



INTERPOL

INFORME SOBRE LA EVALUACIÓN DE LAS CIBERAMENAZAS EN ÁFRICA

PANORAMA DE LAS TENDENCIAS DE LAS CIBERAMENAZAS, POR LA OFICINA DE OPERACIONES CONTRA LA CIBERDELINCUENCIA EN LA REGIÓN AFRICANA



Marzo 2023

ÍNDICE

| | |
|---|-----------|
| AVISO LEGAL | 2 |
| PRÓLOGO | 3 |
| PRÓLOGO | 5 |
| ABREVIATURAS Y ACRÓNIMOS | 7 |
| AGRADECIMIENTOS | 8 |
| RESUMEN | 9 |
| 1. DESARROLLO DIGITAL ACTUAL EN LA REGIÓN AFRICANA | 11 |
| 2. REFLEXIONES SOBRE LAS TENDENCIAS DE LAS CIBERAMENAZAS EN ÁFRICA EN 2022 | 13 |
| 2.1 Business Email Compromise | 14 |
| 2.2 Phishing | 16 |
| 2.3 Ransomware | 18 |
| 2.4 Troyanos bancarios y stealers | 21 |
| 2.5 Estafas en línea y extorsión | 22 |
| 2.6 Crimeware como servicio | 25 |
| 3. BREVE PERSPECTIVA DE LAS CIBERCAPACIDADES EN LA REGIÓN AFRICANA | 27 |
| 4. PRÓXIMAS ETAPAS: ACCIÓN PROACTIVA CONTRA LAS CAMBIANTES CIBER AMENAZAS EN LA REGIÓN AFRICANA | 29 |
| 5. CICLO DE PLANIFICACIÓN ANUAL DE LA OFICINA DE OPERACIONES CONTRA LA CIBERDELINCUENCIA EN LA REGIÓN AFRICANA | 30 |

AVISO LEGAL

Las denominaciones empleadas y la presentación del material en esta publicación no implican la expresión de ninguna opinión por parte de INTERPOL en relación con la situación jurídica de ningún país, territorio, ciudad o área, o de sus autoridades, o en relación con la delimitación de sus fronteras o límites.

Las denominaciones de grupos de países tienen únicamente fines estadísticos o analíticos y no expresan ningún juicio sobre un determinado país o área.

Las referencias a nombres de empresas y productos comerciales y procesos no implican que estén respaldados por INTERPOL, y el hecho de no mencionar a una determinada empresa, un producto comercial o un proceso no es signo de desaprobación.

INTERPOL ha tomado todas las precauciones razonables para verificar la información contenida en esta publicación. No obstante, el material aquí publicado se distribuye sin garantía expresa o implícita alguna. La responsabilidad por la interpretación y uso del material recae en el lector. INTERPOL no se responsabilizará en ningún caso por cualquier daño que pueda derivarse de su utilización.

INTERPOL no se responsabiliza de la exactitud constante de la información ni del contenido de ningún sitio web externo.

INTERPOL tiene el derecho de alterar, limitar o suprimir contenidos de esta publicación.

PRÓLOGO

Actualmente, la tecnología es una parte indispensable de nuestras vidas, especialmente internet, que tiene un papel esencial tanto en nuestras actividades profesionales como personales. La utilizamos para controlar sistemas de infraestructuras críticas, realizar operaciones financieras de forma segura y eficiente, mantenernos en contacto con amigos y familiares, y comprar conveniente y rápidamente en línea, así como entretenernos viendo vídeos o jugando. Además de sus muchas aplicaciones, internet también nos posibilita un acceso sin precedente a información que anteriormente era inalcanzable. Internet nos ha permitido ponernos en contacto con personas de todo el mundo y ha simplificado el proceso de recopilación de datos e información con fines de investigación. Incluso nos ha permitido explorar mundos virtuales que van más allá de lo posible en el campo físico. Con todas estas ventajas, no es sorprendente que internet esté muy presente en nuestra vida diaria.

Con el surgimiento de nuevas tecnologías, la ciberdelincuencia también ha supuesto una creciente preocupación en los últimos años. Los ciberdelincuentes mejoran continuamente sus técnicas a fin de explotar nuevas vulnerabilidades, lo que implica un mayor riesgo tanto para las personas como para las organizaciones de todo el mundo. La ciberdelincuencia hoy día no tiene nada que ver con lo que era. Ahora, hay vectores de ataque más sofisticados como ataques DDoS, intentos de phishing, campañas de malware, ataques de ransomware y otras actividades maliciosas que pueden causar mucho daño y afectar considerablemente a organizaciones y comunidades.

En general, está claro que el panorama de las amenazas evoluciona y cambia constantemente, y diariamente surgen nuevas formas híbridas de ciberdelincuencia. Por tanto, es imperativo que las organizaciones de todo el mundo se mantengan vigilantes ante estas amenazas, actualizando continuamente sus protocolos de seguridad y sus prácticas como corresponda. Conforme avanzamos en este año 2023 y en adelante, será crucial para las empresas grandes y pequeñas aplicar soluciones globales de ciberseguridad que les ayuden a protegerse del gran volumen de ciberataques tradicionales y de los nuevos métodos híbridos que los agentes maliciosos están creando por todo el mundo.

Con el mandato de reducir el impacto mundial de la ciberdelincuencia y proteger a las comunidades para lograr un mundo más seguro, las actividades esenciales de la Dirección de Ciberdelincuencia de INTERPOL están previniendo, detectando, investigando y desarticulando la ciberdelincuencia. A fin de conseguirlo, y ofrecer un mejor apoyo a los países miembros para que comprendan las ciberamenazas a nivel nacional, regional y mundial, la información y los datos sobre ciberdelincuencia deben ser recopilados, tratados, analizados y evaluados.

Como parte de estos esfuerzos, me complace presentar la segunda edición de la Evaluación de las ciberamenazas en África elaborado por la Oficina de Operaciones contra la Ciberdelincuencia en la región africana ("Oficina Africana").

El presente informe aporta un profundo análisis y reflexiones sobre el panorama de las ciberamenazas más recientes en países miembros de la región africana. Conforme avanza la tecnología, avanzan los métodos utilizados por los delincuentes para aprovechar las vulnerabilidades en las redes y sistemas. En los últimos años, los estados africanos han sufrido un aumento en ciberataques dirigidos a infraestructuras críticas, entidades financieras y otras organizaciones que son cada vez más dependientes de los servicios digitales.

Debemos reconocer que la cooperación internacional entre las fuerzas del orden es esencial para cualquier estrategia que busque contrarrestar y combatir la ciberdelincuencia. Los ciberdelincuentes están cada vez más organizados y utilizan métodos más sofisticados, por lo que se requiere un esfuerzo mundial coordinado para garantizar que se haga frente a las amenazas de forma adecuada.

Trabajar juntos con nuestros 195 países miembros y utilizar metodologías coordinadas a nivel regional y nacional puede ayudar a mejorar los resultados de las investigaciones, pues se facilitaría el intercambio

de inteligencia sobre nuevas amenazas y de buenas prácticas en técnicas de investigación. Asimismo, se utilizaría de la mejor forma posible la tecnología para mejorar las capacidades.

Además, deben fomentarse las operaciones conjuntas siempre que sea posible, puesto que ayudan a crear confianza entre los países miembros participantes, permitiéndoles a la vez aprender de la experiencia de los demás en el abordaje de amenazas similares.

Asimismo, es importante que las fuerzas del orden trabajen en estrecha colaboración con organizaciones del sector privado, pues a menudo estas pueden aportar inteligencia valiosa sobre nuevas ciberamenazas, ofrecer programas de formación para el personal y compartir conocimientos técnicos con los que no cuentan las entidades gubernamentales. Colaborar con el sector privado permite a las fuerzas del orden utilizar bases de datos policiales y poderes legislativos que les permiten dar una respuesta rápida a las amenazas antes de que causen un daño o un impacto importante.

Con el objetivo de proteger a las economías y comunidades digitales en la región africana, este informe también destaca las estrategias y presenta una vía de actuación para la región.

Además de abarcar la Ciberdelincuencia Persistente y Avanzada como ransomware, phishing, troyanos bancarios, y stealer malware, el informe contiene un análisis de varios tipos de estafas y fraudes cibernéticos. Tan pronto como se detectaron estos tipos de delitos, la Oficina Africana pudo dirigir acciones sobre el terreno contra los ciberdelincuentes implicados desarrollando un plan de acción que implicaba a múltiples jurisdicciones y coordinando operaciones conjuntas (nombres en clave Falcon II y Delilah).

Un apoyo operativo intensificado y mejorado, y el intercambio de inteligencia de forma proactiva, posibilitará un mejor apoyo para los países miembros, de una forma que refleje las necesidades y los desafíos únicos en esta región.

El propósito del presente informe es ayudar a mejorar la comprensión del panorama regional de las ciberamenazas, a fin de ofrecer una respuesta priorizada y dirigida a las amenazas de la ciberdelincuencia a través de los canales de INTERPOL.

Agradecemos a los países miembros de la región africana y a nuestros socios su sólido compromiso en este proyecto. Apreciamos profundamente su dedicación, su gran esfuerzo y su perseverancia en la promoción de esta causa.



Craig Jones
Director, Dirección de Ciberdelincuencia
INTERPOL

PRÓLOGO

A finales de los años 1990, los pioneros del acceso a internet en África se conectaban utilizando satélites geoestacionarios. Solamente unos pocos privilegiados tenían acceso a internet. Veinte años más tarde, todos los países del continente están conectados a la red mundial a través de cables submarinos o terrestres, satélites e incluso mediante drones y globos. El 25 % de la población africana subsahariana tiene acceso permanente a internet, comparado con el 60 % de la población en el Norte de África, mientras que de media sólo el 50,8 % de la población mundial está conectada a la internet.

Hay 37 países africanos que han establecido fondos destinados al acceso universal para ampliar la cobertura nacional de internet, lo que ha llevado al continente africano a tener una de las mayores tasas de crecimiento de la conectividad del mundo. No obstante, como con cualquier nueva tecnología, el desarrollo de internet ha conllevado un aumento de la ciberdelincuencia. Los delitos dependientes de internet y los delitos facilitados por internet afectan ya a todos los sectores de actividad. Las nuevas tendencias implican colaboración entre formas tradicionales de delincuencia y la ciberdelincuencia. Por ejemplo, los grupos terroristas pueden recurrir a los servicios de ciberdelinquentes para recaudar fondos utilizando criptodivisas, y las redes de trata de personas exploran la web oscura para aprender cómo diseñar documentos de viaje falsos. Estas nuevas tendencias en la delincuencia organizada impiden disociar la lucha contra la ciberdelincuencia de la lucha contra todas las otras formas de delincuencia.

Un segundo hecho alarmante es que dos años después de la pandemia de COVID-19, las secuelas todavía se dejan sentir en el continente africano, particularmente por la pérdida de puestos de trabajo, con sectores totalmente arruinados como la hostelería, el turismo y la aviación. Además, los métodos de trabajo han evolucionado desde la COVID-19 y algunos empleados prefieren ahora trabajar de forma remota, lo que abre una vía a ataques tipo phishing y BEC.

El nivel de sensibilización general sobre la amenaza de la ciberdelincuencia es muy real en el continente africano. Iniciativas como campañas de sensibilización y conferencias regionales y continentales, así como campos de formación y programas de desarrollo de capacidades, son cada vez más frecuentes en los últimos años. Como parte de esta política de respuesta a la ciberdelincuencia, AFRIPOL organizó del 21 al 23 de septiembre de 2022 la primera sesión de su Campo de formación sobre investigación de la ciberdelincuencia, incluyendo phishing, malware, OSINT, la red oscura y criptodivisas. En esta primera sesión hubo 136 participantes de 22 países.

AFRIPOL está satisfecha con su colaboración con INTERPOL, que sigue siendo nuestro socio principal. Trabajamos juntos a través del Programa de apoyo de Interpol a la Unión Africana en relación con AFRIPOL (ISPA). El año 2022 fue particularmente fructífero para esta colaboración, con la ejecución de numerosos proyectos: Africa Cyber Surge, la compra de dispositivos digitales de triaje SPEKTOR y formación para siete países, la adquisición de doce licencias CHAINALYSIS y formación para los países beneficiarios, y la compra de aproximadamente veinte licencias de las herramientas CYBERBELT y formación para los países beneficiarios.

Otras asociaciones fructíferas, con la Policía Federal Alemana a través de GIZ y con el Ministerio británico de Asuntos Exteriores, de la Commonwealth y de Desarrollo, también han posibilitado la realización de numerosos proyectos, como Network of Excellence in Forensics y el primer Campo de formación sobre Ciberdelincuencia. Para 2023 están previstos muchos proyectos a gran escala, con el próximo lanzamiento del nuevo centro de datos y bases de datos forenses de AFRIPOL, y el establecimiento de una Unidad de Análisis de Información Policial.

Cuanto más progresamos en la lucha contra la ciberdelincuencia, más nos damos cuenta de que esta lucha es costosa y de que debemos unir recursos. Existen enormes disparidades entre los países africanos. Algunos cuentan con expertos altamente cualificados y laboratorios de investigación equipados con herramientas modernas, mientras que otros sólo están empezando a desarrollar marcos legislativos y jurídicos básicos para combatir la ciberdelincuencia. El principio sagrado de la solidaridad que impera en la Unión Africana implica la necesidad de un enfoque global ante este problema, y que los avances sean beneficiosos para todos.

Por tanto, a partir de ahora AFRIPOL está centrando el elemento operativo de su lucha contra la ciberdelincuencia en los siguientes tres ejes:

1. Formación con tecnologías sin derechos de propiedad y sin licencia cuando el costo de licencias caras no permite que las unidades de lucha contra la ciberdelincuencia respondan con celeridad.
2. Crear un fondo para la lucha contra la ciberdelincuencia con contribuciones de todos los socios interesados en este ámbito, para financiar la compra conjunta de licencias y equipos con el fin de reducir costes y la logística.
3. Reforzar la colaboración con el sector privado a fin de armonizar y normalizar los procedimientos y las tecnologías, y con fines de recopilación de inteligencia por todo el continente.

África se está poniendo rápidamente al día en términos de conectividad; una espada de doble filo que crea a la vez oportunidades de desarrollo y amenazas para la seguridad de las personas y de sus propiedades. Asimismo, está claro que la internet ha borrado las fronteras en todo el mundo. Un ciberataque con origen en África puede alcanzar un blanco en cualquier lugar del mundo. Por ello, debemos crear una respuesta común ante esta lacra mundial de la ciberdelincuencia. Las capacidades de defensa y lucha tienen que nivelarse entre los países africanos y el resto del mundo. Esto puede lograrse a través de una completa armonización mundial de los procedimientos, las tecnologías y los programas de formación.

Finalmente, esperamos que en 2023 podamos alcanzar nuestros objetivos y coordinemos mejor las acciones de las fuerzas del orden.



Embajador Jalel CHELBA
Director Ejecutivo en funciones
AFRIPOL

ABBREVIATIONS AND ACRONYMS

| | |
|--------------|--|
| AFJOC | African Joint Operation against Cybercrime |
| BEC | Business E-mail Compromise |
| CERTs | Computer Emergency Response Teams |
| CII | Critical Information Infrastructure |
| CnC | Command and Control server |
| CARs | Cyber Activity Reports |
| DDoS | Distributed Denial-of-Service |
| DNS | Domain Name System |
| EU | European Union |
| FBI | Federal Bureau of Investigation |
| HTTPS | Hypertext Transfer Protocol Secure |
| IGCI | INTERPOL Global Complex for Innovation |
| IP | Internet Protocol |
| IRC | Internet Relay Chat |
| OSINT | Open-Source Intelligence |
| P2P | Peer-to-Peer |
| PoS | Point-of-Sale |
| PPP | Public Private Partnerships |
| RATs | Remote Access Tools |
| SMEs | Small and Medium-sized Enterprises |
| SSL | Secure Sockets Layer |

AGRADECIMIENTOS

This assessment report was written by the Africa Cybercrime Operations Desk under the aegis of the African Joint Operation against Cybercrime (AFJOC), and funded by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO). INTERPOL's Support Programme for the African Union (ISPA) also contributed to this report, with the support of the German Federal Foreign Office.

This report is based on assessments of information provided to INTERPOL by the relevant Member Countries and INTERPOL's private partners, including Group-IB, Kaspersky, Shadow Server, and Trend Micro.



RESUMEN

En un mundo globalizado, en el que las economías están cada vez más interconectadas y la tecnología avanza a un ritmo sin precedente, la amenaza de la ciberdelincuencia plantea un grave peligro para los gobiernos, negocios y ciudadanos. La variedad y complejidad de los ataques han crecido exponencialmente en los últimos años, y los delincuentes utilizan nuevos métodos de infiltración para acceder a datos confidenciales y a información sensible.

Mientras esta tendencia continúa, los riesgos para la seguridad de todas las organizaciones aumentan considerablemente, lo que supone un coste incalculable para la economía mundial.

Un artículo publicado por el Centro para la Ciberseguridad del Foro Económico Mundial¹ afirmaba que «cerca de la mitad de los negocios están viéndose afectados por la delincuencia financiera, siendo la ciberdelincuencia la amenaza más grave».

La ciberdelincuencia se ha convertido en una industria de muchos miles de millones de dólares, y para los grupos delictivos tradicionales es tentador pasar sus actividades al ciberespacio o incluso cometer ciberdelitos utilizando herramientas sofisticadas y tácticas evolutivas, lo que significa que tanto las organizaciones como las personas deben mantener al día las medidas de protección. Se sabe que los ciberdelincuentes han estado implicados en actividades como explotación de contraseñas débiles, ocultación de identidad mediante servidores proxys, robo de información confidencial de negocios y gobiernos, usurpación de identidad y ataques de ransomware.

Los gobiernos de todo el mundo han reconocido la amenaza que plantea la ciberdelincuencia y continúan invirtiendo importantes recursos para proteger a sus ciudadanos en línea. Las fuerzas del orden han desarrollado tácticas eficaces como el desarrollo de capacidades, el rastreo de los orígenes de malware y el establecimiento de buenas prácticas en materia de ciberseguridad para las organizaciones. Además, muchos países están trabajando juntos a través de mecanismos internacionales como el Marco Operativo Conjunto de INTERPOL con miras a mejorar el intercambio de información relacionada con la ciberdelincuencia.

A pesar de estas medidas tomadas por las fuerzas del orden y los gobiernos de todo el mundo, los ciberdelincuentes siguen yendo un paso por delante.

Los ciberdelincuentes aprovechan las vulnerabilidades en los sistemas de protección a fin de acceder a información sensible o activos financieros, y esto tiene como resultado la pérdida anual de miles de millones de dólares.

Un buen ejemplo son las estafas BEC (Business Email Compromise), una forma transnacional de ciberdelincuencia cada vez más presente que no requiere unas habilidades técnicas sofisticadas, pero con capacidad de provocar pérdidas monetarias enormes.

Solamente en los Estados Unidos de América, el Centro de Denuncias de Delitos en Internet (IC3) informó haber recibido cerca de 20 000 quejas por estafas BEC en 2021, con pérdidas estimadas de unos 2 400 millones USD.

La Oficina Federal de Investigación informó de pérdidas asombrosas por estafas BEC, alcanzando más de 43 000 millones USD a nivel mundial, con un incremento del 65 % entre 2019 y 2021, probablemente debido a la pandemia de COVID-19, que forzó a muchas personas a realizar sus actividades de forma virtual.

Incluso sin el efecto de la pandemia de COVID-19, se espera que el volumen y la persistencia de estos ciberataques sigan aumentando.

Los ciberdelincuentes no conocen límites a la hora de compartir recursos e intercambiar conocimientos, lo que, en parte, les permite prosperar. Del mismo modo, unirnos aún más mediante el intercambio de información y asesoramiento profesional puede ser nuestra mejor baza para combatir la frustrante amenaza planteada por la ciberdelincuencia.

Con miras a reducir el impacto mundial de la ciberdelincuencia y proteger a las comunidades creando un mundo más seguro, los organismos deben mantenerse informados de estas nuevas tendencias y desarrollar medios innovadores para darles respuesta. Hacer esto en el momento oportuno frustrará posibles actividades delictivas y disuadirá de antemano a posibles perpetradores.

Con datos procedentes de los países miembros de INTERPOL, socios privados e investigación realizada por la Oficina de Operaciones contra la Ciberdelincuencia en la región africana, este informe de 2022 ofrece un completo panorama de las tendencias de la

¹ Centro para la Ciberseguridad del Foro Económico Mundial (<https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/>)

ciberamenaza en la región africana. Estas son algunas de las ciberamenazas más importantes identificadas en el informe, y esta tendencia continúa en la región africana:

- Los **ataques BEC (Business Email Compromise)** siguen siendo los más frecuentes, con importantes pérdidas para los negocios. Es un método muy económico y de bajo riesgo para los ciberdelincuentes, pero con grandes ganancias. Los ciberdelincuentes responsables de estafas BEC son cada vez más sofisticados y utilizan herramientas de alta tecnología para perpetrar sus actividades fraudulentas.
- Los **ataques de phishing** son una preocupación creciente en África por la rápida adopción y uso de tecnologías digitales. El número de personas que utilizan los servicios y aplicaciones en línea va en aumento, así como su vulnerabilidad ante ataques de phishing.
- Los **ataques de ransomware**, en los que los ciberdelincuentes toman como blanco gobiernos, comercios e instituciones públicas, están aumentando con rapidez. Han estado dirigidos a infraestructuras críticas, incluyendo a los sectores de la energía y el transporte.
- Los **troyanos bancarios y los stealers** plantean una nueva e inminente amenaza a compradores en línea, y dañan la confianza en los pagos en línea. Es fácil obtener varios tipos de troyanos y stealers en foros clandestinos, lo que facilita a los ciberdelincuentes lanzar sus ataques maliciosos. Además, las funcionalidades van evolucionando, lo que dificulta aún más la labor de investigación de las fuerzas del orden.
- Las **estafas en línea** son cada vez más frecuentes por la mejora de la accesibilidad a internet. Este problema se agrava por los bajos niveles de cultura digital de las víctimas. Esto las convierte en un blanco fácil para los ciberdelincuentes que las atraen con falsas promesas que finalmente tendrán un coste financiero para ellas.
- La **ciberextorsión** todavía tiene que controlarse: va unida a la proliferación de internet y las tecnologías móviles, de forma que hay más personas susceptibles de recibir exigencias de pagos y sufrir extorsión.
- El **crimeware como servicio** es cada vez más popular en África dada su facilidad de uso, asequibilidad y falta de consecuencias a causa de los marcos jurídicos débiles para la aplicación de la ley en temas de ciberdelincuencia. Ofrece a

los delincuentes una forma sencilla de llevar a cabo ataques de carácter financiero contra sistemas y negocios vulnerables con un esfuerzo mínimo y pocos conocimientos técnicos.

Es importante señalar también que el mayor acceso a la tecnología viene acompañado de un mayor riesgo de ser víctima de estos tipos de delitos, por lo que es esencial que tanto ciudadanos como organizaciones se mantengan vigilantes en sus actividades digitales. Además, los organismos regionales encargados de la aplicación de la ley deben estar mejor equipados con los instrumentos y conocimientos necesarios para detectar, investigar, y enjuiciar a los responsables de estos actos maliciosos y, si fuese necesario, deben colaborar con socios internacionales como INTERPOL a nivel mundial.

Con el mandato de reducir el impacto mundial de la ciberdelincuencia y proteger a las comunidades para lograr un mundo más seguro, la Oficina de INTERPOL de Operaciones contra la Ciberdelincuencia en la región africana, como parte del proyecto de AFJOC, tiene por objetivo utilizar esta evaluación de amenazas como base para impulsar acciones coordinadas y basadas en inteligencia contra la ciberdelincuencia y sus perpetradores en países miembros africanos.

Los esfuerzos colectivos para intercambiar inteligencia y elaborar un marco operativo conjunto fortalecerán considerablemente las capacidades regionales y la capacidad para luchar contra la ciberdelincuencia. La cooperación entre gobiernos, fuerzas del orden, empresas privadas e instituciones académicas es clave para aprovechar todos los volúmenes de datos y recursos disponibles, que podrán utilizarse posteriormente para elaborar estrategias más eficaces en la lucha contra la ciberdelincuencia.

La eficacia de estas operaciones conjuntas ya se ha comprobado en la reciente operación África Cyber Surge, coordinada por la Dirección de Ciberdelincuencia de INTERPOL y el Programa de apoyo de INTERPOL a la Unión Africana (ISPA) en colaboración con AFRIPOL.

Además de mejorar el intercambio de inteligencia, INTERPOL tiene el firme compromiso de desarrollar las habilidades y capacidades regionales que necesitan las fuerzas del orden de todo el continente para investigar eficaz y correctamente casos de delincuencia basada en tecnología.

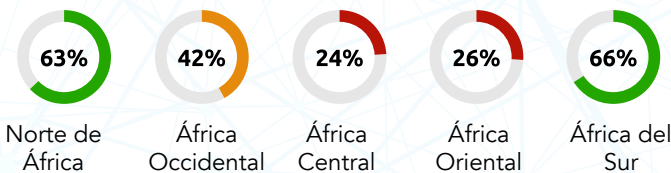
1. DESARROLLO DIGITAL ACTUAL EN LA REGIÓN AFRICANA

África es una región increíblemente diversa, pasando de paisajes desérticos a exuberantes islas tropicales. Alberga la segunda mayor población del mundo y es una de las regiones con más diversidad cultural del planeta. Cuenta también con una gran riqueza en recursos naturales como petróleo y gas, oro y diamantes, estaño y cobre, uranio, bauxita y muchos otros minerales. Estos son algunos de los elementos impulsores del crecimiento económico en África, junto a industrias como el sector agroindustrial, la manufactura y el turismo.

África cuenta con gran cantidad de tierra cultivable que permite a muchos países tener una importante base agrícola que contribuye con un cuarto de su PIB.



La manufactura ha ido adquiriendo un papel cada vez más importante en el desarrollo de África en los últimos años. El creciente enfoque en la producción de valor añadido ha dado como resultado un aumento significativo de la inversión extranjera directa, creando empleos e impulsando las economías locales en muchos puntos de la región.



El PIB combinado de la región² se ha quintuplicado, y más, en sólo 20 años, desde 695 880 millones USD en 2002 a 2,98 billones USD en 2022. La región africana es uno de los mayores mercados

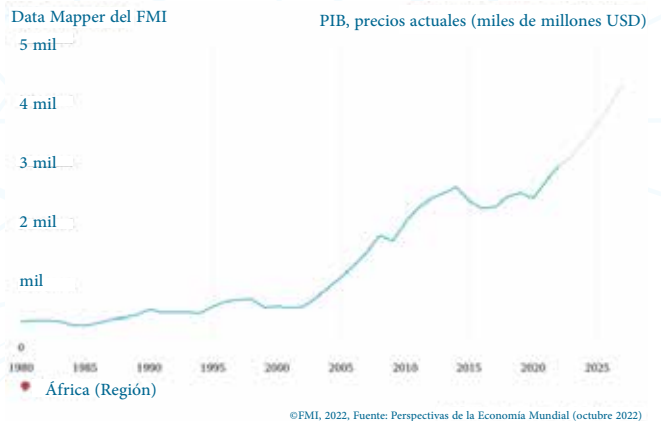
del mundo, y se prevé que sobrepase los 4 billones USD para 2027.

La tasa de penetración de internet en África es relativamente alta comparada con las tasas mundiales.

Según el Global Digital Report 2022,³ la tasa media de penetración de internet en África es aproximadamente de un 44 %.

Ha estado aumentando rápidamente en los últimos años y no da muestras de ralentizarse. Algunos países africanos están realizando importantes inversiones financieras en infraestructuras y acceso digital. Además, muchos países están desplegando la cobertura 5G por sus respectivos territorios, amplificando así este aumento.

Cabe también resaltar que la mayoría de este crecimiento puede atribuirse al uso de internet móvil (y no conexiones fijas), por su conveniencia y asequibilidad. Las redes móviles son cada vez más fiables en la mayoría de los países africanos, por lo que es más fácil mantenerse conectado en línea y acceder a servicios como el comercio electrónico y las plataformas de los medios sociales.



Además, muchos gobiernos en África están tomando medidas para que todos tengan acceso a las herramientas digitales y puedan beneficiarse de las nuevas oportunidades ofrecidas por un entorno digital en continua evolución. Por ejemplo, la Unión Africana lanzó la Estrategia Nacional de Transformación Digital para África (2020-2030),⁴

² PIB (actual) en USD. Fuente: Fondo Monetario Internacional

³ 2022 Digital Global Report (www.wearesocial.com)

⁴ The Digital Transformation Strategy For Africa 2020-2030 (https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf)

cuyo objetivo es proveer conexión internet a todos los ciudadanos de África para 2030, así como fomentar las capacidades digitales y personales inclusivas en varios campos como cifrado, programación, análisis, seguridad, blockchain, herramientas de aprendizaje automático, inteligencia artificial, robótica, ingeniería, innovación, emprendimiento y políticas y normativas en el ámbito de la tecnología.

Por otra parte, la penetración media de los medios sociales en la región africana es aproximadamente de un 27 %, con una mayor proporción de usuarios de medios sociales activos en las regiones del norte y sur de África (56 % y 45 % respectivamente).

La región africana está experimentando un crecimiento y desarrollo sin precedentes en el sector de la tecnología digital, particularmente en las tecnologías financieras y el comercio electrónico. Esto ha provocado el aumento de la demanda de internet y de servicios de banda ancha, convirtiéndose en uno de los mercados más competitivos del planeta. Una multitud de inversores de todo el mundo están rivalizando para capitalizar esta oportunidad. Sin embargo, la mayor dependencia de las infraestructuras en línea ha traído consigo también una serie de amenazas que pueden causar graves problemas.

La transformación digital de África es un fenómeno creciente. Muchos países del continente han aprovechado los avances de la tecnología moderna para impulsar su crecimiento económico, así como para aumentar el acceso a servicios esenciales. Conforme las tecnologías digitales se extienden por el continente, las naciones africanas comienzan a adoptarlas e integrarlas en sus economías. Este proceso de transformación digital ha estado facilitado por diversos factores, incluyendo la mayor disponibilidad de datos e información, un mejor acceso a internet, el surgimiento de start-ups y organizaciones innovadoras, una infraestructura mejorada para la comunicación y el comercio, e iniciativas gubernamentales dirigidas a la promoción de la inversión digital.

Recientemente, muchos países africanos han realizado notables progresos incorporando la transformación digital. Etiopía, por ejemplo, ha aplicado estrategias facilitadas por la tecnología⁵ como NRLAIS (National Rural Land Administration Information System), que ha ayudado a mejorar la eficacia en el sector agrícola. En Kenia, empresas tecnológicas como Microsoft están ayudando a agricultores a utilizar datos para que sus prácticas agrícolas sean más eficaces. Ruanda también se ha unido a la transformación digital con iniciativas que forman parte de su Smart City Rwanda Masterplan.⁶

5 Digital Ethiopia 2025 (<https://www.pmo.gov.et/media/other/b2329861-f9d7-4c4b-9f05-d5bc2c8b33b6.pdf>)

6 Smart City Rwanda Masterplan (https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Strategies/Smart_City_Rwanda_Masterplan.pdf)

2. REFLEXIONES SOBRE LAS TENDENCIAS DE LAS CIBERAMENAZAS EN ÁFRICA EN 2022

Utilizando datos de países miembros de INTERPOL en la región africana y socios privados, y de investigaciones llevadas a cabo por la Oficina de Operaciones contra la Ciberdelincuencia en la región africana, esta sección analizará en profundidad las amenazas y tendencias en ciberdelincuencia, así como las motivaciones subyacentes.

La Oficina de Operaciones contra la Ciberdelincuencia en la región africana identificó algunas de las principales ciberamenazas en 2022. Estas tendencias en las amenazas a las que se enfrentan los países miembros, en la región africana continúan.

Business Email Compromise (BEC)

Business Email Compromise (estafa a empresas por e-mail mediante suplantación de identidad) es un tipo de ciberataque con el que agentes maliciosos obtienen acceso no autorizado a la cuenta de correo electrónico de una organización y luego la utilizan para enviar mensajes fraudulentos a sus socios empresariales con el fin de obtener beneficios financieros. Estos correos a menudo contienen enlaces o documentos adjuntos maliciosos que, al pinchar en ellos, pueden instalar malware en el dispositivo del receptor o proporcionar al atacante acceso a información confidencial. Además de enviar correos electrónicos, los perpetradores también pueden manipular conversaciones existentes de correo electrónico y eliminar correos importantes como solicitudes de pago con información de cuentas bancarias. Las estafas BEC pueden causar importantes pérdidas económicas y dañar la reputación de una organización.

Phishing

Phishing es un tipo de ciberataque que los agentes maliciosos llevan a cabo para robar a víctimas desprevenidas información sensible como nombres de usuario, contraseñas e información de tarjetas de crédito. Los phishers utilizan típicamente correos electrónicos o sitios web falsos con apariencia legítima para lograr que las personas proporcionen información personal. También pueden hacer uso de tácticas de ingeniería social como spoofing, usurpación de identidad y ataques de malware para acceder a datos confidenciales. Los ataques de phishing pueden causar importantes daños económicos e incluso ser utilizados para la usurpación de identidad.

Ransomware

Ransomware es una forma maliciosa de software que impide el acceso de los usuarios a sus propios datos, sistemas y dispositivos mediante el cifrado de los ficheros. Una vez que el proceso de cifrado se completa, la víctima recibe un mensaje informándoles de que debe abonar una cierta cantidad de dinero (normalmente en bitcoin u otra criptomoneda) para que los archivos sean descifrados y vuelva a tener acceso a ellos. Este tipo de ataque ha ganado popularidad entre los ciberdelincuentes por la facilidad de generar rápidamente grandes beneficios con un esfuerzo mínimo: en muchos casos un atacante puede llevar a cabo con éxito un ataque de ransomware simplemente enviando un único correo electrónico. El ransomware también puede difundirse a través de anuncios maliciosos en sitios web y medios sociales, así como en descargas maliciosas en sitios web.

Troyanos bancarios y stealers

Los troyanos bancarios y los stealers son programas de software maliciosos diseñados para robar información sensible como nombres de usuario, contraseñas, y datos financieros a víctimas desprevenidas. Estos troyanos pueden instalarse a través de correos electrónicos de phishing, sitios web maliciosos, descargas ocultas u otros medios. Una vez que el troyano está instalado en el ordenador de una víctima, intenta acceder a cuentas bancarias en línea capturando pulsaciones del teclado o robando credenciales de acceso. También puede modificar páginas web en el navegador con el fin de redirigir cualquier transferencia de fondos a la cuenta de los delincuentes y no a la del destinatario deseado. Los troyanos bancarios a menudo se utilizan junto a otras herramientas de malware como spyware y rootkits para extenderse con más rapidez en una red o sistema.

Con el tiempo, los troyanos bancarios son cada vez más sofisticados, utilizando técnicas avanzadas como ataques de Man-in-the-Browser por los que los atacantes manipulan las transacciones sin ser detectados.

Estafas en línea

Las estafas cometidas por medios electrónicos son los fraudes más comunes y peligrosos y ocurren a nivel internacional. Los fraudes cometidos por medios electrónicos pueden definirse como cualquier delito fraudulento realizado a través de un ordenador o utilizando datos informáticos.

Ciberextorsión

La ciberextorsión es un tipo de ciberdelincuencia por la que el delincuente utiliza métodos digitales para amenazar o extorsionar a las víctimas pidiendo dinero y/u otros activos. Con frecuencia el atacante amenaza con revelar información personal incómoda, eliminar datos importantes, sabotear los sistemas y redes o lanzar ataques DDoS.

Crimeware como servicio

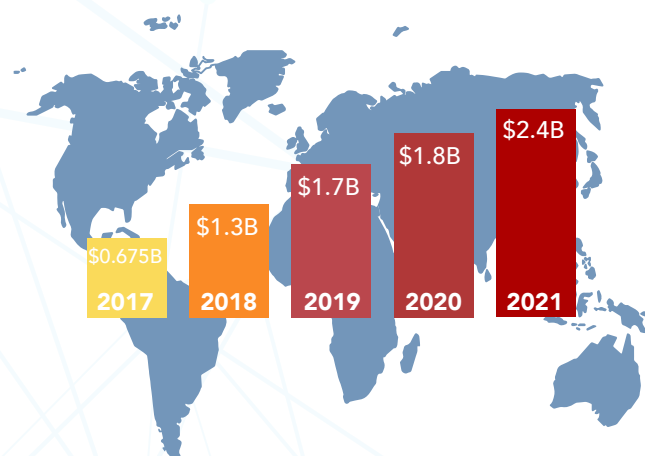
Crimeware como servicio es cualquier programa informático o conjunto de programas diseñados para facilitar actividades ilícitas en línea. Ofrece, entre otros servicios, los de spyware, kits de phishing, secuestradores de navegador y keyloggers I.

2.1 Business Email Compromise

Por séptimo año consecutivo, los ataques BEC han sido la ciberamenaza más devastadora económicamente de todo el mundo. Solamente el año pasado, las empresas de los Estados Unidos perdieron la abrumadora suma de 2 400 millones USD⁷ a causa de estos ataques, lo que representa un aumento del 28 % con respecto a 2020 y un enorme incremento de más de 500 millones de dólares. Esta cifra es un recordatorio alarmante de lo potentes y dañinos que pueden ser los ataques BEC para negocios de todos los tamaños.

Además de causar importantes pérdidas económicas, las estafas BEC también pueden dañar la reputación de una organización si los clientes llegan a saber que han sido víctimas de esta actividad maliciosa.

PÉRDIDAS DE EMPRESAS ESTADOUNIDENSES POR ESTAFAS BEC



Se ha comprobado que muchos de los perpetradores de estafas BEC están ubicados en África Occidental, aunque desafortunadamente para sus víctimas, sus ataques no están limitados por fronteras geográficas. A menudo, estos delincuentes tienen conexiones con redes delictivas más amplias de todo el mundo, lo que les permite atacar a un gran número de víctimas a escala mundial. Sin duda, es un hecho indiscutible que los mismos perpetradores responsables de las estafas BEC también lo son de muchos otros tipos de ciberdelincuencia.

Estos ciberdelincuentes son cada vez más sofisticados y han encontrado formas para evitar ser detectados por las fuerzas del orden, por ejemplo, utilizando múltiples cuentas de correo electrónico y enviando fondos a través de cuentas bancarias internacionales y empresas fantasmas. También ocultan sus actividades utilizando canales de comunicación cifrados como aplicaciones de chat o foros en la web oscura. Todo esto hace aún más difícil para las fuerzas del orden seguirles la pista, especialmente cuando están distribuidos por diferentes países o jurisdicciones.

Es más, algunos estafadores incluso colaboran con «mulas» que ayudan a blanquear el dinero a través de una serie de empresas fantasmas y cuentas bancarias extraterritoriales. Esto les permite guardar el anonimato y los sitúa donde las autoridades no pueden llegar.

⁷ Informe sobre delincuencia en internet 2021, FBI (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)

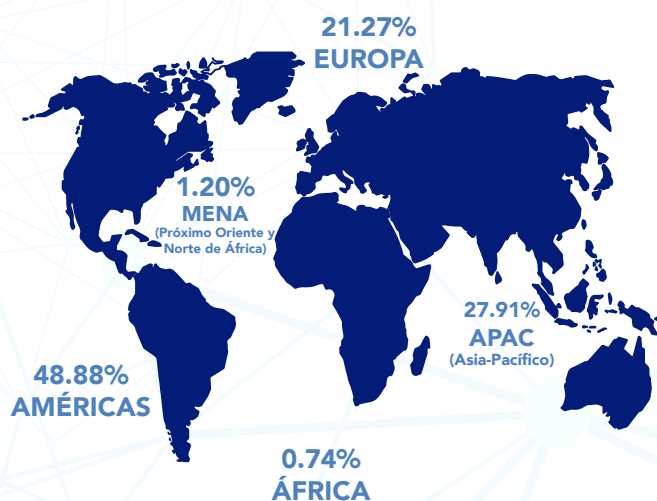
En respuesta a la alta concentración de perpetradores de estafas BEC detectada en la región nigeriana, la Oficina de INTERPOL de Operaciones contra la Ciberdelincuencia en la región africana, junto a sus socios privados Group-IB, Palo Alto Networks y Trend Micro, y la policía de Nigeria, lanzaron una exitosa operación en mayo de 2022: «Operación Delilah».⁸ El propósito de esta operación era desarticular un grupo dedicado a perpetrar estafas BEC conocido como «SilverTerrier» o «MT» y esto condujo a la detención del jefe de un grupo de ciberdelincuencia transnacional.

El equipo responsable de esta operación también identificó con éxito a individuos claves que estaban directamente implicados en la comisión de estos ciberdelitos. Esto redujo significativamente su capacidad de continuar con las actividades delictivas. Además, se obtuvieron pruebas esenciales que llevaron a la identificación y el decomiso de fondos robados, así como documentos incriminatorios y dispositivos digitales utilizados por miembros de la red delictiva.

A esta acción proactiva de aplicación de la ley le siguió otra operación, cuyo nombre en clave es «Killer Bee»⁹, basada en inteligencia recibida de un socio del sector privado, Trend Micro. Esta operación dirigida por INTERPOL dio como resultado la detención de tres perpetradores de estafas BEC nigerianos, tras una exhaustiva investigación por parte de la Comisión contra los Delitos Económicos y Financieros de Nigeria. Se piensa que estos hombres utilizaron un troyano de acceso remoto (RAT) para desviar operaciones financieras y robar información confidencial de conexión en línea de organizaciones corporativas como compañías de petróleo y gas en el Sudeste Asiático, Próximo Oriente y Norte de África.

La eficacia de las operaciones «Delilah» y «Killer Bee» en el desmantelamiento de actividades BEC en Nigeria pone de relieve la importancia de que las fuerzas del orden internacionales como INTERPOL y los organismos locales encargados de la aplicación de la ley como la policía de Nigeria y la Comisión contra los Delitos Económicos y Financieros colaboren para luchar exitosamente contra las redes

de delincuencia organizada que operan en el país. Estos esfuerzos conjuntos proporcionan un apoyo adicional para hacer frente a estas complejas redes de ciberdelincuencia, ofreciendo una capa más de protección para los ciudadanos frente a varias formas de fraudes y actividades maliciosas en línea. Trend Micro también señaló que los ataques de los ciberdelincuentes se dirigen cada vez más a otras regiones, particularmente a aquellas con mayores concentraciones de objetivos de alto valor, donde el impacto económico es mayor.



INTENTOS DE ESTAFAS BEC POR REGIÓN (2021 – MAYO DE 2022)

FUENTE: TREND MICRO

La región africana también ha sido víctima de ataques BEC en los últimos años. Las pérdidas económicas y las perturbaciones en los negocios causadas por ciberataques siguen aumentando.

A pesar de que los países africanos representan solamente un 0,75 % de los intentos de ataques BEC a nivel mundial entre 2021 y mayo de 2022, los datos de Trend Micro revelan que Sudáfrica contabilizaba más de la mitad de los casos BEC denunciados en la región durante el mismo periodo.

La amenaza de los ataques BEC se ha agudizado particularmente en la región africana por la rápida transición a una economía cada vez más digitalizada. El continuo aumento de usuarios dependientes de la tecnología para las transacciones diarias, ofrece más oportunidades para que los agentes maliciosos

⁸ Presunto jefe de banda de ciberdelincuencia detenido en Nigeria, mayo de 2022. (<https://www.interpol.int/News-and-Events/News/2022/Suspected-head-of-cybercrime-gang-arrested-in-Nigeria>)

⁹ Estafas en línea: detención de tres nigerianos durante la operación «Killer Bee» de INTERPOL, mayo de 2022. (<https://www.interpol.int/en/News-and-Events/News/2022/Online-scamming-fraud-three-Nigerians-arrested-in-INTERPOL-Operation-Killer-Bee>)

se aprovechen de organizaciones vulnerables. Además, muchas partes de África adolecen de medidas de ciberseguridad eficaces, lo que incrementa aún más el riesgo de sufrir ataques BEC.

Otro factor que contribuye al aumento de estos ataques por toda África es la falta de prácticas básicas de ciberseguridad en las empresas que operan en el continente. Muchas organizaciones no cuentan con políticas adecuadas para gestionar los protocolos de control de acceso, los procesos de autenticación o las normas de cifrado, poniéndose por tanto en una posición vulnerable ante los ataques, con sus sistemas no protegidos y sus cuentas de usuario con contraseñas débiles. Esto significa que, aunque los empleados detectasen correos electrónicos fraudulentos enviados por estafadores, seguiría sin haber un medio para que pudieran protegerse contra la amenaza que se plantea –financiera u operativa– ya que desde el principio no existen las defensas apropiadas.

Una de las características más comunes de los ataques BEC en África es el uso por parte de los estafadores de técnicas de ingeniería social. Estos agentes maliciosos aprovechan sus conocimientos de la cultura y lengua regional. Suplantando la identidad de alguien conocido por sus víctimas y crean una sensación de urgencia o pánico, llevando a las víctimas a satisfacer las peticiones que aparecen en el correo electrónico sin comprobar su legitimidad.

Datos estadísticos de los 22 países miembros en la región africana muestran que en 2021 se denunciaron 399 casos de ataques BEC ante las fuerzas del orden.

Un análisis de los datos relacionados con casos de ataques BEC en la región africana ayudaría a perfilar una imagen más exacta de la situación. Desafortunadamente, está cada vez más claro que un número importante de casos de ataques BEC no se denuncian en esta zona, lo que empeora el panorama.

Esta falta de notificación también afecta a la capacidad de las fuerzas del orden para enjuiciar adecuadamente a los delincuentes implicados y asignar recursos de una forma más eficaz para hacer frente a este tipo de ciberdelincuencia.

Así las cosas, es fundamental sensibilizar al público para que los negocios denuncien cualquier amenaza de ataque BEC que puedan sufrir. Esta valiosa información relacionada con operaciones BEC puede entonces ser recopilada por las fuerzas del orden de toda África y, posteriormente, utilizarse para conocer mejor esta tendencia delictiva y aplicar las medidas necesarias para combatirla.

2.2 Phishing

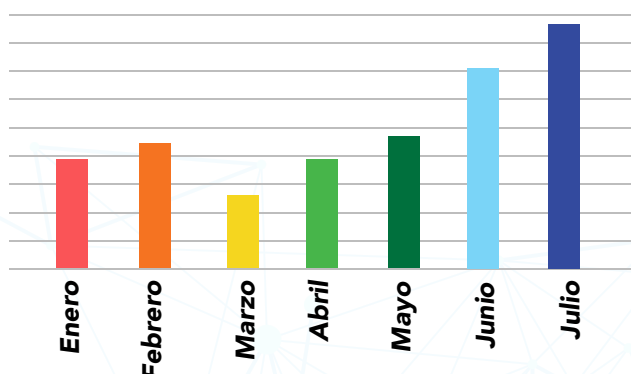
Phishing es una de las ciberamenazas más antigua y generalizada que existe. Se estima que hasta el 90 % de las violaciones de la seguridad de los datos¹⁰ están relacionados con ataques de phishing exitosos, siendo una de las principales causas de robo de credenciales de acceso e información. Las técnicas de phishing son cada vez más sofisticadas y los perpetradores aprenden a seleccionar a sus víctimas con más precisión. Los atacantes pueden elaborar mensajes que parecen provenir de fuentes de confianza como bancos, gobiernos o incluso amigos y miembros de la familia. Estos mensajes típicamente contienen enlaces o documentos maliciosos que pueden dirigir a las víctimas a sitios web o archivos maliciosos que contienen virus o malware.

Además de robar las credenciales de acceso, el objetivo último de los ataques de phishing es frecuentemente obtener acceso a datos confidenciales, entre otros, información financiera, contraseñas e información de contacto. Una vez obtenida, esta información puede utilizarse para lograr un beneficio económico y/o para usurpar la identidad, vendiéndose en mercados de la web oscura o utilizándose para otros propósitos maliciosos como extorsión, o para dar impulso a otros tipos de actividades relacionadas con la ciberdelincuencia. Todo esto hace del phishing un peligro considerable, no solamente por las pérdidas económicas potenciales, sino también por el daño causado por las otras formas de ciberdelincuencia que pudieran resultar de un ataque exitoso.

Con los avances tecnológicos y técnicas cada vez más complejas, phishing sigue siendo una amenaza constante para las organizaciones y particulares. Los atacantes utilizan tácticas de ingeniería social como usurpación de identidad y tácticas de intimidación para aumentar sus posibilidades de

¹⁰ Informe de CISCO sobre amenazas para la ciberseguridad 2021 (<https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list>)

Detección de objetos de phishing por Kaspersky entre enero y julio de 2022



éxito. Además, herramientas automatizadas como los spam-bots han facilitado el envío de grandes cantidades de correos electrónicos o mensajes, aumentando así las posibilidades de éxito.

Todos estos factores unidos llevan a un nivel de riesgo continuo y sin precedente asociado a ataques de phishing, lo que los convierten en una de las ciberamenazas más peligrosas de la actualidad.

Entre enero y julio de 2022, Kaspersky informó de la alarmante detección de 15 769 298 objetos phishing en África. La mayoría de estas actividades maliciosas se realizaron mediante correos electrónicos o páginas web utilizando un popular método de ingeniería social conocido como phishing.

Group-IB identificó la alarmante cifra de 1 352 412 URLs de phishing entre enero y agosto de 2022 en la región africana. Se trata de un serio motivo de preocupación en materia de seguridad, pues los ataques de phishing pueden tener resultados devastadores para los particulares y las organizaciones, a los que les puede coger desprevenidos.

Una de las estafas de phishing más generalizadas en África son las falsas promociones de aniversario. Los responsables fingen ser una marca bien conocida, como las aerolíneas etíopes, a fin de persuadir a personas confiadas a rellenar una breve encuesta o cuestionario, ofreciéndoles un regalo si lo hacen. Una vez que la persona ha introducido sus datos, se les pide que difundan el mensaje a cinco grupos de WhatsApp o a 20 amigos antes de que puedan recibir el obsequio. Desafortunadamente, estos estafadores utilizarán esta oportunidad para recopilar información personal e incluso

información sobre el dispositivo de aquellos que inadvertidamente cumplen sus exigencias.

La estafa por falsa promoción de aniversario es solamente un ejemplo de lo potentes y eficaces que pueden ser los ataques de phishing para delincuentes en busca de un beneficio rápido a expensas de víctimas inocentes. Los correos electrónicos con estafas phishing son cada vez más complejos en cuanto a diseño y contenido, por lo que cada vez es más difícil detectarlos para una persona promedio. Es más, se sabe que los delincuentes han utilizado tácticas de ingeniería social para que parezcan más auténticos. Por ejemplo, muchos estafadores crean cuentas de correo electrónico falsas utilizando nombres de dominio similares a nombres de empresas legales con el fin de aumentar sus posibilidades de éxito al dirigirse a usuarios desprevenidos. Con frecuencia, las víctimas piensan que están interactuando con un representante genuino de la empresa que está siendo suplantada.

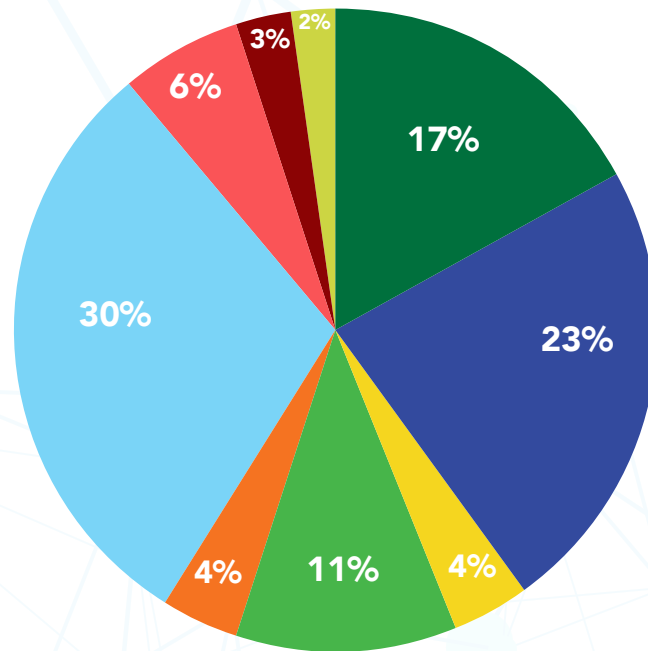
Para empeorar las cosas, faltan campañas de sensibilización y educación. Los ciudadanos no están debidamente informados sobre estos tipos de estafas, ni disponen de recursos ni orientaciones sobre cómo protegerse de las ciberamenazas. La falta de conocimiento sobre ciberhigiene en África hace que las personas sean aún más vulnerables, y facilita a los perpetradores de estos delitos lanzar campañas de phishing exitosas sin ser detectados ni perseguidos por las autoridades locales.

El último¹¹ informe publicado por el Grupo de trabajo de lucha contra el phishing revela que el sector financiero, que incluye a los bancos, seguía siendo el principal blanco de los ataques de phishing, con un 23 % de todos los ataques. El número de ataques contra proveedores de webmail y software como servicio se mantuvo igual, mientras que los ataques contra sitios de minoristas/comercio electrónico disminuyeron a un 4 %, desde un 14,6 %.

La proliferación de ataques de phishing puede atribuirse a la relativa facilidad con la que las personas pueden introducirse en este tipo de actividad delictiva. En parte, esto se debe a la disponibilidad de phishing como servicio en el

11 Informe de la APWG sobre la actividad de phishing – 3er trimestre de 2022 (<https://apwg.org/trendsreports/>)

Sector más afectado, 3T 2022



30% Otros

23% Instituciones financieras

17% SAAS / Webmail

11% Medios sociales

6% Logísticas / Envíos

4% Comercio electrónico / Minoristas

4% Pagos

3% Telecomunicaciones

2% Criptodivisas

mercado oscuro. Por tan solo 20 USD, se puede comprar un kit de phishing que lleva todo el material necesario para lanzar un ataque exitoso. Además, se ofrecen tutoriales en vídeo donde se muestra cómo utilizar y montar el kit. Asimismo, existen paquetes de servicios posventa con actualizaciones regulares que impiden que los correos electrónicos utilizados para cometer el delito sean detectados por soluciones modernas de protección en internet. Por tanto, está al alcance de personas sin conocimientos técnicos lanzar sus propios ataques de phishing con un esfuerzo mínimo.

En sus investigaciones, Group-IB también identificó una publicación en un foro en la XSS en la que se anunciaba la venta de páginas de phishing para dirigir ataques a bancos. Entro los bancos enumerados estaba BIC, un banco portugués/angoleño con numerosas sucursales en todo el mundo. En la publicación se jactaban de que por una módica suma cualquiera podía adquirir las páginas de phishing y acceder a cuentas de usuarios.

Esta facilidad de acceso ha dado como resultado un aumento en la actividad de phishing en los últimos años. Los kits a menudo contienen fragmentos

de código y scripts escritos por desarrolladores experimentados que permiten a los usuarios alojar sus sitios web sin necesidad de conocimientos sobre cómo funciona el alojamiento de sitios web. Además, incluyen herramientas contra la detección y plantillas ya hechas para diseñar correos electrónicos eficaces que puedan eludir los filtros de spams y llegar a las bandejas de entrada de las víctimas sin ser detectados. Esto implica que las personas que realizan este tipo de actividad delictiva ni siquiera necesitan tener los conocimientos de codificación básicos ni ninguna habilidad técnica. Cualquier persona con acceso al mercado negro y con unos pocos dólares puede convertirse en un ciberdelincuente de nivel profesional casi instantáneamente.

Si bien se han detectado numerosos ataques maliciosos de phishing en la región africana, el número de notificaciones a las fuerzas del orden es mucho más bajo de lo esperado. En 20 países de África, sólo ha habido 2087 notificaciones. Esta discrepancia puede atribuirse a varios factores que van desde la incorrecta clasificación de los casos a una falta de sensibilización pública en cuanto a la forma de notificar estos delitos.

En África, de los 42 países analizados, 24 países comunicaron que todavía tienen que crear alguna plataforma o mecanismo en línea para que el público pueda notificar casos de ciberdelincuencia. Estas carencias dificultan la capacidad de las fuerzas del orden para detectar y dar una respuesta adecuada a los ciberataques. En consecuencia, a menudo estos sucesos no se denuncian o se ignoran por completo.

2.3 Ransomware

El número de ataques de ransomware ha estado aumentando drásticamente en los últimos años, y actualmente están considerados como una de las amenazas más graves a la que se enfrentan organizaciones de todos los tamaños y de todo el mundo. Los ciberdelincuentes utilizan este software malicioso para tomar el control de los sistemas empresariales críticos de la organización, codificar sus datos y exigir pagos a cambio de devolver el acceso. Estos ataques pueden ser extremadamente onerosos para los negocios, pues se acumulan las pérdidas económicas ocasionadas por el tiempo de inactividad y por los esfuerzos de recuperación.

El número de ataques de ransomware no parece estar ralentizándose y se espera que en 2023 aumenten los costes asociados a estos ataques. Una de las principales empresas de investigación y edición, Cybersecurity Venture¹², estima que los costes mundiales del ransomware alcanzarán los 265 000 millones USD para 2031.

Las empresas afectadas por ataques de ransomware también sufren un importante daño a su reputación. Los datos de los clientes pueden hacerse públicos o ser robados durante estos ataques, poniendo así en peligro la fiabilidad de la empresa a ojos de los clientes y de otras partes interesadas.

Según el informe de IBM «Costes de una brecha de datos 2022»¹³, el coste medio total de un ataque de ransomware era considerablemente mayor que el coste medio de una brecha de la seguridad de los datos, ascendiendo los ataques de ransomware a la alarmante cifra de 4,54 millones USD comparada con la ya costosa de 4,35 millones USD por una brecha de la seguridad de los datos. La proporción

de brechas causadas por ransomware creció en un 41 % el año pasado y se tardó 49 días más que la media en ser identificadas y contenidas.

3x aumento en la proporción que pagó rescates de 1 millón USD o más

21% rescates pagados de menos de 10 000 USD

812 360 USD pago medio para el rescate (excluyendo casos atípicos)

FABRICACIÓN, SERVICIOS pago medio de rescate más elevado (2 millones USD)

ATENCIÓN SANITARIA pago medio de rescate más bajo (197 000 USD)

FUENTE: SOPHOS STATE OF RANSOMWARE 2022

Esto queda igualmente patente en la «Situación del ransomware 2022», de Sophos¹⁴, que encontró que las organizaciones de tamaño medio pagaron rescates promedio aún más elevados: 812 360 USD por ataque. Estos costes pueden desglosarse en varios componentes como tiempo de inactividad y tiempo del personal requerido para las actividades de mitigación, el coste de los dispositivos (reemplazo o reparación de hardware afectado), costes de red (restauración de las redes o los servicios), oportunidades perdidas por los retrasos en las operaciones y pagos de rescate realizados por las organizaciones llegado el caso.

¹² Costes a nivel mundial de los daños causados por ransomware (<https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/13>)

¹³ Cost of a Data Breach Report 2022 (<https://www.ibm.com/reports/data-breach>)

¹⁴ The State of Ransomware 2022 (<https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf>)

El Departamento del Tesoro estadounidense¹⁵ también ha informado que los bancos estadounidenses trataron aproximadamente 1 200 millones USD en pagos de rescate en 2021. Esto supone muchísimo más dinero de lo que la mayoría de los piratas informáticos jamás hubiese esperado conseguir cuando desarrollaron los primeros ransomware hace décadas. Con tales incentivos económicos, es posible que este aumento en el uso de ransomware continúe a menos que se tomen medidas significativas para combatirlo, pues este tipo de delito requiere poco esfuerzo, está en gran parte automatizado, el riesgo de ser descubierto es bajo y los beneficios son grandes.

Según Shadowserver, los datos recopilados de sitios víctima de ataques ransomware en el periodo de enero a septiembre de 2022 indica que víctimas africanas están siendo el blanco de una amplia variedad de familias de ransomware. Durante este periodo, la familia de ransomware más frecuente fue Lockbit2.0, que contabilizaba aproximadamente el 38,8 % de todas las infecciones en África. Le seguía de cerca Pysa con un 14,3 %, y después Lockbit 3.0 con un 8,2 %. Otras familias destacables de ransomware en este periodo fueron Conti, HiveLeaks, Midas y BlackByte (4,1 %, cada una).

No debe subestimarse el impacto de otros programas maliciosos. Todas estas amenazas pueden perturbar significativamente las operaciones empresariales mediante el cifrado de datos o sistemas, con los consiguientes elevados pagos de rescate y tiempos de inactividad mientras las organizaciones luchan por recuperar los ficheros afectados. Además, la proliferación de los casos de ransomware ha provocado un alarmante aumento de las actividades de ciberdelincuencia con motivaciones financieras por toda África.

Shadowserver informó también que Sudáfrica es la nación que más ataques de ransomware recibe, con un 42 % de todos los ataques detectados. Le sigue Marruecos con un 8 %, y Botsuana y Egipto con un 6 %. Tanzania y Kenia contabilizan un 4 % cada una de los ataques de ransomware detectados. Este alto nivel de actividades maliciosas en Sudáfrica es motivo de preocupación, y sugiere que el número de actividades de ransomware no detectadas en el país es aún mayor.

La mayoría de estas actividades maliciosas puede haber estado facilitada por sistemas obsoletos y soluciones de protección ineficaces que dejan lagunas que los ciberdelincuentes pueden aprovechar. La falta de normativa y legislación en materia de ciberdelincuencia también puede estar contribuyendo al aumento de los ataques de ransomware. Sin normas ni orientaciones claras sobre cómo protegerse ante estas amenazas, muchas organizaciones quedan expuestas a la explotación por parte de los ciberdelincuentes.

Según Trend Micro, el ransomware supone el 1,4 % de toda la ciberdelincuencia detectada en el mundo entre enero y julio de 2022. Sin embargo, la amenaza del ransomware en la región africana es muy real, detectándose un número importante de estos casos. No obstante, cabe señalar que los porcentajes fueron menores tanto en el primer como en el segundo trimestre de 2022 comparado con 2021. Esta disminución puede deberse a diferentes factores. Uno de ellos puede ser el pico en el número de detecciones en marzo. Parece ser que este pico estuvo causado principalmente por un gran número de detecciones de ransomware Conti en Túnez. Trend Micro señala que el cierre de esta familia de ransomware puede ser la causa de la importante caída en el número de detecciones en abril.

Otro informe de Trend Micro reveló que los cinco sectores atacados con más frecuencia son organismos gubernamentales, educación, energía, comercio minorista y bienes de gran consumo. En otro informe se señalaba que las infraestructuras críticas, incluyendo atención sanitaria y transporte, también fueron objeto de ataques.

La protección de los datos y las herramientas para crear copias de seguridad han ido mejorando considerablemente, por lo que las tácticas tradicionales de ransomware son cada vez menos eficaces. Cuando una organización tiene una copia de seguridad de sus datos bloqueados, no necesita desembolsar el pago del rescate solicitado por los ciberdelincuentes. En consecuencia, los perpetradores se han visto obligados a ser más creativos y han desarrollado formas de extorsión doble y triple con ransomware.

¹⁵ Observaciones del Secretario adjunto del Tesoro (<https://home.treasury.gov/news/press-releases/jy1067>)

DETECCIÓN DE RANSOMWARE



FUENTE: TREND MICRO

Lo último ha sido el desarrollo de ransomware como servicio. Los ciberdelincuentes alquilan versiones de ransomware desarrolladas previamente que pueden utilizarse para llevar a cabo ataques. Gracias a la disponibilidad de ransomware como servicio, realizar ataques de ransomware exitosos es más fácil que nunca y los atacantes ya no necesitan tener conocimientos técnicos avanzados y experiencia. Además, a causa de su escalabilidad y flexibilidad, este tipo de servicio facilita mucho a los atacantes dirigirse a numerosas víctimas a la vez. Es más, los atacantes pueden ajustar fácilmente sus técnicas dependiendo de qué funcione mejor en cada caso, pues pueden cambiar rápidamente de una versión a otra del malware. Todas estas características hacen que el ransomware como servicio sea aún más peligroso, ya que no es necesario que los atacantes tengan habilidades o infraestructuras altamente complejas para llevar a cabo ataques exitosos.

Los datos compartidos por 42 países en la región africana mostraron que solamente se habían denunciado 59 casos de ransomware ante las fuerzas del orden en 11 países africanos. Se piensa que la situación actual es incluso peor, pues muchas personas y negocios no quieren denunciar estos casos a la policía. Se piensa que solo se da a conocer un pequeño porcentaje de los casos de ransomware.

Las razones para no notificar un ataque de ransomware pueden ser el miedo de que los datos que han sido cifrados pierdan su valor, o no querer que los clientes sepan que sus datos se han visto comprometidos –una preocupación mucho más seria para los negocios. Con frecuencia, las víctimas permanecen en silencio y pagan el rescate discretamente, mientras que los atacantes no siempre publican los datos de redes comprometidas.

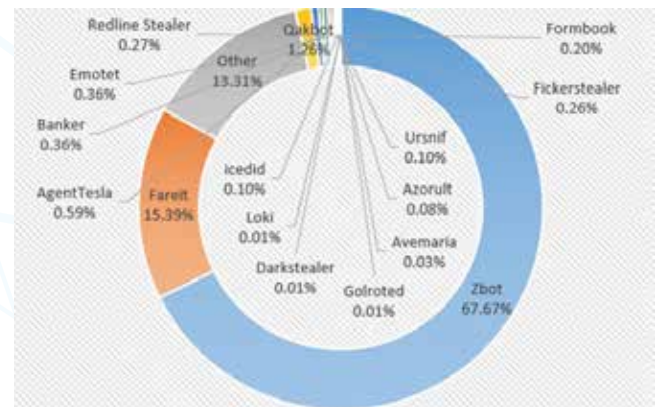
2.4 Troyanos bancarios y stealers

La región africana está pasando por un periodo de gran actividad en el sector de la tecnología digital, particularmente en tecnología financiera y comercio electrónico. Este crecimiento se debe al mayor acceso a internet y a una penetración del móvil mejorada, lo que permite a las personas acceder a servicios que anteriormente no estaban disponibles. Esto ha abierto nuevas oportunidades para el crecimiento de los negocios y la expansión de sus operaciones por todo el continente.

Sin embargo, este rápido crecimiento también facilita ataques con software malicioso como los troyanos bancarios o stealers, que representan una de las mayores amenazas para la seguridad de las personas y de las infraestructuras informáticas de las organizaciones por su potencial para causar un daño generalizado si no se detecta con prontitud. Los troyanos bancarios y stealers pueden instalarse de forma manual o remota utilizando técnicas de ingeniería social como correos electrónicos con enlaces o archivos adjuntos maliciosos. Una vez instalados, los troyanos bancarios y stealers recopilan información personal de un ordenador infectado y comunican los datos robados a través de internet a un servidor remoto controlado por el atacante. Los ciberdelincuentes pueden utilizar la información obtenida para robar dinero directamente a la víctima, o vender la información en mercados clandestinos.

Tal como revelan las detecciones de Trend Micro, Marruecos es el país africano más afectado, con 18 827 detecciones. Sudáfrica le sigue de cerca con 6 560 detecciones de software malicioso. También se detectaron casos de software malicioso en Nigeria, 5 366, Camerún, 1 462, y Argelia, 691. Los informes también han puesto de relieve que los malwares de troyanos bancario y stealers más frecuentes son Zbot y Fareit. El primero representa el 67,67 % de todas las detecciones en la región, mientras que el segundo representa un 15,39 %. El uso de ambos programas de software maliciosos ha aumentado en los últimos años, afectando a particulares y a negocios africanos.

Tanto Zbot como Fareit son difíciles de detectar y, por tanto, a menudo consiguen robar información personal y financiera de sus víctimas antes que estas se den cuenta de que ha habido un ataque, causando grandes pérdidas.



Otro malware stealer al que hay que prestar atención en la región africana es RedLine Stealer. La investigación de Group-IB ha puesto de manifiesto que sólo entre enero y agosto de 2022, se adquirieron 5 862 188 cuentas comprometidas localizadas en IPs africanas utilizando RedLine Stealer.

Se ha demostrado que este malware stealer se distribuye normalmente a través de juegos pirateados, aplicaciones y servicios, con la intención de robar información sensible como datos del navegador, monederos de criptodivisas y credenciales de acceso de aplicaciones de usuarios de conocidos programas como FileZilla, Discord, Steam, Telegram y VPNs.

Los troyanos bancarios y stealers son una amenaza real en África que debe tomarse en serio para proteger a los ciudadanos de pérdidas económicas resultantes del robo de fondos o la usurpación de identidad. Los ciudadanos marroquíes son particularmente vulnerables ante los troyanos bancarios, tal como demuestran los altos niveles de software malicioso detectados en el país. No obstante, los ciudadanos de otros países africanos deben estar también atentos y mantener las medidas de protección en línea actualizadas para evitar posibles ataques. Es importante señalar que estas cifras no incluyen casos de fraude que no han sido detectados ni denunciados. El daño real infringido por los troyanos bancarios puede ser mucho mayor de lo que indican estos datos. Los bancos y las entidades financieras tienen que aplicar medidas para proteger a los clientes de la ciberdelincuencia, como estafas de phishing e infecciones con malware, pero los particulares también deben ser conscientes y mantenerse alertas cuando utilizan internet para operaciones financieras. Mantener los dispositivos actualizados,

con el software de protección anti-virus/malware más reciente puede ser una primera línea de defensa contra amenazas como los troyanos bancarios. Sin embargo, los usuarios deben utilizar también contraseñas que sean únicas y difíciles de conseguir para los atacantes a fin de lograr una protección óptima. Finalmente, se necesita un esfuerzo colectivo entre bancos, organismos gubernamentales y usuarios para contener la oleada de la ciberdelincuencia causada por los troyanos bancarios en África.

2.5 Estafas en línea y extorsión

Las estafas en línea incluyen una amplia variedad de actividades fraudulentas en el entorno digital. Estafas de pagos por adelantado y pedidos que no se entregan, estafas en compras, estafa sentimental por internet, extorsión sexual, estafas de asistencia técnica y estafas con criptodivisas están entre las más frecuentes y son cada vez más comunes en la región africana.

En las estafas de pagos por adelantado, los estafadores piden el abono de una suma antes de entregar la mercancía o el servicio. Normalmente, los delincuentes utilizan esta estrategia para cobrar tasas a particulares confiados y después desaparecen sin entregar la mercancía o el servicio. A fin de que parezca legítimo, los estafadores incluso pueden enviar documentos falsos o



pedir información personal como información de tarjetas de crédito, números de cuentas bancarias o direcciones de correo electrónico.

En las estafas en compras, los delincuentes intentan engañar a compradores en línea para que crean que están comprando productos genuinos a precios reducidos. En vez de estos productos, las víctimas reciben artículos falsificados o nada en absoluto. Los clientes pueden ser engañados fácilmente para que realicen un pago por adelantado sin darse cuenta de que están tratando con un falso vendedor.

Las estafas sentimentales por internet ocurren cuando los estafadores establecen una conexión afectiva con una persona confiada creando una falsa identidad en una plataforma de medios sociales



o en un sitio web de citas. Una vez ganada su confianza y obtener acceso a cuentas personales, el delincuente utiliza esta relación para solicitar dinero a la víctima con falsos pretextos, o para robar información sensible como contraseñas o información de cuentas bancarias.

La extorsión sexual es otro preocupante tipo de estafa en línea. Es una forma híbrida de estafa sentimental por internet, en la que los delincuentes chantajean a las víctimas amenazándolas con compartir imágenes o vídeos íntimos a menos que paguen un rescate.

Las estafas de asistencia técnica son un tipo de fraude en el que los delincuentes fingen ser representantes legítimos de empresas de tecnología que ofrecen asistencia técnica para obtener acceso a los ordenadores de los usuarios y extraer datos valiosos como contraseñas e información financiera. Los delincuentes pueden emplear diversas estrategias como llamadas no solicitadas, ventanas emergentes con publicidad, correos electrónicos falsos o mensajes automatizados diciendo que el ordenador del usuario está infectado con malware para convencer a la víctima de que permita el acceso remoto al sistema.

Las estafas con criptodivisas aprovechan la creciente popularidad de las criptodivisas como bitcoin y ethereum persuadiendo a los inversores a comprar

divisas falsas. También se ha visto que los estafadores de criptodivisas utilizan complejas tácticas como la creación de monederos y cambios falsos con el fin de robar a las víctimas desprevenidas.

Con miles de millones de usuarios y un uso diario disparado, las plataformas de medios sociales se han convertido en un blanco lucrativo para los ciberdelincuentes y estafadores.

Aunque la actitud de las personas con los medios sociales ha cambiado en los últimos años, su comportamiento no se ha adaptado al cambio. Muchos usuarios todavía funcionan con los mismos supuestos erróneos sobre cómo se trata su información personal, lo que les deja expuestos a la acción de agentes maliciosos. Los ciberdelincuentes utilizan tácticas engañosas como correos electrónicos de phishing o enlaces maliciosos para obtener acceso a cuentas de usuarios, robar datos sensibles o secuestrar cuentas para usurpar la identidad. Las estafas también son muy comunes en las plataformas de los medios sociales, desde ofertas de trabajo falsas a estafas piramidales y estafas de inversión. Desafortunadamente, estas estafas a menudo están dirigidas a aquellas personas que ya están pasando por problemas financieros y, por tanto, son incluso más vulnerables ante una pérdida económica y la angustia emocional. Los estafadores más entendidos incluso pueden jaquear



cuentas de usuario o crear cuentas falsas con el fin de enviar enlaces maliciosos o mensajes que contengan malware.

Los ciberdelincuentes también aprovechan las enormes audiencias de todo el mundo accesibles a través de estas plataformas creando estafas específicamente adaptadas a diferentes localizaciones. Esta táctica les permite difundir desinformación rápida y fácilmente, consiguiendo que las personas creen falsas noticias o inviertan en planes fraudulentos. Además, algunos agentes maliciosos explotan la naturaleza interactiva de los medios sociales suplantando a personalidades o empresas conocidas para aumentar su credibilidad y poder acceder a más víctimas.

Estos tipos de delitos en línea son particularmente prolíficos en la región africana por la falta de sensibilización sobre su existencia y la forma en la que operan. Con el rápido avance de la tecnología, puede resultar difícil para los particulares mantenerse al día en las últimas tendencias de la ciberdelincuencia e identificar los signos de peligro que le llevarían a ser víctima de estos delitos. Además, las personas que se enfrentan a dificultades financieras a menudo son más propensas a aceptar ofertas de estafadores, pensando que les están ofreciendo una salida a sus problemas económicos, cuando no es precisamente el caso. Por tanto, es importante que los gobiernos y las fuerzas del orden tomen medidas proactivas para educar a los ciudadanos sobre las diferentes formas de estafas en línea y la forma en la que operan, así como las medidas que los particulares pueden adoptar para protegerse.

Los efectos de este tipo de ciberdelincuencia pueden ser devastadores. Las víctimas no sólo pierden dinero, sino que también ven su vida arruinada y su identidad robada. Es más, este tipo de fraude a menudo se perpetra a escala internacional: los piratas informáticos pueden abrir fácilmente cuentas falsas en múltiples países que les permiten operar sin ser detectados, mientras perpetran sus delitos contra víctimas desprevenidas de todo el mundo. Por ello, es importante que los usuarios se mantengan vigilantes en sus actividades en línea y eviten así convertirse en víctimas. También es importante que las empresas de medios sociales tomen medidas proactivas para proteger a sus usuarios ante estas actividades maliciosas. Para

ello, deben aumentar las medidas de protección de forma que se cierren fisuras en sus sistemas que los delincuentes pudieran explotar.

Si bien estos ciberdelitos parecen estar orquestados desde la ingeniería social, los investigadores de Trend Micro identificaron 7,7 millones de detecciones web maliciosas. La mayoría de estas detecciones estaban relacionadas con sitios web fraudulentos (40,31 %). También informaron de que las estafas por extorsión siguen siendo un método generalizado de ciberataque por todo el mundo. De los países africanos estudiados, el 69,24 % (13 002) de los planes de extorsión detectados ocurrieron en Marruecos.

Según la distribución mundial de spams de extorsiones detectadas por Trend Micro, el 2,44 % de las direcciones IP emisoras estaban geolocalizadas en Sudáfrica, el 2,13 % en Marruecos, el 0,94 % en Kenia y el 0,91 % en Túnez, sugiriendo que estos servidores estaban comprometidos o formaban parte de una botnet utilizada para actividades maliciosas como campañas de extorsión. Es muy probable que los atacantes hayan aprovechado vulnerabilidades en estos servidores para tomar el control y llevar a cabo actividades maliciosas como la difusión de malware y ataques de phishing. En respuesta al panorama de la ciberdelincuencia en constante evolución, las comunidades mundiales de las fuerzas del orden y de la ciberseguridad han creado una alianza para proteger al público.

Aprovechando los conocimientos de esta alianza, INTERPOL ha lanzado varias campañas mundiales de sensibilización (#YouMaybeNext (el próximo puede ser usted), #JustOneClick (solo un clic), #OnlineCrimelsRealCrime (la ciberdelincuencia es una delincuencia real)) para mantener el nivel de sensibilización sobre cómo los ciberdelincuentes intentan explotar, robar datos, cometer estafas en línea o simplemente perturbar el mundo virtual.

2.6 Crimeware como servicio

El modelo del crimeware ofrecido como un servicio es algo de lo que los expertos en ciberseguridad, las comunidades de las fuerzas del orden y otras partes interesadas implicadas en la protección digital siempre han sido conscientes. Este modelo ha permitido a los ciberdelincuentes ofrecer sus códigos maliciosos como un «servicio» a otros

delincuentes, que los utilizan para infectar ordenadores, robar datos y, finalmente, ganar dinero con sus actividades ilícitas.

Esta forma de actuar de la delincuencia clandestina ha revolucionado la manera en la que operan los ciberdelincuentes, permitiéndoles un acceso fácil a herramientas y servicios difíciles de encontrar como botnets, ransomware como servicio, y recursos para ataques DDoS. Además, al pasar a ser un modelo empresarial, estos delincuentes están mejor organizados y pueden mejorar sus capacidades técnicas y sus márgenes de beneficio.



Al ofrecer crimeware como servicio, los ciberdelincuentes proporcionan ahora acceso a una amplia gama de variantes de malware a un precio asequible. La facilidad con la que pueden adquirirse o suscribirse a estos servicios, o incluso utilizarlos con un modelo de «pago por uso», les posibilita desplegar rápidamente malware a escala mundial sin necesidad de ningún conocimiento técnico especializado. Estos servicios también permiten a los atacantes mantener el anonimato, pues la mayoría de los proveedores garantizan el anonimato a lo largo de la transacción.

Mientras que las operaciones tradicionales de la ciberdelincuencia a menudo están limitadas por límites geográficos o conexiones lentas a internet, que pueden limitar el acceso o afectar seriamente a los plazos de entrega, los nuevos modelos de crimeware como servicio que utilizan tecnologías de computación en la nube han cambiado totalmente esta dinámica, posibilitando el rápido despliegue de paquetes de crimeware en minutos desde cualquier lugar del mundo. Esto reduce significativamente los costes de explotación para los delincuentes y, a la vez, les facilita seleccionar a víctimas con más rapidez y eficacia que antes.

Este enfoque también elimina gran parte del riesgo asociado con los métodos tradicionales de adquirir malware. Como todas las transacciones se realizan en línea utilizando criptodivisas o métodos de pago similares, las probabilidades de ser descubiertos se reducen considerablemente. Esto es un incentivo añadido para los delincuentes que buscan beneficiarse de las lucrativas oportunidades creadas por los modelos de crimeware como servicio sin preocuparse por ser detectados.

En general, el crimeware como servicio ha bajado el listón permitiendo la entrada de nuevos ciberdelincuentes con menos conocimientos tecnológicos. Al poder realizar complejos ataques sin necesidad de conocimientos técnicos avanzados, se facilitan las actividades maliciosas de los ciberdelincuentes. Los servicios de crimeware en los foros y mercados de la ciberdelincuencia en la web oscura están ampliamente anunciados como una solución económica. Ya se encuentran disponibles varios servicios. Se ofrece también como una opción óptima para atacantes avanzados que quieren realizar campañas relámpago.

Otro elemento que atrae a los ciberdelincuentes al crimeware como servicio, con miras a aventurarse en nuevos ámbitos o blancos, es la disponibilidad de datos robados que pueden utilizarse para realizar nuevas campañas.

| |  Kits de phishing |  Phishing-as-a-Service (PhaaS) |
|---------------------------------|---|--|
| Pago | Pago único | Basado en suscripciones (Disponible semanalmente, cada dos semanas, mensual o anual) |
| Modelos de correos electrónicos | ✓ | ✓ (Opcional) |
| Modelos de sitios | ✓ | ✓ |
| Envío de correo electrónico | | ✓ (Opcional) |
| Alojamiento de sitios | | ✓ |
| Robo de credenciales | | ✓ |
| Redistribución de credenciales | | ✓ |
| Redistribución de credenciales | | ✓ |

Comparación entre kits de phishing y phishing como servicio

FUENTE: Microsoft

El modelo de crimeware como servicio dificulta atribuir un delito a un individuo concreto porque los medios y la infraestructura se comparten entre varios agentes maliciosos o grupos delictivos. Lo que hace que este modelo sea particularmente peligroso es su papel como facilitador de ataques cada vez más sofisticados que impulsan el rápido desarrollo de nuevas amenazas más avanzadas.

Mediante combinaciones de varios servicios de ataques, los ciberdelincuentes también pueden desafiar eficazmente las capacidades de las fuerzas del orden para investigar y atribuir los ataques a determinados actores y grupos delictivos.

El phishing como servicio ofrece campañas de phishing automatizadas y de mayor duración, que pueden desplegarse con celeridad y de manera rentable. Sencillamente realizando un pago en bitc in por servicios botnet, innumerables m quinas infectadas con malware por todo el mundo pueden lanzar potentes ataques DDoS en blancos seleccionados, con la capacidad de red y duraci n del ataque deseada.

En los  ltimos a os, ha habido un crecimiento sin precedente en el n mero de ataques de ransomware, en gran medida debido a la disponibilidad de ransomware como servicio listo para ser utilizado. Esto permite a los usuarios llevar a cabo f cilmente m ltiples campa as sin tener que escribir ning n c digo. A trav s de sus portales en l nea de f cil uso, las plataformas de ransomware como servicio proporcionan servicios de apoyo y ofrecen cuotas bajas de suscripci n. Normalmente, se llevan entre el 20 % y el 40 % de cualquier rescate obtenido.

Este incremento en el uso de estas herramientas de ciberdelincuencia ha causado una oleada de actividades maliciosas en la web, as  como un incremento de las p rdidas asociadas a estos delitos. Adem s, es habitual que los delincuentes colaboren entre s  compartiendo conocimientos t cnicos y recursos mediante foros espec ficos, a fin de aumentar sus posibilidades de  xito al realizar diferentes tipos de ciberataques. Adicionalmente, algunos de estos servicios proporcionan inteligencia sobre amenazas; esto permite a los usuarios seleccionar determinadas organizaciones o segmentos de clientes para incrementar las posibilidades de  xito de una operaci n de phishing. Con la creciente facilidad para lanzar estos ataques y su rentabilidad, no sorprende que los piratas inform ticos contin en utilizando servicios de ransomware como servicio a pesar del riesgo que conlleva.

Dado este aumento de oferta de crimeware como servicio en foros de ciberdelincuencia y pirater a, especialmente aquellos alojados en la red oscura, es fundamental controlar dichas plataformas a fin de identificar nuevas amenazas con prontitud e intercambiar informaci n r pidamente para detectarlas y reducir los riesgos planteados por los ciberataques.

3. BRIEF OVERVIEW OF CYBER CAPABILITIES IN THE AFRICAN REGION

A fin de combatir eficazmente la ciberdelincuencia, las fuerzas del orden en la región africana necesitan mecanismos de ciberseguridad y de lucha contra la ciberdelincuencia robustos y bien estructurados. Contar con políticas, legislación y organismos puede aportar un nivel apropiado de respuesta a la amplia gama de ciberamenazas e incidentes a los que se enfrentan los países de todo el mundo. Esto debe ser una prioridad fundamental.

Los datos compartidos por los 42 países estudiados revelan que la mayoría de los países en la región africana cuentan con políticas, legislación y organismos adecuados en relación a la ciberdelincuencia como para aportar un nivel apropiado de respuesta a la amplia gama de ciberamenazas a las que se enfrentan los países de todo el mundo, concediendo a este asunto un considerable grado de prioridad.

No obstante, ocho de los países dijeron no poseer una unidad específica para los casos de ciberdelincuencia, y siete de los países afirmaron no tener la legislación necesaria sobre ciberdelincuencia.

Con una legislación débil sobre ciberdelincuencia –inexistente en algunos países– los delincuentes pueden operar con impunidad, porque aun siendo descubiertos no se les enjuicia ni extradita a países con leyes más estrictas.

Con miras a mantener el paso a la naturaleza evolutiva de la ciberdelincuencia y los actos delictivos dirigidos a sistemas informáticos, se recomienda encarecidamente que los países en la región africana continúen revisando la legislación sobre ciberdelincuencia existente y la mantengan al día con los últimos avances tecnológicos.

También se reconoce que las unidades específicas sobre ciberdelincuencia pueden tener el mayor impacto para ciudadanos y negocios en cuanto a prevención, detección, investigación y enjuiciamiento de casos de ciberdelincuencia. Ciertamente, para proporcionar un servicio visible al público y satisfacer sus expectativas y necesidades, una unidad específica de investigación de la ciberdelincuencia es una parte integral de cualquier respuesta gubernamental.

El creciente uso de la tecnología lleva de la mano un mayor riesgo de que los delincuentes hagan un mal uso de ella. Es un hecho ampliamente reconocido por todas las instituciones pertinentes. Si bien una mayoría de las fuerzas del orden en la región africana han establecido o reforzado unidades de ciberdelincuencia para hacer frente a este tipo de delito, está claro que siguen existiendo limitaciones en cuanto a capacidades dentro de estas unidades para abordar actos complejos de ciberdelincuencia. Es más, la región africana cubre una amplia zona geográfica, y hay pocas iniciativas para mejorar las capacidades de los investigadores de la ciberdelincuencia a nivel provincial y de distrito. En un entorno con una floreciente economía, existen varias opciones que las fuerzas del orden pertinentes en la región africana y otras partes interesadas gubernamentales pueden considerar. Una estrategia o un plan de acción sobre ciberdelincuencia integrado y coordinado puede ayudar a crear la visión, los objetivos y las prioridades necesarias para combatir mejor la ciberdelincuencia: directamente mediante la provisión de una respuesta de las fuerzas del orden, e indirectamente mediante el trabajo intergubernamental y el establecimiento de alianzas con los sectores público y privado, a nivel nacional e internacional, para crear un entorno cibernético resiliente y fiable.

El objetivo es evitar duplicar el trabajo realizado y abordar cuestiones como las relacionadas con el contenido y la regulación de internet, para proporcionar un marco estratégico propicio y duradero que permita examinar los retos y las oportunidades que se nos presentan y, finalmente, identificar áreas prioritarias en las que las naciones deben enfocar sus esfuerzos en cuanto a ciberseguridad y lucha contra la ciberdelincuencia en beneficio de todas las partes interesadas (como la prevención de la ciberdelincuencia y la promoción de buenas prácticas de ciberhigiene y de seguridad entre el público en general).

El ritmo de los casos de ciberdelincuencia y de los delitos facilitados por internet está aumentando a nivel mundial, y las fuerzas del orden de todo el mundo son conscientes de ello, a menudo realizando inversiones considerables y ampliando las unidades de investigación de la ciberdelincuencia.

A nivel de gestión, se reconoce que las unidades específicas sobre ciberdelincuencia pueden tener el mayor impacto para ciudadanos y negocios en la prevención, detección, investigación y enjuiciamiento de casos de ciberdelincuencia. Ciertamente, para proporcionar un servicio visible al público y satisfacer sus expectativas y necesidades, una unidad específica de investigación de la ciberdelincuencia es una parte integral de cualquier respuesta gubernamental.

Las fuerzas del orden deben considerar también invertir en la mejora de sus capacidades para combatir la ciberdelincuencia y los delitos facilitados por internet, y aumentar la eficacia de las divisiones/ unidades de investigación de la ciberdelincuencia y otras divisiones de investigación, por ejemplo:

- Revisar las capacidades de las unidades de investigación y de criminalística digital en materia cibernética;
- Facilitar el uso de herramientas como el análisis de Big Data y el rastreo de criptodivisas;
- Establecer relaciones externas con importantes entidades de la industria para mejorar el intercambio de información y de conocimientos;
- Desarrollar Procedimientos Operativos Normalizados (PON) para investigaciones y exámenes forenses;
- Centralizar herramientas de criminalística digital utilizando un modelo de centro de servicios que atienda a todas las partes de la organización policial, con beneficios en términos de transferencia de conocimientos y especialización individual, y mejoras en la eficiencia en términos de aprovisionamiento;
- En cuanto a la escalabilidad, debe crearse una plataforma de aprendizaje en línea con contenido sobre ciberdelincuencia y pruebas digitales.

La prevención siempre será la primera y mejor línea de defensa contra los ciberdelincuentes. Como con cualquier otra actividad delictiva, los más vulnerables tienden a ser los primeros blancos. La educación y la sensibilización contribuirán considerablemente a ayudar a los más vulnerables a protegerse contra muchos tipos de ciberdelincuencia.

Aunque la mayoría de los países en la región africana ha creado algún tipo de iniciativa de sensibilización y prevención de la ciberdelincuencia, diez de los países afirmaron no contar con ninguna iniciativa relacionada con la prevención de la ciberdelincuencia. Hay cabida de mejora en este ámbito para lograr mejores resultados.

Dado que gran parte de la población utiliza plataformas de medios sociales como Facebook, WhatsApp, Instagram, Twitter etc., también puede ser beneficioso disponer de una página específica en la que las fuerzas del orden puedan dar al público consejos para la prevención de la delincuencia y recopilar información sobre ciberdelitos.

4. PRÓXIMAS ETAPAS: ACCIÓN PROACTIVA CONTRA LAS CAMBIANTES CIBERAMENAZAS EN LA REGIÓN AFRICANA

Hemos considerado hasta ahora los distintos tipos de ciberamenazas y tendencias que constituyen un peligro para la región africana. Necesitamos un mayor nivel de sensibilización y comprensión de las amenazas a las que la región tendrá que enfrentarse en el futuro. Las estrategias en materia cibernética tienden a centrarse en medidas reactivas para prevenir ciberataques como ransomware, phishing, BEC y ataques de malware. No obstante, como los ciberdelincuentes principalmente operan, venden e intercambian conocimientos en la web oscura, las fuerzas del orden y los equipos corporativos de ciberseguridad deben ser proactivos en la recopilación y análisis de inteligencia externa sobre amenazas, y buscar estas ciberamenazas antes de que se produzcan los ataques.

La recopilación de inteligencia es una pieza vital del puzzle. INTERPOL apoya a sus países miembros en este ámbito para frenar con éxito el impacto de ciberamenazas en continua evolución, estableciendo capacidades como la Oficina de Operaciones contra la Ciberdelincuencia en la región africana. Esta oficina, apoyada por la Unidad de Ciberinteligencia de INTERPOL, intercambia inteligencia sobre ciberamenazas y coordina operaciones conjuntas que implican a entidades públicas y privadas. Saber cómo van a atacar los responsables de las amenazas y cuándo piensan hacerlo es crucial para impedir un ciberataque al comienzo de la Cyber Kill Chain.

En un mundo cada vez más digitalizado, cuanto antes sean los países conscientes de las amenazas, antes podrán tomar medidas para mitigar los riesgos y neutralizarlas.

Además, las fuerzas del orden deben mejorar sus esfuerzos colectivos en cuanto a intercambio de inteligencia e implementación de un marco operativo conjunto para combatir con éxito la ciberdelincuencia en la región africana.

Aunque las fuerzas del orden en la región africana han establecido buenas relaciones y acuerdos de cooperación bilateral para abordar formas tradicionales de la delincuencia, falta un marco operativo para hacer frente a la ciberdelincuencia. Con miras a mejorar la eficacia de las operaciones conjuntas intrarregionales e interregionales, la Oficina de Operaciones contra la Ciberdelincuencia en la región africana ha establecido un marco

operativo conocido como «Marco operativo conjunto para la mejora de la acción coordinada contra la ciberdelincuencia en la región africana».

Este marco guiará las operaciones dirigidas por INTERPOL con la comunidad de las fuerzas del orden en la región africana, estableciendo cómo formular, coordinar y comunicar operaciones conjuntas a fin de garantizar el intercambio eficaz y oportuno de información. El marco hace un llamamiento específico en pro de la cooperación efectiva entre comunidades de las fuerzas del orden, otras organizaciones internacionales e intergubernamentales, y el sector privado.

Con la elaboración de nuevas políticas y marcos legislativos en los países africanos, este marco será un documento evolutivo y, como tal, adoptará los nuevos avances a fin de seguir siendo relevante y mantenerse al día con las normas actuales regionales e internacionales.

5. CICLO DE PLANIFICACIÓN ANUAL DE LA OFICINA DE OPERACIONES CONTRA LA CIBERDELINCUENCIA EN LA REGIÓN AFRICANA

A fin de lograr su propósito, el Marco Operativo Conjunto en la Región Africana propone un ciclo de planificación anual de cuatro fases para la Oficina de Operaciones contra la Ciberdelincuencia en la región africana. El objetivo es promover un planteamiento coherente y metodológico para mejorar las operaciones coordinadas proactivas contra la ciberdelincuencia en la región.

Fase I – Recopilación y análisis

Esta primera fase se centra en un profundo análisis de la información sobre las ciberamenazas predominantes, las infraestructuras maliciosas y los responsables de las amenazas que operan en/contra la comunidad en la región africana. La Oficina de Operaciones contra la Ciberdelincuencia en la región africana utilizará inteligencia de las comunidades de las fuerzas del orden, 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, para elaborar el Informe sobre la 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 los países.

Fase II – Prioridades y estrategia

El Informe sobre la 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. África es una región diversa y cada país se enfrenta a sus propios desafíos. 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. Para finales de esta fase se tendrá una hoja de ruta regional preparada para su publicación, basada en una estrategia conjunta acordada y con resultados operativos claros para el año.

Fase III – Operaciones

La Oficina de Operaciones contra la Ciberdelincuencia en la región africana elaborará planes tácticos estándar (Standard Tactical Plans, STP) para ejecutar la estrategia acordada en la Fase II. Los STP ofrecen una serie bien definida de objetivos, papeles y responsabilidades, y un concepto operativo para tratar ciberamenazas específicas. Cada STP incluye normalmente planes pormenorizados para lo siguiente: (1) planificación y análisis; (2) organización; (3) tácticas; y (4) evaluación.

Seguidamente, el STP se comparte con los países participantes para su aprobación.

Las unidades de ciberdelincuencia participantes designadas por la OCN se comprometerán con la acción detallada en el STP y ofrecerán un apoyo total para lograr los objetivos operativos acordados. Tras la fase de 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 STP. Los datos relacionados con las operaciones se enviarán a INTERPOL para su análisis a través del sistema de comunicación protegida I-24/7, o a través de su Plataforma Colaborativa sobre Ciberdelincuencia – Operaciones.

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 africana intercambiando 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 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 inteligencia específica que puedan ayudar a otros países miembros con 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 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 inteligencia recopilada durante la Fase III también se evaluará para mejorar la comprensión a nivel regional de las ciberamenazas predominantes, y fundamentar el subsiguiente Informe sobre la Evaluación de las Ciberamenazas en África.



INTERPOL

Complejo Mundial de INTERPOL para la Innovación
18 Napier Road
Singapur 258510

SÍGANOS:



INTERPOL



YouTube

INTERPOLHQ



INTERPOL_HQ



@INTERPOL_HQ



INTERPOL HQ



www.interpol.int