto delictivo de esta operación culmina cuando el autor extorsiona a las víctimas, amenazándolas con publicar su contenido privado en plataformas de redes sociales a menos que se efectúe un pago, o con compartirlo de cualquier forma. Otro fenómeno reciente es el uso de inteligencia artificial para generar imágenes "reales" sexualmente explícitas con el fin de intimidar y extorsionar a las víctimas, que pueden ser incluso menores[25]. Dadas las importantes dificultades a las que pueden enfrentarse para retirar estos contenidos manipulados una vez publicados en línea, algunas víctimas prefieren pagar a los extorsionadores.

Las estafas sentimentales han resultado ser muy rentables. Los informes de los países miembros africanos revelan que los pagos efectuados en respuesta a estafas sentimentales, que van del catfishing a la extorsión sexual, no son meros incidentes aislados. Las víctimas a menudo acaban pagando cuotas mensuales recurrentes, ya sea para preservar la relación que perciben como sentimental o para evitar la divulgación de su contenido personal. Según algunas estimaciones, las pérdidas mundiales asociadas a esta ciberamenaza superaron los 1 300 millones de dólares entre 2017 y 2022 y la víctima media perdió unos 4 400 dólares por estafa[26]. Además de su impacto financiero, las estafas sentimentales por Internet pueden tener un impacto emocional devastador en las víctimas que, en algunos casos, llegan al suicidio. De hecho, debido al sentimiento de vergüenza, culpa o negación que experimentan las víctimas, así como al estigma social persistente, muchos incidentes no se llegan a denunciar. Como ocurre con otros ciberdelitos, es probable que el impacto real de las estafas sentimentales sea incluso mayor de lo que sugieren las cifras oficiales. Dado que el volumen, la escala y la complejidad crecientes de las estafas sentimentales plantearán un número cada vez mayor de problemas de investigación a los organismos encargados de la aplicación de la ley en toda África, será esencial proporcionar una formación y una capacidad forense adecuadas.

OPERACIÓN CONTENDER: CONTRA LAS ESTAFAS SENTIMENTALES POR INTERNET

Durante la operación Contender, INTERPOL colaboró con unidades de lucha contra la ciberdelincuencia de Benín, Côte d'Ivoire, Nigeria, Finlandia y Suiza, así como con varios socios privados, para desarticular redes organizadas de ciberdelincuentes implicadas en estafas sentimentales. La operación se saldó con la detención de tres sospechosos en Cote d'Ivoire y Benín a primeros de 2023 y con la incautación de dispositivos móviles y digitales utilizados con fines delictivos.

23 US FTC (2023): https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed
24 Avast (2023): https://decoded.avast.io/threatintel/lovegpt-how-single-ladies-looking-for-your-data-upped-their-game-with-chatgpt/
25 Reuters (2023): https://www.reuters.com/world/us/fbi-says-artificial-intelligence-being-used-sextortion-harassment-2023-06-07/
26 US FTC (2022): https://www.ftc.gov/news-events/blogs/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

Pig butchering (estafa del despiece del cerdo), una amenaza híbrida emergente

Como en otras partes del mundo, en 2023 los países miembros de INTERPOL identificaron la denominada pig butchering, o estafa del despiece del cerdo, como una de las formas de estafa por Internet de más rápido crecimiento. A pesar de que es un fenómeno relativamente nuevo, más de un tercio de los países africanos miembros notificaron incidentes de este tipo en 2023, especialmente en África Occidental y Austral[27]. Según datos internos, este tipo de estafa está provocando grandes daños económicos en todo el continente, en línea con los patrones mundiales. Las investigaciones sugieren que la suma media transferida a los monederos de criptomonedas de los estafadores oscila entre los 10 000 y los 100 000 dólares estadounidenses, mientras que las pérdidas mundiales atribuidas a las estafas con criptomonedas de este tipo casi se han duplicado desde 2022, hasta superar los 3 300 millones de dólares en 2023[28].

Como se explica en la Evaluación Mundial de INTERPOL sobre el Fraude Financiero 2024, el pig butchering es una estafa híbrida que combina elementos de las estafas de inversión en criptomonedas y las estafas sentimentales por Internet. El proceso sigue normalmente tres pasos: en primer lugar, los delincuentes se ponen en contacto con las víctimas a través de plataformas digitales, incluidas las redes sociales como Facebook e Instagram, servicios de mensajería como SMS, WhatsApp, Telegram y Signal, o bien aplicaciones de citas. Pueden indicar que han recibido los datos de contacto de la víctima a través de un amigo común o una recomendación. Para atraer mejor a sus objetivos, los delincuentes suelen utilizar una cuenta falsa, haciéndose pasar por una persona atractiva con fotos robadas a otros individuos o generadas mediante IA, en un modus operandi similar al de las estafas sentimentales. En la fase siguiente, "engordan" a la víctima ganándose su confianza y presentándose gradualmente como expertos en inversiones. La táctica de los delincuentes consiste en engañar a las víctimas para que inviertan en empresas de criptomonedas aparentemente legítimas y rentables. Sin embargo, en cuanto la víctima ha transferido cantidades sustanciales o empieza a darse cuenta de que está siendo estafada, los delincuentes retiran el dinero y desaparecen. Para dificultar al máximo el rastreo y la recuperación de los activos, los delincuentes suelen tratar de convertir los fondos de sus víctimas a través de pagos digitales o plataformas de criptomonedas. Durante esta última fase, a veces conocida como "sacrificio", los agresores dejan de responder a los mensajes o llamadas de la víctima, lo que provoca daños económicos y emocionales.

Las fases de la estafa "pig butchering" (Source: IGCR 2023)

27 INTERPOL Global Financial Fraud Assessment 2024: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/INTERPOL-led-operation-targets-growing-cyber-threats

28 Trend Micro (2023): https://www.trendmicro.com/vinfo/sg/security/news/cybercrime-and-digital-threats/unmasking-pig-butchering-scams-and-protecting-your-financial-future

En los casos de estafas pig butchering notificadas por los países miembros africanos, se ha observado una distinción general entre los métodos iniciales de contacto utilizados por los ciberdelincuentes, que pueden ser redes sociales (como Facebook e Instagram) y servicios de mensajería móvil (como WhatsApp, Telegram, Signal y SMS), lo que incluye el uso de chats grupales. Las víctimas abordadas a través de redes sociales a menudo experimentaron técnicas de ingeniería social más agresivas en comparación con el enfoque más amplio y menos personalizado observado en las plataformas de mensajería. Además, los países miembros destacaron la simplicidad de los tramas de pig butchering y la amplia disponibilidad de kits de suplantación de identidad como factores principales del aumento constante de casos a lo largo de 2023.

Este aumento ha llevado a las fuerzas del orden de los países africanos miembros a detectar graves obstáculos en sus investigaciones. Entre ellos se encuentran la dificultad para que los proveedores de servicios aporten datos y el gran número de dispositivos que requieren un análisis forense. Además, el crecimiento de las estafas pig butchering, en línea con otros ciberdelitos, agrava los problemas jurisdiccionales. Para dar respuesta a estos retos, los países han adoptado medidas positivas. En África Austral se ha creado un grupo operativo conjunto para combatir las estafas pig butchering, con algunos éxitos notables. Además, INTERPOL ha organizado una serie de sesiones de formación y ha facilitado la celebración de reuniones con los proveedores de servicios pertinentes del continente a fin de reforzar la acción regional contra este tipo de estafas.

Los teléfonos inteligentes, objetivo creciente de los estafadores en África

Los países miembros africanos están sufriendo un aumento del número de estafas dirigidas a los usuarios de teléfonos móviles en 2023. Esta realidad refleja tanto el crecimiento constante de la tasa de penetración del móvil en África como el rápido aumento del uso de los servicios bancarios móviles en todo el continente[29]. Las estafas más comunes a través de teléfonos inteligentes detectadas por las fuerzas del orden africanas suelen pertenecer a dos categorías principales, a menudo interrelacionadas: **los ataques de phishing móvil y los troyanos bancarios.**

El primer tipo de ataque es una mejora de los ataques de phishing comentados más arriba, en los que los delincuentes intentan redirigir a las víctimas a sitios fraudulentos, como falsos sitios web bancarios, a través de los navegadores web de sus teléfonos móviles. El segundo tipo de estafa con teléfonos inteligentes que observan con frecuencia las fuerzas del orden africanas consiste en el uso de troyanos bancarios similares a programas malignos. Se trata de malware diseñado para robar información financiera y otra información confidencial, como credenciales de banca en línea, números de cuenta o datos de tarjetas de crédito de las máquinas infectadas. Los troyanos bancarios pueden desplegarse a través de varios vectores de ataque, como correos electrónicos de phishing, ataques drive-by-download o la descarga de programas manipulados, lo que incluye aplicaciones móviles falsas. Al igual que otros troyanos, suelen disfrazarse de software legítimo para acceder a una máquina, lo que dificulta su detección. Además, actúan como troyanos de acceso remoto (RAT), lo que permite al autor controlar a distancia el sistema infectado y llevar a cabo otros ataques, incluido el ransomware[30]. Una vez instalado, el malware recopila y extrae datos confidenciales a través de diversos métodos, como el registro de pulsaciones de teclas, la captura de pantallas, el volcado de credenciales almacenadas en caché y la búsqueda de contraseñas guardadas en el sistema. Los autores de la amenaza pueden utilizar esta información directamente para robar dinero a sus víctimas, por ejemplo accediendo de forma remota a sus aplicaciones bancarias, o para cometer otros delitos, como el robo de identidad y otros tipos de estafas.

Los troyanos bancarios y las estafas en línea asociadas a ellos suponen un reto importante para el continente africano, con un elevado número de casos registrados, especialmente en África Austral. Teniendo en cuenta la creciente dependencia de los ciudadanos respecto a los teléfonos inteligentes y los pagos móviles, todos los países miembros africanos han expresado su preocupación por el posible impacto socioeconómico de las estafas relacionadas con los teléfonos inteligentes. Además, los troyanos bancarios están ejerciendo una mayor presión sobre las capacidades forenses digitales de toda la región. Para hacer frente a este reto, varios países han realizado importantes inversiones en herramientas forenses que les han permitido notificar el análisis forense de cientos de dispositivos durante el periodo de referencia. Muchos Estados africanos también están tomando medidas importantes para prevenir, investigar y desactivar mejor los troyanos bancarios móviles. Para ello, se establecen asociaciones con bancos para incautar y recuperar el producto del delito y se ponen en marcha campañas de sensibilización para informar a los ciudadanos sobre los riesgos asociados al uso de la banca en línea.

29 Véase, por ejemplo, Statista (2023): https://www.statista.com/statistics/1133777/sub-saharan-africa-smartphone-subscriptions/
30 Checkpoint (2023): https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/what-is-a-banking-trojan/

ESTAFAS A EMPRESAS POR E-MAIL MEDIANTE SUPLANTACIÓN DE IDENTIDAD (ESTAFAS BEC)

Puntos clave:

- Las estafas BEC combinan componentes técnicos y sofisticados métodos de ingeniería social y constituyen una amenaza creciente para organizaciones y particulares en toda África, especialmente en el sector financiero.
- El auge de esta amenaza híbrida se ve impulsado por los avances en el ámbito técnico, incluido el crecimiento de la ciberdelincuencia como servicio y el impacto creciente de la inteligencia artificial.
- A pesar de los importantes éxitos obtenidos por las fuerzas del orden, la presencia constante de delincuentes especializados en estafas BEC en y desde el continente africano plantea importantes retos en materia de investigación.

Las estafas BEC son una amenaza creciente en África

Dentro de la amplia categoría de estafas en línea, los países miembros de INTERPOL señalaron las estafas a empresas por e-mail mediante suplantación de identidad como una de las amenazas más importantes. Se trata de un tipo de ciberdelincuencia que recurre a la estafa por correo electrónico para atacar a organizaciones y a particulares. Por lo general, los ciberdelincuentes se hacen con el control de cuentas de correo electrónico personales o de empresas legítimas mediante ingeniería social y/o intrusión informática e intentan engañar a organizaciones y particulares para que transfieran fondos no autorizados o divulguen información confidencial.

La actividad de los ciberdelincuentes en torno al correo electrónico está aumentando en toda África, tanto en lo que se refiere al volumen de los ataques como a su repercusión. Este desarrollo refleja las tendencias mundiales: entre abril de 2022 y abril de 2023, Microsoft detectó e investigó 35 millones de intentos de estafa BEC, lo que corresponde a unos 156 000 intentos de ataque diarios[31]. Mientras tanto, se informa de que el impacto financiero mundial de las estafas BEC ha crecido desde 2013 hasta superar los 50 000 millones de dólares en 2023[32]. Además de las pérdidas económicas directas, las estafas BEC pueden provocar daños a largo plazo, incluida la pérdida de datos confidenciales en los casos en que se divulga correspondencia sensible o propiedad intelectual. También puede tener un impacto psicológico en las víctimas.

En 2023, las empresas fueron el objetivo más común de los ataques BEC en los países africanos miembros de INTERPOL. Las empresas que operan en el extranjero realizan transacciones financieras frecuentes y disponen de controles de seguridad menos desarrollados, por lo que parecen estar especialmente expuestas. Sin embargo, los objetivos pueden ser desde pequeñas y medianas empresas hasta grandes corporaciones. **El sector financiero fue el más afectado en todos los países africanos miembros, pero ningún sector o industria es inmune a las estafas BEC.** Además de los bancos y empresas de microfinanciación, se registraron ataques frecuentes contra empresas dedicadas a la importación y exportación, petróleo y gas, productos farmacéuticos, transporte y comercio electrónico. Asimismo, aumentó el número de ataques contra instituciones gubernamentales, especialmente las paraestatales, así como contra el sector del voluntariado y particulares en todo el continente africano.

El modus operandi es común a todos los países africanos

En términos de modus operandi, **los correos electrónicos de phishing se identificaron como el vector de ataque más común para acceder al correo electrónico empresarial en casi el 80 % de los países miembros de África en 2023.** En comparación con otras formas de phishing, los correos electrónicos utilizados en casos de estafas BEC tienden a ser más difíciles de detectar porque no contienen enlaces malignos y no se envían en masa, por lo que es menos probable que se marquen como spam. Los países miembros informaron de que, además de los mensajes de correo electrónico de

31 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe
32 IC3 (Estados Unidos, 2023) https://www.ic3.gov/Media/Y2023/PSA230609

phishing, los delincuentes están utilizando diversos medios de comunicación como parte de los sistemas BEC, incluidos los mensajes de texto, las llamadas telefónicas y las reuniones virtuales. Por ejemplo, algunos actores de amenazas se han incorporado a reuniones virtuales como si fueran usuarios para robar información corporativa confidencial. También se recurre cada vez más a las redes sociales y servicios de mensajería instantánea para llevar a cabo actividades de reconocimiento y/o para ponerse en contacto con las víctimas[33].

La mayor parte de los casos notificados por los países miembros de INTERPOL pueden clasificarse en cinco categorías:

1. **Robo de datos:** Los actores de la amenaza controlan el correo electrónico y las credenciales de empleados con funciones específicas, como personal de recursos humanos y contabilidad, para obtener información de identificación personal o declaraciones de impuestos de otros empleados o directivos. Los datos obtenidos se utilizan después para lanzar otras estafas BEC. Según la información disponible, este procedimiento está aumentando, ya que los delincuentes utilizan los datos obtenidos para aplicar tácticas de doble e incluso triple extorsión contra sus víctimas.

2. **Secuestro de cuenta / violación de la seguridad del sistema:** En otra variante de estafa BEC de la que informan a menudo los países miembros los actores de la amenaza piratean el correo electrónico de un empleado o un directivo y luego utilizan la cuenta secuestrada para reclamar el pago de facturas a múltiples proveedores. Por ejemplo, varios países africanos han informado de los llamados ataques de intermediario, en los que los delincuentes interceptan y reenvían secretamente mensajes entre dos partes.

3. **Suplantación de directivos:** Se trata de una estafa de suplantación de identidad de directivos de empresas en la que los delincuentes se hacen pasar por un directivo de alto nivel para solicitar un pago en una cuenta controlada por ellos. Esta versión de la estafa BEC implica un cierto nivel de investigación y reconocimiento por parte de los delincuentes sobre el objetivo de la operación.

4. **Suplantación de funcionarios de la administración pública, policías o abogados:** En esta versión de la estafa BEC, los atacantes se ponen en contacto con sus objetivos haciéndose pasar por una figura de autoridad, como un funcionario de la administración pública o un abogado, que se ocupa de asuntos confidenciales y urgentes. En 2023, varios países también informaron de casos de suplantación de identidad de funcionarios encargados de la aplicación de la ley o de organizaciones internacionales, incluida INTERPOL. A continuación, los delincuentes utilizan diversos métodos para presionar a sus víctimas para que transfieran fondos de manera rápida y discreta.

5. **Facturas falsas:** Los delincuentes intentan aprovecharse de las relaciones existentes entre la víctima y sus proveedores. Haciéndose pasar por un proveedor, envían una factura falsificada y piden a su víctima que transfiera fondos a una cuenta fraudulenta.

OPERACIÓN HARRIER: DETENCIÓN DE MIEMBROS DE ORGANIZACIONES DELICTIVAS IMPLICADOS EN ESTAFAS BEC

En respuesta a los riesgos importantes y constantes que plantea la delincuencia organizada transnacional, incluidas sus consecuencias económicas, emocionales y psicológicas descritas en esta evaluación, INTERPOL y el Grupo Atlas del Foro Económico Mundial han establecido una alianza estratégica. Esta colaboración se estableció con el doble objetivo de mejorar la comprensión del panorama mundial de las ciberamenazas y facilitar el intercambio de información policial para mitigar el impacto mundial de la ciberdelincuencia.

INTERPOL, en colaboración con los miembros de la iniciativa Atlas de la Ciberdelincuencia del Foro Económico Mundial, pudo identificar al autor de una sofisticada estafa multimillonaria que utilizaba el modus operandi de las facturas falsas. Gracias a un amplio intercambio de información policial, se vinculó al individuo en cuestión con una compleja red de delincuencia asociada al grupo delictivo organizado Black Axe, con base en África Occidental. Esta información se transmitió a los países miembros africanos implicados, lo que permitió detener al delincuente.

Aunque los vectores de ataque iniciales y los esquemas generales de la estafa BEC estaban bien asentados, la evolución de las técnicas de ingeniería social, la creciente disponibilidad de kits de crimeware como servicio y el impacto creciente de la inteligencia artificial están impulsando un aumento de la actividad en las estafas BEC.

33 Africa Center (2023) https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Evolución de las técnicas de ingeniería social

Como ocurre con muchas estafas en línea, las estafas BEC se basan en gran medida en la explotación de vulnerabilidades humanas. Teniendo esto en cuenta, es alarmante que muchos países miembros de África hayan informado del aumento de técnicas sofisticadas de ingeniería social. Por ejemplo, los autores de estafas BEC dedican mucho tiempo a investigar y vigilar objetivos potenciales para reforzar el señuelo inicial o vector de ataque. Aprovechan información públicamente disponible o bien obtenida en filtraciones de datos anteriores para diseñar mensajes lo más personales y auténticos posible. En algunos casos, los delincuentes han llegado a imitar el estilo de escritura de su objetivo o a hacer referencia a próximos eventos a los que sus víctimas han sido invitadas. **Como reflejo de estos niveles de sofisticación cada vez mayores, más de la mitad de los países africanos miembros de INTERPOL observaron un índice de éxito alto o muy alto de los correos electrónicos de suplantación de identidad utilizados en las estafas BEC.**

Muchos delincuentes que practican este tipo de estafas parecen dedicar más tiempo a moverse subrepticiamente a través del sistema de su objetivo después de haber obtenido el acceso inicial. Pueden utilizar distintos métodos para lograrlo, como añadir una aplicación de autenticación secundaria a la cuenta interceptada para eludir la autenticación multifactor[34]. A continuación, los atacantes buscan información en los correos electrónicos de la víctima o en las aplicaciones web de intercambio de archivos. La información obtenida se utiliza para elaborar planes más convincentes. Por ejemplo, mediante el análisis de un hilo de correo electrónico específico, algunos delincuentes han conseguido utilizar nombres de dominio falsos para crear múltiples direcciones de correo electrónico fraudulentas. Estas direcciones se utilizan para crear múltiples personalidades y simular una empresa, haciendo creer a su víctima que se está comunicando con distintos destinatarios del hilo original.

En un desarrollo similar, INTERPOL ha detectado una tendencia creciente a utilizar la filtración de datos obtenidos por extorsión en las estafas BEC. Tras obtener el acceso inicial, los delincuentes extraen datos que usan, no solo para diseñar ataques más eficaces, sino también para potenciar la extorsión a sus víctimas. Amenazan con filtrar información sensible (doble extorsión) o datos de terceros (triple extorsión). El uso cada vez mayor de estrategias de filtración de datos es otro recordatorio de la creciente sofisticación del panorama de las estafas BEC

RECUADRO: Señales de peligro en las estafas BEC:

Aumentan las operaciones de ciberdelincuencia como servicio

Otra pista de la creciente sofisticación, organización y especialización del ecosistema BEC es el rápido desarrollo de la ciberdelincuencia como servicio. Como reflejo de esta evolución, la Unidad de Delitos Digitales de Microsoft detectó un aumento del 38 % en la ciberdelincuencia como servicio en ataques a cuentas de correo electrónico empresariales entre 2019 y 2022[35]. Actualmente existe una gran cantidad de kits de phishing que ofrecen plantillas y scripts listos para usar que permiten a los delincuentes ampliar sus actividades de estafa BEC de forma rápida y sencilla. Por ejemplo, en 2023, Group-IB, socio de INTERPOL Gateway, alertó sobre las operaciones de W3LL, un delincuente que proporcionaba kits de

34 Véase por ejemplo: https://www.kroll.com/en/insights/publications/cyber/mfa-bypass-leads-to-account-compromise
35 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

phishing personalizados a al menos 500 autores de estafas BEC[36]. Con un volumen de negocio estimado en 500 000 dólares estadounidenses, los servicios de ciberdelincuencia de W3LL proporcionaban a los usuarios herramientas altamente personalizadas para llevar a cabo estafas BEC que les permitían, entre otras cosas, puentear la autenticación multifactor. Se estima que entre octubre de 2022 y julio de 2023 el kit de phishing de W3LL se utilizó para atacar a más de 56 000 cuentas corporativas de Microsoft 365.

Además, los investigadores en ciberseguridad han identificado un número creciente de plataformas ilícitas que ofrecen sus servicios de principio a fin, incluidas plantillas, servicios de alojamiento y otros servicios automatizados, para lanzar campañas de estafas BEC a gran escala. Un ejemplo de este tipo de plataforma es BulletProftLink, que permite a los delincuentes, no solo obtener las credenciales y la dirección IP de sus víctimas, sino también aprovechar las **direcciones IP residenciales** para que sus campañas de ataque parezcan generadas localmente. A su vez, esto les permite eludir eficazmente las alertas de «viaje imposible», un método de detección utilizado habitualmente para identificar y bloquear actividades sospechosas[37].

El impacto emergente de la inteligencia artificial

Las tendencias van hacia una sofisticación cada vez mayor de las tácticas de ingeniería social y la ciberdelincuencia como servicio supone una preocupación adicional, dado el rápido desarrollo de la inteligencia artificial y el auge de los medios de comunicación sintéticos. El año 2023 estuvo marcado por avances revolucionarios en tecnología de la IA: modelos de lenguaje de gran tamaño (LLM) como Chat GPT acapararon la atención mundial. Desafortunadamente, a pesar de los muchos casos de uso positivo, la IA también tiene el potencial de ser utilizada indebidamente por los delincuentes, incluidos los que se dedican a poner en peligro el correo electrónico de las empresas. Consciente de esta amenaza emergente, INTERPOL ha publicado una notificación morada para advertir a los países miembros sobre el riesgo de que los delincuentes utilicen la IA y la tecnología de ultrafalsificación para dar credibilidad a las estafas, por ejemplo, ocultando la identidad para hacerse pasar por familiares, amigos o parejas sentimentales[38].

En un nivel básico, la IA generativa puede permitir a los actores de amenazas BEC crear fácilmente correos electrónicos fraudulentos o falsificar mensajes de solicitud de autenticación (potencialmente a escala industrial) eludiendo al tiempo parámetros básicos de detección como errores ortográficos y gramaticales. Cuando se alimentan con los datos adecuados, los LLM pueden permitir incluso a los autores de las amenazas imitar el estilo y los patrones lingüísticos de organizaciones y personas concretas, ayudándoles a elaborar correos electrónicos más personalizados y convincentes para atraer y engañar a sus víctimas[39]. Además, los ciberdelincuentes ya están aprovechando los rápidos avances de las tecnologías de ultrafalsificación para engañar a sus víctimas, por ejemplo replicando la imagen y la voz de una persona durante llamadas telefónicas o videollamadas[40]. Dada la velocidad a la que evoluciona la tecnología de la IA, así como su importante potencial para aumentar el volumen de las estafas BEC y mejorar su nivel de sofisticación y autenticidad, los países miembros tendrán que seguir de cerca su evolución futura.

Neutralizar a los actores de estafas BEC que operan desde África

En 2023, los países miembros africanos de INTERPOL siguieron adoptando medidas operativas para desarticular las tramas BEC que trabajan desde la región. Durante la operación Nervone, INTERPOL, AFRIPOL, Group-IB y la Direction de l›Information et des Traces Technologiques (DITT) de Côte d›Ivoire lograron detener al miembro más importante del grupo conocido como OPERA1ER. Se cree que esta organización delictiva de gran nivel de organización, también conocida bajo los alias de NXM, DESKTOP Group y Common Raven, ha utilizado campañas a gran escala para comprometer el correo electrónico de las empresas y robar hasta 35 millones de dólares en 15 países de África, Asia y América Latina[41]. Mientras tanto, en el marco de la operación Jackal, INTERPOL coordinó y apoyó a las fuerzas policiales, las unidades de delincuencia financiera y los organismos encargados de la ciberdelincuencia en la represión de los grupos delictivos organizados de África Occidental, entre ellos Black Axe, una violenta banda de tipo mafioso famosa por cometer estafas en línea y de otros tipos[42]. Operaciones como esta demuestran el compromiso de los países miembros africanos con la protección de sus comunidades ante el impacto de las estafas BEC.

36 Group-IB (2023): https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

37 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

38 INTERPOL (2023): https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

39 CSA Singapur (2023): https://www.csa.gov.sg/Tips-Resource/publications/cybersense/2023/chatgpt---learning-enough-to-be-dangerous

40 INTERPOL (2023): https://www.interpol.int/content/download/20035/file/ChatGPT-Impacts%20on%20Law%20Enorcement-%20August%202023.pdf

41 INTERPOL (2023): https://www.interpol.int/en/News-and-Events/News/2023/Suspected-key-figure-of-notorious-cybercrime-group-arrested-in-joint-operation

42 INTERPOL (2023) https://www.interpol.int/en/News-and-Events/News/2023/Closing-ranks-on-West-African-organized-crime-more-than-EUR-2-million-seized-in-Operation-Jackal

OPERACIÓN NERVONE: DETENCIÓN DE UNA FIGURA CLAVE DE UN GRUPO ORGANIZADO DE CIBERDELINCUENTES

En los últimos cuatro años, el grupo de ciberdelincuentes conocido como OPERA1ER ha orquestado esquemas BEC a gran escala, campañas de phishing y ataques de malware contra servicios bancarios financieros y móviles en todo el mundo, haciéndose con hasta 35 millones de dólares estadounidenses. A principios de junio de 2023, INTERPOL, junto con AFRIPOL, Côte d'Ivoire, Estados Unidos y socios privados como Orange, Group-IB, Booz Allen Hamilton y DarkLabs, identificó y detuvo a personas sospechosas de ser altos cargos de gran importancia del grupo. El éxito de esta operación, denominada Nervone, solo fue posible gracias a una diligente puesta en común de información y a una estrecha cooperación a lo largo de varios años.

Junto a estos éxitos operativos, los países miembros africanos también han reforzado los esfuerzos de prevención y mitigación. **Más del 60 % de los países miembros encuestados pusieron en marcha campañas en 2023 para advertir a particulares y organizaciones del riesgo de ataques BEC.** Estas campañas de sensibilización se lanzaron a través de diferentes plataformas mediáticas, como la radio, la televisión, los sitios web gubernamentales y las redes sociales, con el objetivo de mejorar la ciberhigiene y evitar que los ciberdelincuentes sigan explotando el factor humano.

A pesar de estos pasos positivos, siguen existiendo grandes obstáculos para reducir el impacto de las estafas BEC en África. **Un número considerable de autores de estafas BEC están localizados en África, en particular en África Occidental, pero también cada vez más en las zonas australes del continente.** Algunos estudios indican que 11 países representan la mayor parte de la actividad de este tipo de delincuencia en el continente[43]. Algunos de los grupos delictivos implicados se han convertido en empresas multimillonarias[44]. Pueden estar respaldados por estructuras organizativas sofisticadas, con una serie de funciones especializadas que van desde administradores de infraestructuras a operadores de correo electrónico y "mulas bancarias". Además, en parte como respuesta a los éxitos de las fuerzas del orden, las estafas BEC recurren cada vez más a métodos de ofuscación para ocultar su infraestructura delictiva y se están dispersando geográficamente, lo que agrava los retos de investigación a los que se enfrentan las fuerzas del orden.

CIBERRESILIENCIA Y CAPACIDADES POLICIALES EN EL CONTINENTE AFRICANO

Para crear una imagen completa del panorama actual de las ciberamenazas, es importante, no solo tener en cuenta sus amenazas más acuciantes, sino también evaluar las capacidades existentes para contrarrestarlas. Por consiguiente, esta sección examina cuatro áreas de la ciberresiliencia africana, a partir de datos proporcionados por los países miembros: **marcos legislativos, capacidades policiales, cooperación y compromiso con el público.**

1. Los marcos legislativos contra la ciberdelincuencia en África se expanden

Unos marcos legislativos eficaces son un componente fundamental de la ciberresiliencia y un parámetro fundamental para las actividades de aplicación de la ley. A este respecto, es alentador observar el desarrollo de leyes destinadas a combatir la ciberdelincuencia en toda África. En 2023, varios países africanos aplicaron nuevas leyes, modificaron las existentes o activaron legislación de reciente introducción destinada a combatir la ciberdelincuencia[45]. Algunos ejemplos notables son el reglamento sobre la interceptación de comunicaciones en Uganda, la ley sobre la protección en línea de la infancia en Camerún, la ley sobre la protección de datos personales en Gabón, las directrices para los operadores de TIC en materia de preservación de datos en Burkina Faso y la ley sobre activos virtuales en Botsuana. Otros seis países indicaron que están en proceso de promulgar nueva legislación. Estos importantes esfuerzos se suman a la ampliación de los instrumentos regionales e internacionales existentes, como el **convenio sobre ciberseguridad y protección de datos personales de la Unión africana, conocido también como Convenio de Malabo;** la estrategia de transformación digital para África de la Unión Africana (2020-2030); el convenio de Budapest sobre la Ciberdelincuencia y sus Protocolos Adicionales.

INTERPOL apoya activamente los esfuerzos de los países miembros por transformar la legislación con el fin de combatir la ciberdelincuencia a través de

43 Agari (2023) ag-acid-geography-of-bec-gd.pdf (fortra.com)
44 Agari (2023): https://www.agari.com/resources/videos/scattered-canary-evolution-business-email-compromise-enterprise
45 Lexology (2023): https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45

diferentes abordajes. En 2023, INTERPOL participó en la ejecución del proyecto de acción mundial ampliada contra la ciberdelincuencia (GLACY+, actualmente ampliada de nuevo como proyecto GLACY-e). Esta iniciativa, fruto de la colaboración entre la Unión Europea y el Consejo de Europa, pretende reforzar las capacidades cibernéticas de los países de África, Asia-Pacífico, América Latina y el Caribe, en el ámbito del Convenio de Budapest. La ambición principal de GLACY+ es promover una legislación, unas políticas y unas estrategias coherentes en materia de ciberdelincuencia. INTERPOL desempeña un papel fundamental en este empeño, al mejorar las capacidades y las aptitudes operativas de las fuerzas del orden de los países participantes. Este esfuerzo se dirige a mejorar las competencias en la investigación de ciberdelitos y a reforzar la cooperación policial internacional mediante una serie de actividades.

Al mismo tiempo, a lo largo de 2023 INTERPOL ha participado proactivamente en los principales procesos legislativos y de política internacional, en particular en el Comité Especial de las Naciones Unidas encargado de elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos[46]. Este comité especial pretende establecer un nuevo tratado mundial para combatir las ciberamenazas que, una vez ratificado, proporcionará herramientas legislativas mejoradas a los Estados de África y de otros continentes. A través de sus contribuciones, INTERPOL ha tratado de garantizar que los intereses y las necesidades de sus numerosos miembros estén debidamente representados en la próxima Convención.

Por último desde la creación del programa de INTERPOL sobre ciberdelincuencia, la Organización ha venido desarrollando instrumentos esenciales para apoyar a los países miembros en la lucha contra la ciberdelincuencia. Entre estos instrumentos están las resoluciones mundiales (la más reciente, la resolución de 2021: Combatir las ciberamenazas mundiales por conducto de INTERPOL),[47] la estrategia mundial de INTERPOL contra la Ciberdelincuencia para 2022-2025 y, en lo que respecta específicamente a África, la recomendación regional de 2022[48]. De este modo, se insta a los países miembros africanos a aprovechar plenamente los recursos de INTERPOL para mejorar la colaboración operativa, intercambiar información policial y reforzar sus capacidades.

2. Desarrollo de las capacidades cibernéticas de las fuerzas del orden

Los datos recibidos por INTERPOL indican que los recursos humanos asignados a la lucha contra la ciberdelincuencia siguen siendo insuficientes, aunque los países están tomando medidas proactivas para mejorar la situación. Por ejemplo, en 2023, casi la mitad de los organismos encargados de la aplicación de la ley de los países miembros de INTERPOL notificaron un aumento del personal destinado a combatir la ciberdelincuencia. Además, al menos cuatro países destacaron el hecho de haber creado recientemente una unidad de ciberdelitos o estar en vías de hacerlo. Mientras tanto, a lo largo de 2023, más del 70 % de los organismos encargados de la aplicación de la ley de los países miembros africanos declararon que habían realizado actividades de ciberformación o habían participado en ellas: un total de 32 países y más de 130 iniciativas de formación. Todo ello pone de relieve los esfuerzos que se están realizando para invertir en personal y competencias con la finalidad de combatir mejor las ciberamenazas, lo que subraya el compromiso de los países miembros africanos de reforzar la ciberresiliencia en todo el continente.

En consonancia con el Objetivo 3 de la Estrategia Mundial contra la Ciberdelincuencia para 2022-2025, la Organización se propone apoyar el desarrollo de estrategias y capacidades de sus países miembros para combatir la ciberdelincuencia. Por consiguiente, INTERPOL contribuye a varias iniciativas de desarrollo de capacidades en el continente africano, como AFJOC, GLACY-e y el Programa ISPA. En 2023, estos esfuerzos se tradujeron en la realización de ocho sesiones de formación y talleres centrados en técnicas de ciberinvestigación, con especial énfasis en los activos virtuales. Además, en 22 países miembros se han adquirido y distribuido 72 herramientas y licencias especializadas cruciales para las investigaciones sobre ciberdelincuencia, con el apoyo de formación a medida sobre su utilización. INTERPOL también proporciona dos plataformas especializadas para garantizar una conexión mundial sin fisuras entre los organismos encargados de la aplicación de la ley de los países miembros. Se trata del Intercambio de Conocimientos sobre la Ciberdelincuencia para el intercambio de información no operativa, y de la Plataforma Colaborativa sobre la Ciberdelincuencia - Operaciones para el intercambio seguro y restringido de información policial operativa. Se trata de herramientas eficaces para coordinar una respuesta internacional a la ciberdelincuencia y ofrecen un sofisticado mecanismo de colaboración.

46 Más información sobre el Comité Especial: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

47 INTERPOL (2021): https://www.interpol.int/en/News-and-Events/Events/2021/89th-INTERPOL-General-Assembly

48 INTERPOL (2022): https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-African-conference-ends-with-call-for-greater-data-exchange

3. Retos de la coordinación en todo el ecosistema cibernético

Establecer y reforzar asociaciones abiertas, integradoras y diversas es clave para fomentar una cooperación eficaz en la lucha contra la ciberdelincuencia. Sin embargo, los países miembros africanos han señalado dificultades para fomentar la colaboración entre las fuerzas del orden y las partes interesadas en el ecosistema cibernético. Al parecer, trabajar con proveedores de servicios, especialmente cuando se encuentran en el extranjero, sigue siendo una dificultad importante para las investigaciones sobre ciberdelincuencia. Mientras tanto, se ha informado de que la cooperación entre el sector público y el privado a menudo se desarrolla a medida que surgen las necesidades, en lugar de contar con marcos establecidos y normalizados.

Con todas estas dificultades para establecer asociaciones y plataformas formales entre los sectores público y privado que ayuden a las empresas a combatir la ciberdelincuencia, las iniciativas estratégicas de INTERPOL pueden desempeñar un papel crucial. La iniciativa específica de INTERPOL **Gateway** es la base para llevar cabo un análisis detallado de la ciberdelincuencia, utilizando un amplio espectro de fuentes de información para localizar a los autores de los delitos, identificar a las víctimas y señalar las infraestructuras comprometidas para llevar a cabo las intervenciones necesarias. Sobre la base del Estatuto de INTERPOL y de sus principios rectores de soberanía, respeto de los derechos humanos, neutralidad y cooperación activa, Gateway establece un marco jurídico para el intercambio de información con entidades privadas mediante la firma de acuerdos de intercambio de datos. Además, INTERPOL también participa en iniciativas clave para fomentar la cooperación entre múltiples partes interesadas. Una de ellas es el **Atlas de la Ciberdelincuencia del Foro Económico Mundial**[49], que reúne a las fuerzas del orden y a los sectores público y privado para obtener nuevos conocimientos sobre el ecosistema de la ciberdelincuencia. La cooperación entre INTERPOL y la comunidad del Atlas de la Ciberdelincuencia también ha tenido resultados operativos impresionantes basados en análisis, entre ellos la elaboración de perfiles y la detención de miembros de un importante grupo de delincuentes denominado "Silver Terrier", que operaba principalmente desde África Occidental.

4. Sensibilización de la ciudadanía e higiene cibernética

Como respuesta al aumento de las técnicas de ingeniería social utilizadas para cometer ciberdelitos, los países han adoptado medidas importantes para mejorar la concienciación pública y la ciberhigiene. Es alentador que aproximadamente el 80 % de los países miembros africanos encuestados hayan puesto en marcha campañas de concienciación pública destinadas a prevenir la ciberdelincuencia. Aunque sobre todo se han llevado a cabo en línea, estas campañas se desarrollaron ocasionalmente en entornos físicos, sobre todo en instituciones educativas, centrándose así en los jóvenes y sus redes de apoyo, incluidos padres, familias y educadores. Estas campañas se desarrollaron a través de diversas plataformas en línea, como la televisión, la radio, las páginas web de noticias y las redes sociales, entre las que destacó Facebook. Una característica fundamental de estos esfuerzos es la colaboración entre los organismos encargados de la aplicación de la ley y entidades de los sectores público y privado. Las principales áreas de interés de estas campañas incluían la promoción de buenas prácticas de ciberhigiene y la concienciación general sobre las estafas en línea. Estos esfuerzos nacionales están en consonancia con la Estrategia de Educación Digital de la Unión Africana[50], que se centra principalmente en acelerar la adopción de tecnologías digitales para la enseñanza, el aprendizaje, la investigación, la evaluación y la administración.

49 Para más información sobre el Atlas de la Ciberdelincuencia del FEM: https://initiatives.weforum.org/cybercrime-atlas/home

50 Estrategia de Educación de la Unión Africana (2022): https://au.int/en/documents/20221125/digital-education-strategyand-implementation-plan

En un esfuerzo global complementario, INTERPOL ha puesto en marcha varias campañas de concienciación, como #ElPróximoPuedeSerUsted (#YouMayBeNext), #SoloUnClic (#JustOneClick) y #OnlineCrimeIsRealCrime (la ciberdelincuencia es una delincuencia real), para reforzar la capacidad de vigilancia de la comunidad, a fin de combatir a los diferentes ciberdelincuentes que intentan aprovecharse de las vulnerabilidades, robar datos, cometer estafas en línea o causar trastornos en el ámbito digital. La campaña #ElPróximoPuedeSerUsted , en particular, contó con una notable participación mundial: recibió el apoyo de 79 países miembros, así como de socios privados, diversas organizaciones internacionales, entidades privadas y organizaciones no gubernamentales, lo que le ha dado un enorme alcance. De cara a 2024, INTERPOL tiene previsto mantener este impulso con una nueva campaña centrada en la amenaza que constituye el malware.

APOYO A LA CIBERRESILIENCIA AFRICANA: OPERACIÓN CYBER SURGE II DE INTERPOL EN ÁFRICA

INTERPOL apoya la ciberresiliencia africana mediante asociaciones, plataformas y actividades de desarrollo de capacidades.

Un buen ejemplo de ello es la operación Africa Cyber Surge II:

- Los socios del proyecto Gateway de INTERPOL y del Atlas de la Ciberdelincuencia del Foro Económico Mundial proporcionaron información esencial que resultó crucial para el éxito de la operación.
- Uso de la Plataforma Colaborativa sobre Ciberdelincuencia - Operaciones para el intercambio de información y la coordinación operativa entre los países participantes.
- Una serie de sesiones de formación previa a la operación destinadas a mejorar la competencia de los investigadores en diversos ámbitos de la investigación de la ciberdelincuencia.

PRÓXIMAS MEDIDAS

Sobre la base de los resultados de la evaluación, incluido el análisis de las ciberamenazas de más rápido crecimiento en África y los esfuerzos realizados para contrarrestarlas, esta sección presenta recomendaciones destinadas a reducir el impacto y el daño de la ciberdelincuencia en el continente y en todo el mundo.

1. Introducir instrumentos de ciberseguridad fuertes y armonizados o reforzar los existentes
INTERPOL recomienda a los países miembros africanos que sigan estableciendo o reforzando instrumentos nacionales de ciberseguridad sólidos y armonizados destinados a plantar cara a la ciberdelincuencia y a darle una respuesta. Estas herramientas incluyen estrategias, políticas y marcos jurídicos cuyo objetivo es capacitar a los países para luchar contra las ciberamenazas y mitigar los riesgos asociados a ellas. Esto incluye, entre otras cosas, la eliminación de los obstáculos legales para los investigadores.

2. Invertir en cibercapacidades policiales: personal, procesos, tecnología
En reconocimiento de la importancia de reforzar los recursos de ciberseguridad en el continente, I**NTERPOL está fomentando una mayor inversión y un apoyo a largo plazo para los organismos africanos encargados de la aplicación de la ley por parte de las partes interesadas internas y externas.** La ciberdelincuencia, cada vez más sofisticada, requiere unidades más especializadas, agentes cualificados, herramientas y plataformas. En consecuencia, se anima a los países a que participen activamente en las actividades de desarrollo de capacidades ofrecidas por entidades regionales e internacionales, como las que ofrece la Oficina de Operaciones contra la Ciberdelincuencia en África (AFJOC) de INTERPOL.

3. Establecer sinergias en todo el ecosistema de la ciberseguridad
Dado el carácter transnacional de la ciberdelincuencia, **INTERPOL recomienda encarecidamente a los países miembros africanos que integren los esfuerzos de las partes interesadas pertinentes en la lucha contra la ciberdelincuencia.** La cooperación con partes interesadas pertinentes, como el sector privado y las agencias de ciberseguridad desempeña un papel crucial en la mejora de la respuesta a incidentes, el acceso a los datos, el intercambio de información policial sobre amenazas, el desmantelamiento de infraestructuras dañinas y la concienciación en materia de ciberseguridad. Además, se anima a los países a crear y utilizar equipos nacionales de respuesta a emergencias informáticas y equipos de respuesta a incidentes de seguridad cibernéticos. Para ayudar a promover una colaboración más estrecha entre los organismos encargados de la aplicación de la ley y estos equipos, INTERPOL y el foro de equipos de seguridad y respuesta a incidentes (FIRST) ha creado un Grupo de Interés Especial.

4. Reforzar la educación y sensibilización digitales
Para contrarrestar las técnicas de ingeniería social cada vez más sofisticadas, hay que prestar una atención especial al factor humano y, por tanto, a la prevención. **INTERPOL anima a los países miembros africanos a seguir centrándose en la mejora de la ciberhigiene, con el apoyo de los sectores público y privado.** Esta estrategia incluye sensibilizar a la opinión pública mediante iniciativas gubernamentales y animar a particulares y organizaciones a reforzar la seguridad del correo electrónico, utilizar la autenticación multifactor, impartir una formación exhaustiva a los empleados y adoptar tecnologías de pago seguras.
De la misma forma, se debe animar a los ciudadanos a que informen a las autoridades policiales nacionales siempre que sean víctimas de ciberdelitos. **Para ello, se recomienda a los países miembros que agilicen el proceso de notificación y registro en la medida de lo posible, por ejemplo, mediante el uso de páginas web y plataformas en línea.** Estas medidas proactivas garantizarán, no solo un entorno digital más seguro, sino también una comprensión más completa del panorama cibernético africano.

5. Ampliar y profundizar la cooperación internacional y regional
Una colaboración regional y mundial eficaz es esencial para hacer frente a la expansión geográfica de los grupos delictivos organizados y de sus víctimas. **INTERPOL insta a los países miembros a que sigan ampliando y profundizando su cooperación con el fin de ofrecer un frente unido contra la amenaza mundial de la ciberdelincuencia.** Esto incluye reforzar el intercambio de información y llevar a cabo una acción coordinada y basada en la información policial, a través de la Unidad de Operaciones contra la Ciberdelincuencia en África de INTERPOL.

INTERPOL seguirá apoyando a sus países miembros africanos para que sigan reduciendo la repercusión mundial y los daños causados por la ciberdelincuencia y protegiendo a las comunidades para lograr un mundo más seguro.

MARCO OPERATIVO CONJUNTO PARA ÁFRICA

La Oficina de Operaciones contra la Ciberdelincuencia en África de INTERPOL ha elaborado un Marco Operativo Conjunto para promover un enfoque coherente y metodológico con el fin de mejorar las operaciones proactivas coordinadas contra la ciberdelincuencia en el continente. Este marco tiene cuatro fases.

Fase I – Recopilación y análisis
Esta primera fase se centra en un profundo análisis de la información sobre las ciberamenazas predominantes, las infraestructuras malignas y los responsables de las amenazas que operan en/contra la comunidad en la región africana. Utilizando la inteligencia de las comunidades de las fuerzas del orden, la investigación realizada por la Unidad de Información sobre Ciberdelincuencia de INTERPOL, y los amplios acuerdos de intercambio de datos con socios del proyecto Gateway de INTERPOL, la Oficina de Operaciones contra la Ciberdelincuencia en África publicará el Informe de Evaluación de las Ciberamenazas en África. Este informe ayudará a las comunidades de las fuerzas del orden en África a comprender mejor el panorama de las ciberamenazas en el continente.

Fase II – Prioridades y estrategia
El Informe de Evaluación de las Ciberamenazas en África, publicado durante la Fase I del ciclo, servirá de documento de referencia para ayudar a los países miembros africanos a desarrollar y actualizar sus estrategias de investigación y el enfoque de las investigaciones, así como guiar la priorización regional de los esfuerzos operativos emprendidos conjuntamente con INTERPOL para el año siguiente. Reconociendo la diversidad de la región africana y los retos únicos a los que se enfrenta cada país, la Oficina de Operaciones contra la Ciberdelincuencia en la región africana implicará al jefe de Ciberdelincuencia de cada país durante esta fase (con autorización de la OCN pertinente) para analizar oportunidades de colaboración tanto intrarregional como interregional. Al finalizar esta fase deberá estar lista para su publicación una hoja de ruta regional basada en una estrategia conjunta acordada con resultados operativos claros para el año.

Fase III – Operaciones
La Oficina de Operaciones contra la Ciberdelincuencia en la región africana elaborará planes estratégicos estándar (Standard Tactical Plans, STP) para ejecutar la estrategia acordada en la Fase II. Estos planes ofrecerán una serie bien definida de objetivos, papeles y responsabilidades, y un concepto operativo para tratar ciberamenazas específicas. Cada plan estratégico suele incluir planes detallados sobre los siguiente: (1) planificación y análisis; (2) organización; (3) estrategia; y (4) evaluación. Seguidamente, los planes se comparten con los países participantes para su aprobación.

Las unidades de ciberdelincuencia participantes designadas por la OCN se comprometerán con la acción detallada en los planes estratégicos y ofrecerán un apoyo total para lograr los objetivos operativos acordados. Tras la aprobación, las operaciones estarán coordinadas por la Oficina de Operaciones contra la Ciberdelincuencia en la región africana y llevadas a cabo por investigadores designados de acuerdo con la cronología especificada en el plan estratégico. Los datos relacionados con las operaciones se reciben en INTERPOL a través del sistema de comunicación protegida I-24/7, o a través de su Plataforma Colaborativa contra la Ciberdelincuencia- Operaciones, para su análisis.

Una vez recibida la información operativa, los Puntos de Contacto designados de cada país miembro colaborarán con la Oficina de Operaciones contra la Ciberdelincuencia en la región para intercambiar información de acuerdo con los objetivos y calendario propuestos para la operación. El país miembro que haya tomado la iniciativa mantendrá la dirección operativa durante toda la operación.

La conservación y divulgación de los registros de Internet (información básica de los suscriptores, datos de transmisión, contenido, etc.) serán voluntarias y se alentarán para todas las operaciones de ciberdelincuencia, dada la naturaleza volátil de las pruebas electrónicas. Se insta encarecidamente a los países miembros, dentro de los límites de sus respectivas leyes y políticas, a transmitir actualizaciones de sus investigaciones e información policial específica que puedan ayudar a otros países en sus propias investigaciones. En la medida de lo posible, los Puntos de Contacto facilitarán el intercambio de información con otros organismos nacionales como los Equipos de Respuesta a Emergencias Informáticas (CERT) y los bancos centrales, dependiendo de las necesidades de cada operación.

Fase IV – Evaluación
Durante la Fase IV, se realizará una revisión después de la acción (After-Action-Review) a fin de identificar las lecciones extraídas de estas operaciones. La Oficina de Operaciones contra la Ciberdelincuencia en la región africana recomendará ajustes para futuras operaciones conjuntas basados en las revisiones y en nueva información que surja de las operaciones. La información policial recopilada durante la Fase III también se evaluará para mejorar la comprensión a nivel regional de las ciberamenazas predominantes, y fundamentar el subsiguiente informe de evaluación de las ciberamenazas en África.

NOTAS SOBRE la metodología utilizada para el Informe de INTERPOL de evaluación de las ciberamenazas en África

El Informe 2024 de evaluación de las ciberamenazas en África se basa en ediciones anteriores para ofrecer un análisis detallado del panorama de las ciberamenazas en los países miembros africanos. Esta edición presenta un análisis exhaustivo, centrado en amenazas clave como el ransomware, las estafas BEC y otras formas de estafa en línea. Además de identificar estos problemas acuciantes, el informe investiga las iniciativas nacionales en curso destinadas a reforzar la ciberresiliencia en todo el continente. Se cierra con recomendaciones prácticas destinadas a orientar los esfuerzos futuros en materia de ciberseguridad en el continente.

La evaluación se basa principalmente en información policial y datos operativos resultantes de las diversas actividades de INTERPOL en África. La información adicional procede de una encuesta dirigida por INTERPOL, consistente en 40 preguntas cuantitativas y cualitativas sobre el tema de la prevención, detección, investigación y neutralización. Un total de 46 países miembros aportaron información, lo que representa una respuesta superior al ochenta por ciento.

- **Argelia**
- **Angola**
- **Benín**
- **Botsuana**
- **Burkina Faso**
- **Burundi**
- **Camerún**
- **Cabo Verde**
- **Comoras**
- **Congo**
- **Côte d'Ivoire**
- **República Democrática del Congo**
- **Yibuti**
- **Guinea Ecuatorial**
- **Eritrea**
- **Esuatini**
- **Etiopía**
- **Gabón**
- **Gambia**
- **Ghana**
- **Guinea**
- **Guinea-Bissau**
- **Kenia**
- **Lesoto**
- **Liberia**
- **Madagascar**
- **Malaui**
- **Malí**
- **Mauritania**
- **Mauricio**
- **Mozambique**
- **Namibia**
- **Níger**
- **Ruanda**
- **Santo Tomé y Príncipe**
- **Senegal**
- **Seychelles**
- **Sierra Leona**
- **Somalia**
- **Sudáfrica**
- **Sudán del Sur**
- **Tanzania**
- **Togo**
- **Uganda**
- **Zambia**
- **Zimbabue**

Por último, este conjunto de datos se complementó con consultas estratégicas a los socios de INTERPOL Gateway, como Bi.Zone, Fortinet, Group-IB, Kaspersky Lab y Trend Micro.

INTERPOL

INTERPOL es la organización policial internacional más grande del mundo. Su cometido consiste en prestar ayuda a los organismos encargados de la aplicación de la ley en los 196 países miembros de la Organización para luchar contra todas las formas de delincuencia transnacional. Trabaja para ayudar a la policía de todo el mundo a afrontar los crecientes desafíos que plantea la delincuencia del siglo XXI, ofreciendo una infraestructura de apoyo técnico y operativo de alta tecnología. Nuestros servicios incluyen formación específica, apoyo especializado para la investigación policial, bases de datos especializadas y conductos de comunicación policial protegida.

LA META DE INTERPOL: "MAYOR COMUNICACIÓN POLICIAL PARA UN MUNDO MÁS SEGURO"
La meta de INTERPOL es lograr un mundo en el que todos los profesionales de los organismos encargados de la aplicación de la ley puedan transmitir, intercambiar y consultar de forma segura información policial esencial a través de la Organización cuando y donde lo necesiten y garantizar así la seguridad de los ciudadanos de todo el planeta. La Organización proporciona y promueve constantemente soluciones innovadoras y de vanguardia para afrontar los retos mundiales en materia policial y de seguridad.

SOBRE EL PROGRAMA DE INTERPOL CONTRA LA CIBERDELINCUENCIA
En una era digital dinámica, en la que más de la mitad de la población mundial está expuesta al riesgo potencial de la ciberdelincuencia, el Programa Mundial de INTERPOL contra la Ciberdelincuencia presta apoyo a la comunidad internacional encargada de la aplicación de la ley. Nos consagramos a desarrollar y liderar una respuesta global para prevenir, detectar, investigar y neutralizar la ciberdelincuencia, con el objetivo último de reducir su impacto global y proteger a las comunidades para lograr un mundo más seguro.

La Estrategia Mundial contra la Ciberdelincuencia de INTERPOL se centra en cuatro objetivos principales:

- Permitir un enfoque proactivo y ágil en la prevención y la neutralización de la ciberdelincuencia mediante el desarrollo de un conocimiento profundo del panorama de las amenazas de la ciberdelincuencia a través del intercambio y análisis de la información.
- Prevenir, detectar, investigar y neutralizar eficazmente la ciberdelincuencia que causa daños importantes a escala nacional, regional y mundial, liderando, coordinando y apoyando a los países miembros en las actividades operativas transnacionales.
- Apoyar el desarrollo de estrategias y capacidades de los países miembros en la lucha contra la ciberdelincuencia mediante el cultivo de asociaciones abiertas, inclusivas y diversas y la creación de confianza en el ecosistema mundial de la ciberseguridad.
- Promover el papel y las capacidades de INTERPOL en la configuración de la seguridad mundial mediante la participación en foros internacionales en el ámbito de la ciberdelincuencia.

Ponemos en práctica nuestra estrategia y objetivos mediante un modelo de prestación de servicios sencillo y constructivo, que consta de tres pilares básicos:

- Respuesta a las amenazas de la ciberdelincuencia: hacer frente a las ciberamenazas inmediatas y emergentes con una respuesta rápida y coordinada.
- Operaciones sobre ciberdelincuencia: aplicar una estrategia operativa centrada de alcance regional para combatir eficazmente la ciberdelincuencia.
- Desarrollo de capacidades cibernéticas: mejorar las estrategias y capacidades mediante proyectos y plataformas innovadores.

Estos pilares se sustentan en nuestra amplia red de asociaciones público-privadas, que fomenta la colaboración y aprovecha los conocimientos colectivos para luchar contra la ciberdelincuencia.

Si desea más información, póngase en contacto con nosotros en la siguiente dirección EDPS-CD@interpol.int

LA OFICINA DE INTERPOL DE OPERACIONES CONJUNTAS CONTRA LA CIBERDELINCUENCIA EN ÁFRICA

AFJOC es una iniciativa de INTERPOL que refuerza la capacidad de los organismos africanos nacionales encargados de la aplicación de la ley para prevenir, detectar, investigar y neutralizar la ciberdelincuencia. Las herramientas para conseguirlo son:

- Recopilación y análisis de información sobre actividades de ciberdelincuencia;
- Realización de actividades coordinadas basadas en información policial;
- Promoción de la cooperación y las buenas prácticas entre países miembros africanos.

La fase 1 de la iniciativa fue financiada por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido y se desarrolló de 2021 a 2023. La segunda fase, que cuenta con el apoyo del mismo organismo del Reino Unido, se basa en los logros de la primera y tiene por objeto seguir mejorando las capacidades de los organismos nacionales encargados de la aplicación de la ley en África.

Actividades del proyecto

- Apoyo analítico e información policial: recibir información policial correcta y a tiempo es vital en cualquier respuesta policial a la ciberdelincuencia. Nuestros informes sobre ciberdelincuencia son un recurso importante, y ofrecen información sobre ciberamenazas dirigidas contra países o regiones concretos.
- Desarrollo de la capacidad nacional y de los recursos para combatir la delincuencia: las plataformas colaborativas como la Plataforma Colaborativa sobre Ciberdelincuencia y la Plataforma de Intercambio de Información sobre la Ciberdelincuencia permiten establecer comunicaciones seguras e intercambiar datos sobre las operaciones.
- Marco operativo conjunto: este marco permite abordar las amenazas de ciberdelincuencia mediante la colaboración entre organismos encargados de la aplicación de la ley, el sector privado , y otras organizaciones internacionales e intergubernamentales.
- Apoyo a las operaciones y coordinación: nuestras operaciones ayudan a desmantelar las redes delictivas que se esconden detrás de la ciberdelincuencia.
- Campañas de sensibilización: estas campañas promueven buenas prácticas cibernéticas y están dirigidas a personas y empresas en África.

Nuestra Oficina de Operaciones contra la Ciberdelincuencia en la región africana es la responsable de la ejecución del proyecto AFJOC. Esta Oficina trabaja en estrecha colaboración con las entidades interesadas más importantes de la región, en particular la Unión Africana y AFRIPOL, así como con grupos de las fuerzas del orden y el sector privado.

INTERPOL

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

Síguenos:

INTERPOL HQ | @INTERPOL_HQ | INTERPOL | INTERPOL HQ | INTERPOL_HQ