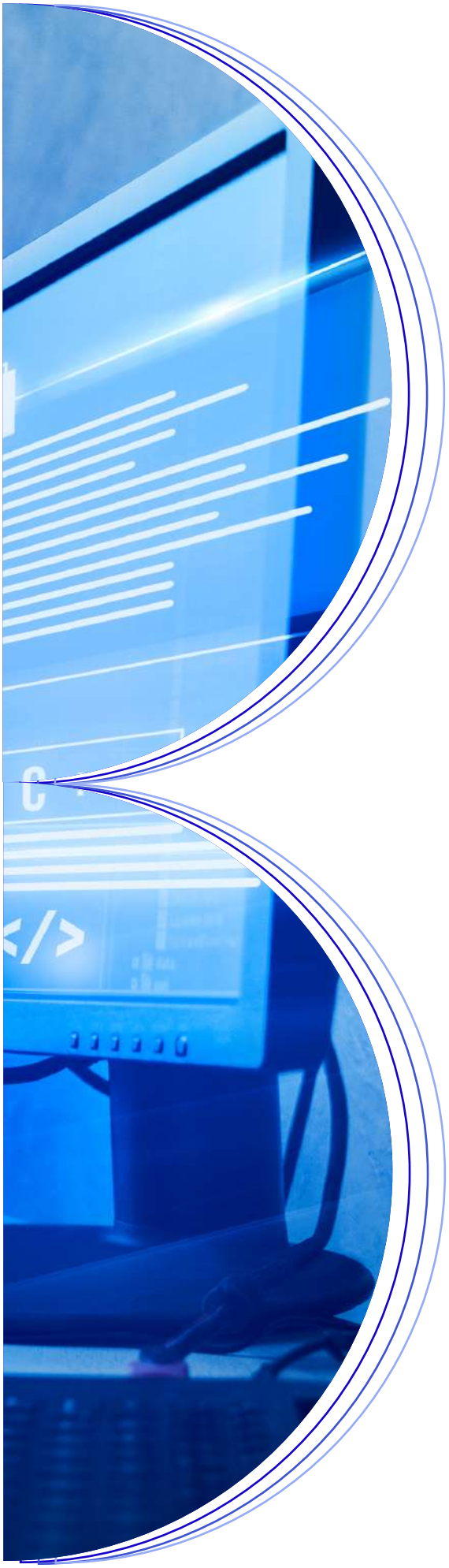
BeDisruptive™

It's an attitude

Cibercrimen en 2024

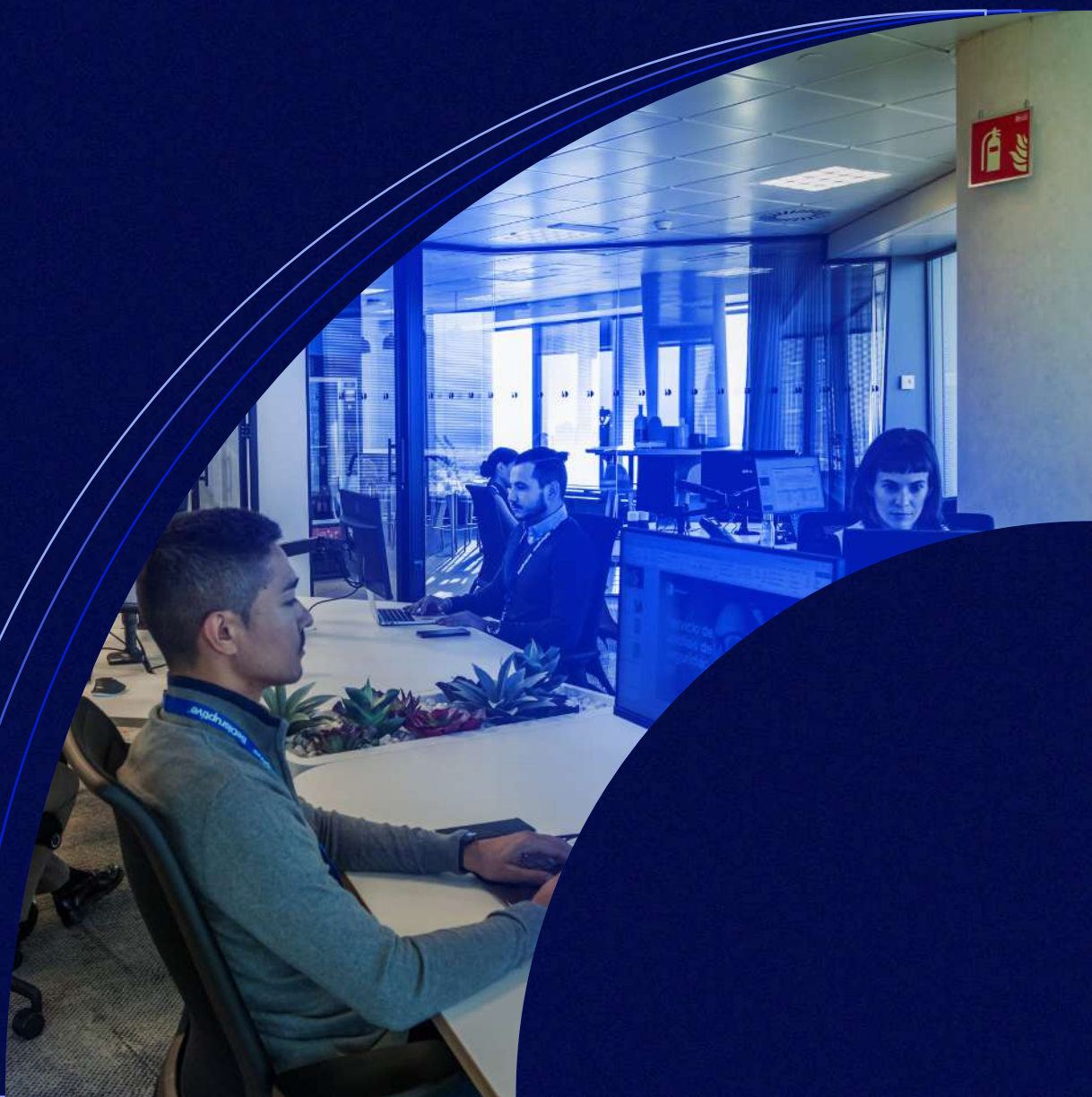
Análisis y tendencias

Tabla de contenidos_



BeDisruptive™

Resumen ejecutivo



01

El panorama de la ciberseguridad para el próximo 2024 se verá fuertemente influenciado por diversos factores, entre los que destacan los conflictos en Ucrania y Oriente Medio, las elecciones en EE. UU., Rusia y varios países europeos, así como, los Juegos Olímpicos de París en verano. La lenta recuperación económica y la amenaza de recesión a nivel mundial, las nuevas regulaciones proyectadas en materia de ciberseguridad previstas globalmente, y, sobre todo, la integración creciente de la inteligencia artificial (IA) en todos los sectores productivos, jugarán un papel crucial en la configuración de este escenario.

Específicamente en el campo de la IA, se prevé que **2024 marcará la convergencia y la adopción generalizada de esta tecnología** en numerosos campos de aplicación a nivel global.

No resulta exagerado contemplar el próximo año como el de la quinta revolución industrial, ya que las transformaciones previstas con la integración de la IA en la vida cotidiana representarán un significativo avance tanto a nivel industrial o de las Administraciones públicas, como en las rutinas diarias de las personas.

Sin embargo, todo este nuevo escenario de continua transformación digital supone nuevas oportunidades para los ciberdelincuentes, que, además, seguirán adaptándose a estos nuevos avances tecnológicos, optimizando la manera en la que éstos lleven a cabo sus ataques y mejorando sus probabilidades de éxito, por ejemplo, a la hora de encontrar objetivos vulnerables, de ejecutar campañas de *phishing* e incluso en la creación de *malware* inteligente.

Por otro lado, se espera que las campañas electorales se vean afectadas por *deepfakes* hiperrealistas realizados mediante inteligencia artificial, que busquen desinformar y manipular la opinión pública.

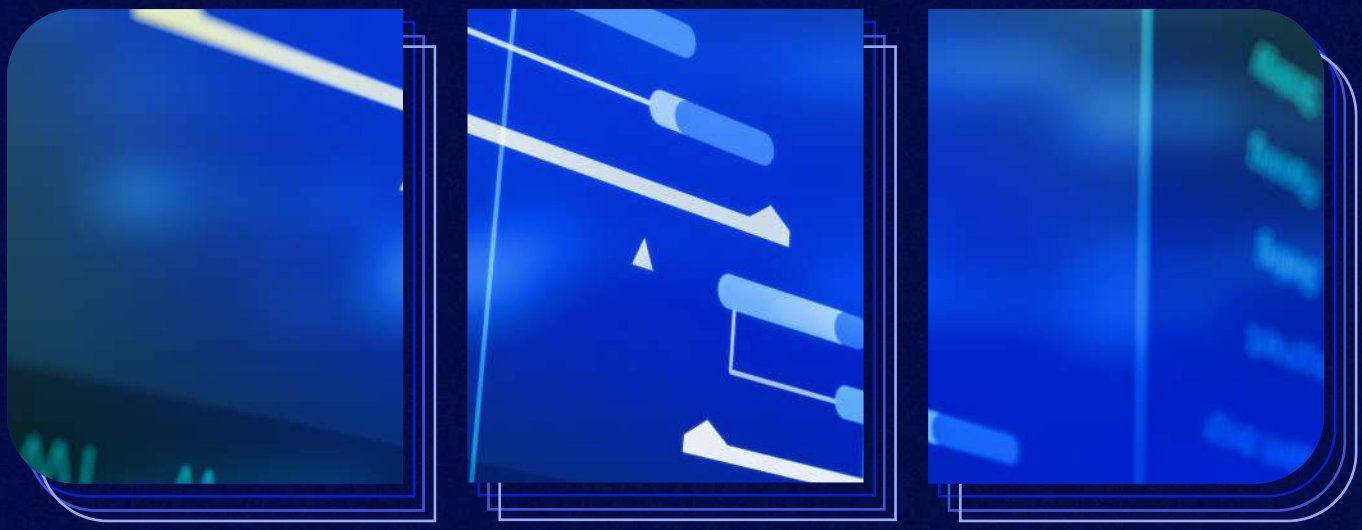
La adopción tecnológica será irregular en cada región del planeta, dependiendo del desempeño de cada economía, de cada contexto sociopolítico y de los distintos marcos regulatorios en aspectos clave de digitalización, como las regulaciones sobre la inteligencia artificial, tanto en ciberseguridad como en protección de datos, lo que también condicionará el comportamiento del cibercrimen.

En 2024 se espera que el hacktivismo siga ampliando sus áreas de actividad y continúe siendo una amenaza creciente, sobre todo en el contexto de los conflictos militares activos. Por otro lado, los ciberataques de *ransomware* complejos, como el de doble y triple extorsión, se espera que sigan siendo preocupantes, mientras que el número de estos grupos y las cifras de rescate seguirán incrementándose. En última instancia, existe la posibilidad de que se registre un incremento en la actividad cibercriminal de baja cualificación, impulsado por la situación económica y la pérdida de poder adquisitivo de la juventud. La intervención de la inteligencia artificial, junto con la función actual de Telegram como el principal punto de entrada al ecosistema cibercriminal, podrían contribuir a este fenómeno.

En este informe, BeDisruptive presenta algunas de las treinta tendencias sobre cibercrimen identificadas, con el propósito de mejorar la comprensión y fortalecer las medidas de prevención contra ciberataques para el año 2024.

BeDisruptive™

Análisis político



02

El año 2024 se vislumbra como un período geopolítico fascinante, con eventos de gran envergadura

Por un lado, se llevarán a cabo elecciones en Estados Unidos, Rusia y diversos países europeos. Por otro lado, los Juegos Olímpicos en Francia están programados para julio y agosto. Estos acontecimientos ejercerán una influencia directa en el comportamiento de los cibercriminales.

Posible cambio de gobierno o dirección política

Las elecciones al Parlamento Europeo y al Reino Unido serán las más importantes de Europa en 2024.

** Es probable que las elecciones en Ucrania sean canceladas bajo la ley marcial*

Fuente: EIU

Escenario electoral

En primer lugar, las elecciones en Rusia se celebrarán en el mes de marzo, un mes después de que la guerra en Ucrania cumpla los dos años. El resultado parece previsible, Vladimir Putin obtuvo un apoyo más que suficiente en las elecciones regionales celebradas en el mes de septiembre de 2023. Además, no parece haber rivales políticos que puedan poner en jaque su mandato hasta 2030.

Parece probable que la actividad cibercriminal por parte de actores rusos aumente, teniendo en cuenta las predicciones económicas para 2024, el desfavorable desarrollo de la guerra en Ucrania para Rusia y que el mandato de Putin se acercará a su fin en la próxima década. Como se destaca en el Informe "Crypto in Conflict" de la empresa Elliptic, la ciberdelincuencia desempeña un papel fundamental en la financiación de la lucha ideológica y, probablemente, también de la guerra, además de la actividad criminal llevada a cabo por APTs (Amenazas Persistentes Avanzadas) o grupos hacktivistas prorrusos.

Como añadido, Ucrania también debería tener elecciones en marzo de 2024, sin embargo, dado que el país se encuentra inmerso en pleno conflicto bélico, se prevé que estás sean canceladas bajo la ley marcial.

En segundo lugar, durante el primer fin de semana de junio, los ciudadanos europeos votarán a sus representantes al Parlamento. De acuerdo con la Economist Intelligence Unit, el voto europeo se caracterizará por su fragmentación y aumentará el apoyo a los partidos más conservadores, lo que dificultará la creación de coaliciones y la formulación de nuevas normativas europeas.

En tercer lugar, 2024 será testigo de nuevas elecciones en Estados Unidos, culminando con las presidenciales en noviembre. El escenario es, cuanto menos, complejo. Por un lado, aunque parece claro que el candidato del Partido Demócrata será el presidente Joe Biden, es menos probable que sea reelegido en el cargo, dado que no está gozando ni de la popularidad, ni del apoyo necesario entre la ciudadanía. Por el otro, parece que Donald Trump será su rival en las elecciones por parte del Partido Republicano y, aunque tiene más apoyos electorales, las causas judiciales a las que se enfrenta comenzarán en la primavera de 2024, pudiendo incluso acarrear penas de cárcel que imposibiliten su investidura.

En Latinoamérica, el 2023 ha supuesto significativos cambios políticos, destacándose las elecciones Colombia y Argentina. El auge de los partidos más conservadores, que comenzó con la victoria de Trump en Estados Unidos en 2016, se ha puesto de manifiesto con la elección de Javier Milei en Argentina el pasado mes de noviembre. En el transcurso de 2024, la región será escenario de elecciones en El Salvador, República Dominicana, Panamá, México, Uruguay y Venezuela.

Estos comicios serán determinantes para dilucidar si la tendencia de votación conservadora se consolida en la región. En anteriores elecciones de estos países hubo alternancia de partidos, los que preferían un presidente progresista optaron por los liberales y viceversa.

Los comicios descritos, especialmente los estadounidenses, acarrearán grandes campañas de desinformación, como ya ocurrió durante las pasadas elecciones al Parlamento Europeo en 2019. Sin embargo, estas serán las primeras elecciones tras la democratización del uso de la IA generativa.

Ahora es más fácil que nunca generar imágenes y vídeos falsos, comúnmente llamados *deepfakes*, lo que maximizará la distorsión de la realidad en favor de intereses particulares políticos.

Para abordar esta situación, en junio de 2023 los miembros del Parlamento Europeo votaron a favor de una estrategia coordinada contra manipulación de información e injerencia externa.

En esta estrategia se muestra una clara preocupación por los mecanismos de desinformación rusos, los ataques a la cadena de suministro en procesos electorales y la implementación de las directivas CER y NIS2.

Además, la Unión Europea cuenta con la iniciativa EUvsDisinfo para combatir esta amenaza.

Conflictos bélicos

Se prevé que los conflictos bélicos que están desarrollándose, por un lado, en Ucrania y por otro, en Oriente Medio, continúen en 2024, acaparando gran parte de la actividad cibercriminal. Es por esto por lo que deben ser muy tenidos en cuenta.

- Si bien Rusia tendrá parte de su atención focalizada en el proceso electoral, no parece que la guerra vea el final de sus días en 2024. Es posible que el primer trimestre del año sea más pacífico y la ofensiva rusa se reactive una vez Putin sea reelegido. Esta predicción concuerda con el aumento de gasto en defensa de Rusia, que en 2024 alcanzará el 6% de su producto interior bruto.

- En el caso de la guerra en los territorios israelí y palestino, parece que las primeras treguas o altos al fuego están cerca, aunque esto no significa necesariamente la antesala a un final definitivo de la guerra. El descenso de la popularidad de Netanyahu entre los israelíes ya provocó protestas a principios de 2023 y el conflicto parece no haber supuesto una mejora de su imagen política, por lo que prolongar la guerra no parece una estrategia beneficiosa para mantener su mandato.

- Los conflictos generan la necesidad de armamento para el combate, lo que a su vez provoca un aumento de la actividad en foros de venta de armas y municiones, tanto en Telegram como en la Deep Web. Esto también será tendencia al alta en 2024 en los mecanismos de lavado de dinero y fomentará el uso de las criptomonedas como método de pago menos rastreable.

Juegos Olímpicos

En último lugar, como destacado acontecimiento internacional, en verano se celebrarán los Juegos Olímpicos en Francia.

Si bien no se considera un evento político, las implicaciones diplomáticas y la congregación de múltiples nacionalidades en torno al deporte lo convierten en un evento de máxima relevancia tanto para los dirigentes de todos los países como para los cibercriminales.

Dicho evento, al ser masivo y de interés internacional implica, por tanto, el uso extenso de medios tecnológicos, dando lugar a una gran superficie de ataque. Es muy probable que se realicen campañas de fraude o ataques de denegación de servicio, entre otros. De hecho, a día de hoy ya se han registrado dominios redireccionados o potencialmente maliciosos relacionados con los próximos Juegos Olímpicos.

PRINCIPALES OBJETIVOS DE ATAQUE

- Sistemas de pago
- Venta de entradas
- Retrasmisiones en directo
- Sistemas de acceso a las instalaciones
- Suministros de energía, redes y telecomunicaciones

CONSIDERACIONES

Si el conflicto entre Israel y Palestina recrudece o hay una escalada de tensión en las fechas cercanas al evento, se podrán producir ataques terroristas o un aumento de los delitos de odio en territorio francés por parte de personas que apoyen la causa Palestina o que se consideren antisemitas.

Esta posibilidad complicaría aún más la logística y la seguridad del evento, no solo en su faceta virtual, sino también en la física. El reflejo en el mundo cibernético se encontrará en las campañas de difusión de discursos de odio y en el reclutamiento de nacionales franceses favorables a la causa palestina, principalmente a través de redes sociales, foros y canales de Telegram.

Tendencias observadas

1 Aumento de la actividad criminal por parte de actores rusos.

2 Aumento de ataques de DDoS asociados a procesos electorales o políticos relacionados con los conflictos en Ucrania y la Franja de Gaza.

3 Evolución de las campañas de desinformación por las capacidades de la IA.

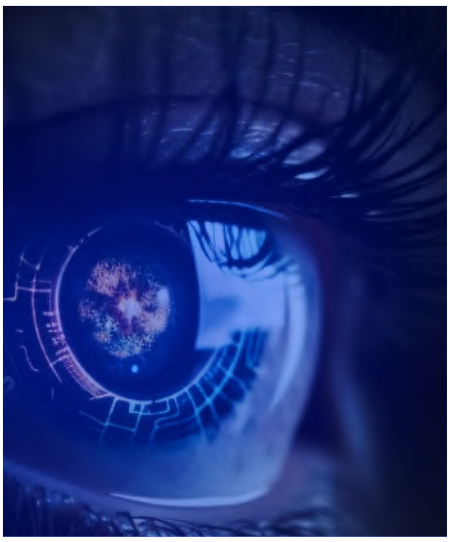
4 Ataques a la cadena de suministro en procesos electorales.

5 Aumento de campañas de fraude con motivo de los JJ.OO.

6 Aumento de ciberataques sobre todo de denegación de servicio, contra Francia y la organización de los JJ.OO. durante todo 2024, especialmente en las fechas del evento.

7 Buena parte de la actividad cibercriminal seguirá asociada a las guerras entre Ucrania y Rusia e Israel y Palestina.

8 Aumento del discurso de odio hacia Israel (o incluso EE. UU.) y difusión de discurso pro-palestino durante la celebración de los JJ.OO. como indicador previo a un ataque terrorista.



BeDisruptive™

Economía

03

En el transcurso de 2023, la economía mundial ha mostrado signos alarmantes de desaceleración. Tras el crecimiento del 2,4% previsto para este año y frente al 3% registrado el año anterior, esta desaceleración obedece a una serie de factores interrelacionados: la herencia económica del COVID-19, los conflictos geopolíticos y la inflación, entre otros.

La economía mundial continúa siendo volátil, principalmente debido a los efectos a largo plazo de la pandemia y a los conflictos bélicos actuales entre Israel-Palestina y Rusia-Ucrania, generando perturbaciones e irregularidades en las cadenas de suministro, que han afectado a la economía de una forma negativa.

Los desafíos en el suministro de ciertos productos básicos en los últimos años han disminuido la oferta, llegando al punto de no poder satisfacer la demanda, cuyo resultado es un aumento de la inflación por encima de las tasas recomendadas. Ello ha motivado en un aumento en las tasas de interés como medida de control de la inflación implementada por los bancos centrales, lo que ha desacelerado el crecimiento económico.

Sin embargo, dichos factores han tenido un impacto distinto en las regiones del mundo. Dado que China ha relanzado su economía tras la pandemia del COVID-19, Asia Oriental y el Pacífico han sido algunas de las regiones con más crecimiento en este 2023.

En sí, la desigualdad económica sigue siendo un desafío clave, donde la mayoría de los países en desarrollo se ven desproporcionadamente afectados por las restricciones económicas.

En lo que respecta a la financiación del cibercrimen, es indispensable analizar el estado y la creciente evolución de la adopción de las criptomonedas por su implicación en la financiación de actividades criminales.

En 2022 el **mercado de las criptomonedas sufrió una caída drástica de valor** debido a varios eventos.

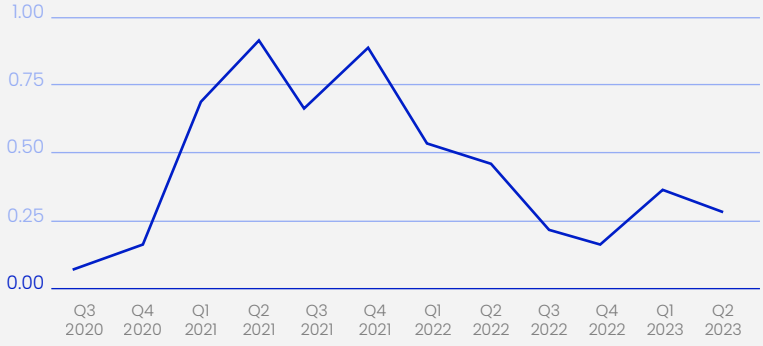
En el primer trimestre, el Banco Central de Rusia propuso la prohibición de la compraventa de criptomonedas y su minado, mientras que EE.UU. endureció sus políticas monetarias con el fin de combatir la inflación.

En el tercer trimestre, el mundo de las criptomonedas experimentó una gran disminución de valor, motivada por el sentimiento de desaceleración causado por la inflación y por los notables incrementos en los costes de la energía que, como resultado, generó mayores costes en el proceso de minado de criptomonedas. Como colofón, en el último trimestre el *exchange* de criptomonedas FTX, segundo en volumen de transacciones mundial, se declaró en bancarrota.

Tras el colapso de las criptodivisas, muchos mercados de la Dark Web se han visto afectados: más de 30 webs cerraron en dicho año a consecuencia del bajo valor y de la inseguridad en el mercado.

Q3 2020 - Q2 2023

Puntuación del índice global por trimestre



Fuente: The 2023 Geography of Cryptocurrency Report

Después del desplome de las criptomonedas en 2022, en 2023 el valor de las criptodivisas ha sufrido un fuerte incremento, influenciado por medidas regulatorias y judiciales impuestas por diversos gobiernos alrededor del mundo (como EE. UU.), restaurando así, aunque de manera lenta, la confianza en esos activos.

Por ello, los mercados de Bitcoin y criptomonedas han registrado una fuerte tendencia ascendente desde principios de año, pero en cifras aún lejanas a los picos históricos.

En términos geopolíticos, el entorno cripto sigue a la expectativa respecto al resultado de la adopción oficial como moneda del bitcoin por El Salvador, que tuvo lugar en septiembre de 2021 en su ya famosa "Ley Bitcoin", seguida en 2022 por la República Centroafricana, aunque recientemente ha realizado fuertes enmiendas a ley que avalaba la adopción Bitcoin.

Ambos países son pioneros tomando esta medida, aunque recientemente en 2023 Brasil ha reconocido el bitcoin como medio de pago (se entiende que esto sería un paso previo) y otros países latinoamericanos, como Argentina, estudian medidas similares, lo cual puede resultar en alguna que otra sorpresa en este 2024.

Desde la perspectiva financiera, la dinámica cripto en 2024 estará influenciada por la esperada aprobación de los ETF de Bitcoin y Ethereum por parte de la Comisión de Valores y Bolsa de Estados Unidos (SEC).

Este acontecimiento podría marcar uno de los momentos más significativos en el ecosistema cripto, al validar un enfoque de inversión más tradicional en criptomonedas en los Estados Unidos, de la mano del gigante financiero BlackRock, el mayor gestor de inversiones del mundo, cuyo volumen total supera el PIB de Alemania.

La confirmación de los rumores que rodean esta noticia podría inaugurar el nuevo año y desencadenar regulaciones similares en muchas otras naciones, impactando así en la cotización de los criptoactivos.

Por su parte muchas entidades privadas se siguen sumando a esta adopción, como por ejemplo Ferrari, en este último trimestre de 2023. Mientras, en Europa crece la desconfianza hacia su propia criptomoneda CBDC, llamada "euro digital", que sería un activo idéntico con valor fijo de 1 euro, completamente controlado por cada estado.

- A su vez, las criptomonedas se han convertido en una herramienta clave para la ciberdelincuencia, debido a que las transacciones criptográficas son anónimas e irreversibles y las autorizades no pueden supervisarlas por falta de trazabilidad.

- Esto supone un mayor riesgo de ciberataque para las empresas fintech de criptodivisas, cuyos usuarios pueden verse afectados por campañas de *malware*, *phishing*, formularios de registro comprometidos y el uso de aplicaciones de terceros con el fin de robar el dinero en sus carteras o las claves criptográficas asociadas a las mismas, con la consiguiente pérdida de fondos.

- Es de esperar, por tanto, que de aumentar significativamente tanto la adopción como la cotización de los criptoactivos, aumente exponencialmente la actividad cibercriminal dedicada al robo de éstos.

Según Cybersecurity Ventures, para 2025 se espera que el coste relacionado con la ciberdelincuencia alcanzará los 10,25 billones de dólares en todo el mundo.

Muchos de los incidentes actuales suelen tener un coste inmediato y concreto en cuanto a seguridad y recuperación de la operación y, además, existen costes más difícilmente medibles, tales como la pérdida de productividad debido al tiempo de inactividad operacional o, por ejemplo, las pérdidas económicas que pueden derivarse de brechas de seguridad donde se vea afectada la reputación.

Por consiguiente, el porcentaje de organizaciones que utilizarán servicios EDR gestionados crecerá hasta el 25% en 2024 y a su vez, más del 90% de las organizaciones que busquen externalizar la seguridad se centrarán en los servicios de detección y respuesta ante incidentes.

Tendencias observadas

1 Empobrecimiento de la población debido a la subida acumulada de la inflación, lo que podría favorecer la economía sumergida.

2 Recuperación del mercado y mayor adopción de las criptodivisas.

3 Aumento de los beneficios de la economía cibercriminal, tanto en cantidad de grupos como en ingresos de cada grupo.

BeDisruptive™

Tecnología

04

El 2024 va a ser un año especialmente interesante, debido a que la IA será adoptada por la mayoría de la población de manera consciente o inconsciente y esto supondrá un cambio en cómo se proveen los servicios y cómo la sociedad se relaciona con la tecnología.

No sería descabellado decir que 2024 va a ser el año del inicio de la quinta revolución industrial por dos motivos

La Inteligencia Artificial se desplegará en la mayor parte de *software* que sea posible.

La IA será adoptada por los usuarios de manera consciente o inconsciente. Las personas podrán beneficiarse de las ventajas de la IA tanto personal como profesionalmente.

Se prevé que la adopción de la IA sea más profunda y requiera que las empresas se mantengan al día y pongan en práctica los últimos avances para una mejor automatización de los procesos. Esta nueva necesidad supondrá un esfuerzo tecnológico para las empresas y un aumento en el ritmo de esta digitalización.

La necesidad de actualizarse con las últimas aplicaciones de inteligencia artificial en tiempo y forma puede resultar en vulnerabilidades o errores de código para las empresas, si los desarrollos no se planifican e implementan desde una perspectiva *security first*. A lo anterior se debe añadir que en las primeras versiones de una tecnología es común que se presenten abusos de funcionalidad o vulnerabilidades. 2024 será el año adecuado para ese ilícito propósito, dado que se desarrollará mucho *software* nuevo para incorporar la IA a sus capacidades.

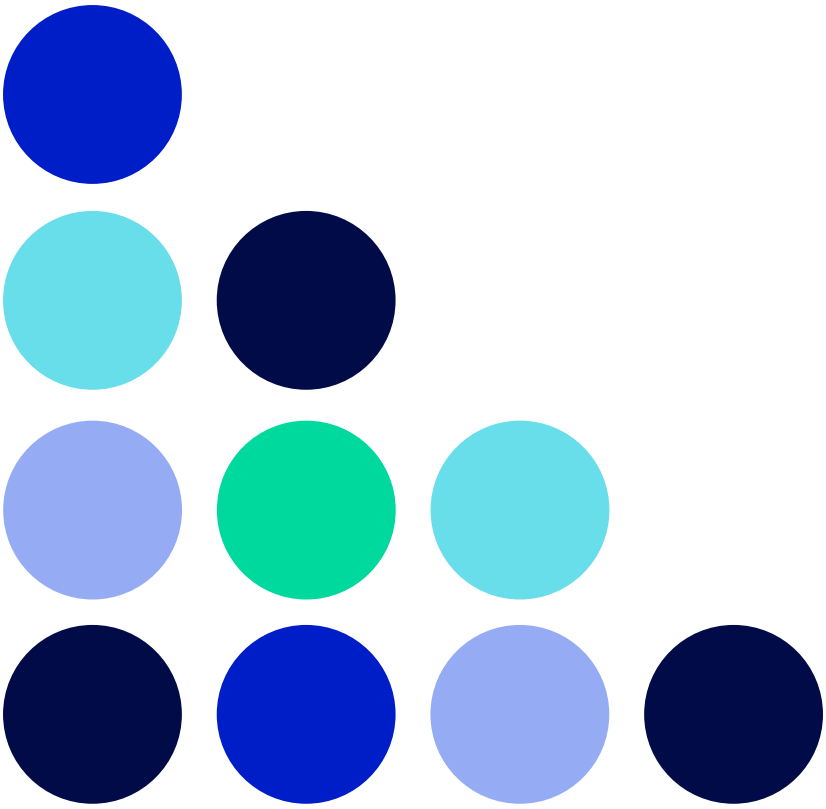
Un ejemplo claro de adopción tecnológica de la IA sería Microsoft Copilot, una herramienta que asiste al trabajador ayudándolo a escribir contenido o como recurso de consulta. La integración de Copilot y su vertiente de seguridad, Security Copilot, está siendo inmediata en casi todos los desarrollos tecnológicos.

Las aplicaciones con inteligencia también estarán disponibles para los cibercriminales, lo que puede ayudarles a encontrar vulnerabilidades en el código con más velocidad, facilidad y eficacia, generar nuevo *malware* más rápido, dirigido y/o sofisticado, etc.

Entre las múltiples aplicaciones y funcionalidades que la IA puede tener para los cibercriminales se consideran tendencias de alta probabilidad:

- **Despliegue de nuevo *malware* inteligente**. El próximo año es probable que se empiecen a detectar los primeros casos de *malware* que mejore sus probabilidades de éxito gracias a la IA. Este nuevo *malware* inteligente, tendrá capacidad de autoaprendizaje o *machine learning*, lo que le dotará de decisión y adaptación sobre sus acciones en función de las restricciones de seguridad a las que se enfrente.

- **Generación de contenido audiovisual mediante inteligencia artificial generativa**. Los cibercriminales dedicados al fraude mediante *pharming*, *adware* o *phishing* y sus variantes, podrán hacer uso de estas tecnologías y hacer que sus campañas sean más creíbles, aumentando sus ratios de eficiencia y, por ende, su rentabilidad, que se verá además potenciada por las nuevas capacidades publicitarias que la IA va a llevar a Internet en general y a las redes sociales en particular.



Tecnologías en observación

Combo IoT + 5G

La tecnología 5G será el raíl sobre el que viajará la información a alta velocidad en las ciudades. Con la rapidez que proporciona la baja latencia de esta tecnología, se aumenta el número de los dispositivos conectados a Internet y, por ende, la superficie de ataque.

Si bien ya se proveen servicios basados en esta tecnología, la adaptación necesaria hasta llegar a una implantación completa del 5G retrasará unos años más la llegada de las *smart cities* tal y como las imaginamos.

No se espera que en 2024 haya un despliegue masivo de dispositivos IoT conectados a la red 5G, sin embargo, se ha de monitorizar el avance de la implantación tecnológica, dado que es muy probable que se produzcan ataques o se descubran vulnerabilidades a manos de cibercriminales, sobre todo en entornos industriales conectados (o IIoT) o en el límite entre las redes IT y OT.

Además toda profiferación de ecosistemas basados en IoT, usen o no la red 5G, son susceptibles de sufrir un secuestro masivo de redes IoT que las conviertan en una *botnet* usada como herramienta APT, por ejemplo, para ataques de denegación distribuida de servicio o DDoS.

Tecnología SCADA/ICS

Los sistemas SCADA (Supervisory Control and Data Acquisition) son tecnologías esenciales para monitorizar y controlar procesos industriales en tiempo real, desempeñando un papel crítico en sectores clave como el de la energía, la cadena de suministro de agua potable y la manufactura. Los ataques a estos sistemas son una preocupación creciente, ya que pueden tener impactos críticos en la seguridad y la economía de un país.

Con el aumento de la conectividad y el acceso remoto, habrá una creciente disposición de los criminales a atacar los sistemas industriales críticos, como los ICS (Industrial Control System) y aprovecharse de sus vulnerabilidades.

Estos ciberataques en infraestructuras críticas representan una amenaza seria para sistemas vitales, como redes eléctricas, transporte y suministro de agua, comprometiendo la capacidad de respuesta en situaciones de emergencia. Por esta razón pueden tener un impacto geopolítico significativo, al desestabilizar naciones, manipular a la opinión pública e influir en dinámicas a nivel regional y global.

El **grupo cibernético CyberAv3ngers**, conocido por apuntar a infraestructuras críticas, ha perpetrado recientes ciberataques a sistemas SCADA en instalaciones de tratamiento de agua, estaciones de petróleo, gas e infraestructuras eléctricas. Estos ataques han tenido repercusiones a nivel global, y atribuyéndose consecuencias para hasta 10 estaciones de tratamiento de agua en Israel hasta octubre de 2023.

La creciente disposición de los criminales a atacar sistemas ICS de industrias críticas subraya la importancia de fortalecer las medidas de seguridad en estos entornos.

Realidad virtual y aumentada: Apple Vision

Si bien las gafas de realidad virtual y aumentada ya llevan un tiempo entre nosotros, Apple ha anunciado el lanzamiento de su producto para marzo de 2024. Es probable que el lanzamiento de este primer producto impulse de nuevo la fiebre de las gafas de realidad virtual normalizando aún más su uso, a pesar de su elevado precio, más de 3.000€.

De la misma manera, se podría prever que los competidores anunciasen o lanzasen productos mejorados en las mismas fechas.

Además, este lanzamiento no solo saca a la luz un dispositivo, también lanza un nuevo sistema operativo visionOS que podría ser víctima de ciberataques por nuevas vulnerabilidades.

La conexión humano-máquina: Neuralink

El polémico Elon Musk es siempre un referente en el panorama tecnológico, por lo que sus planes con Neuralink no pueden quedar fuera de vista. Su intención de crear una interfaz entre una máquina y el cerebro humano parece estar cada vez más cerca. Un indicio de lo anterior es que, en septiembre de 2023, se abrieron las inscripciones para los primeros ensayos en humanos lo que probablemente cosechará resultados que se darán a conocer en 2024.

Por el momento, está previsto que en el próximo año se lanzarán unas gafas de realidad aumentada.

Si los primeros ensayos en humanos son productivos, sería posible que los cibercriminales quieran conocer las posibilidades de ataque contra esa tecnología y exploten vulnerabilidades en ella. De la misma manera, si la tecnología es plenamente funcional, es probable que se lleven a cabo ataques con motivación de espionaje industrial contra la empresa y su líder.

Malware móvil

Se reconoce un riesgo en aumento y observación de *ransomware* móvil, tras la creciente dependencia de dispositivos móviles en ámbitos tanto personales como laborales. Sin embargo, su uso no parece una prioridad para el cibercrimen, debido a la diferencia entre los sistemas operativos y las capas de *software* que producen los fabricantes. Por ello se desarrollan ataques más individualizados y específicos a personas, en vez de a empresas, lo cual aporta menos beneficios. A pesar de esta baja relación esfuerzo / recompensa para los cibercriminales, debe ser una amenaza a monitorizar.

Durante el primer trimestre de 2023, SecureList reportó el bloqueo de más de 4.900.000 ataques de *malware* móvil, *adware* y *riskware*, señalando un aumento en la sofisticación y frecuencia de estos ataques. Un factor que contribuye a esta amenaza es el uso de las APK descargadas desde fuentes no oficiales, puesto que son versiones modificadas de aplicaciones legítimas que ponen en riesgo la ciberseguridad y/o privacidad de los dispositivos. Las APK son especialmente susceptibles a la explotación por parte de actores malintencionados, ya que no se someten a los controles de seguridad que las aplicaciones oficiales en los markets de aplicaciones, como Google Play.

Tendencias observadas

1 Abuso de funcionalidades y vulnerabilidades en herramientas y *software* en general y de ciberseguridad en particular con las nuevas tecnologías de IA.

2 Generación de *malware* inteligente que evolucione de manera autónoma ante unas restricciones de seguridad concretas.

3 Posibles ataques contra el nuevo sistema operativo visionOS.

4 Mayor eficiencia en las campañas de *phishing* apoyadas por IA Generativa.

5 Existe la posibilidad de que se registre un aumento de *ransomware* móvil.

6 Posible aumento de ataques exitosos contra infraestructuras críticas que resulten en interrupción del suministro.

BeDisruptive™

Ámbito legal

05

Marco regulatorio de la inteligencia artificial: la IA-ACT

Dados los riesgos de diversos tipos que se han identificado en el uso de la IA, se prevé que los organismos gubernamentales e internacionales dediquen esfuerzos en legislar esta nueva tecnología. Sin embargo, este será un reto complicado, puesto que no se conoce aún el impacto final que la utilización de esta tecnología tendrá en la sociedad y el cibercrimen y, por ende, habrá que ir legislando a medida que se vayan descubriendo nuevos usos fraudulentos o éticamente cuestionables. Parece que la clave en este caso será regular los usos de la tecnología y no el desarrollo de esta.

La realidad regulatoria con respecto a la IA es heterogénea y está condicionada a cada región. Según los antecedentes, la Unión Europea está adoptando las medidas más restrictivas, incluso algunos países como Italia han prohibido su uso por motivos de transparencia y protección de datos.

Ya en 2021 la Comisión Europea propuso la AI-ACT, que se acaba de aprobar para dar broche a este 2023 en Bruselas, con la que se pretende asegurar que este tipo de recursos sean seguros, transparente, auditables, no discriminatorios y amables con el medioambiente.

China ha enfocado su regulación al control del uso interno por parte de la población, mientras que EE.UU. no parece que vaya a adoptar medidas regulatorias de restricción al respecto, favoreciendo la innovación.

En 2022, en EE.UU. se implantó la AI Bill of Rights en la que, de manera no vinculante, se instó a las empresas a hacer un uso limitado y responsable de servicios de vigilancia con estas tecnologías.

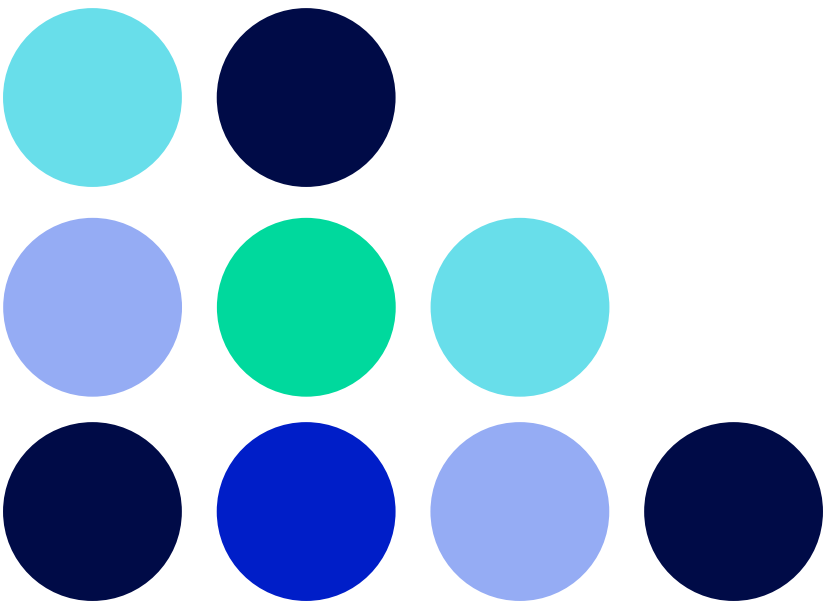
Marco regulatorio de ciberseguridad: NIS2

En octubre de 2024, la directiva sobre ciberseguridad de la Unión Europea NIS2 deberá haberse traspuesto a las legislaciones correspondientes de los estados miembros. Esta ley, junto con su antecesora, la NIS, "proporciona medidas legales para impulsar el nivel general de la ciberseguridad en la UE", tal y como se refleja en la documentación de la Comisión Europea.

Las empresas e instituciones de los 18 sectores calificados como críticos deberán adaptarse a la nueva legislación en cuanto entre en vigor en sus geografías. Si bien esta legislación supone cambios en el gobierno de la ciberseguridad, no parece que la adaptación a la NIS2 vaya a ser un reto para las organizaciones que ya estén familiarizadas con la normativa NIS original.

DORA (Digital Operational Resilience Act)

Es un reglamento de la Unión Europea orientado a regular la resiliencia de los sistemas operativos digitales. Esta ley establece unas normas de protección, detección, contención, recuperación y reparación en caso de incidentes de ciberseguridad en las instituciones financieras, dado que se considera que un ciberataque puede suponer un peligro real para la solidez del sistema financiero. A diferencia de NIS2, este es un reglamento vinculante que todas las entidades financieras deberán haber aplicado para el 17 de enero de 2025.



eIDAS (IDentification, Authentication and trust Services)

La digitalización nos está acercando a regulaciones como el eIDAS, un reglamento que propuso en 2014 una nueva forma de regular las firmas electrónicas, la emisión de certificados y las transacciones, eliminando la necesidad de personarse para realizar un trámite.

En su nueva versión, el eIDAS 2 pretende mejorar la regulación anterior y facilitar el acceso de la población europea a una cartera de documentación digital, es decir, llevar los documentos de identidad en el móvil o dispositivo de nuestra elección.

Esta regulación supone un avance en la digitalización, sin embargo, también puede suponer una oportunidad clave para la suplantación de identidad y la comisión de campañas de fraude, si no se gestiona adecuadamente la autenticación e identificación de los usuarios.

A raíz de la implementación de estas leyes, es posible que se produzcan en Europa campañas de fraude suplantando identidades, especialmente entre el Q4 de 2024 y enero de 2025, momento en el que entrarán en vigor, aprovechando el *impasse* legislativo. Más allá de lo indicado, no se prevén otras campañas o un impacto directo en la actividad cibercriminal.

Lo que sí se prevé para 2024 es que las principales agencias policiales internacionales, tales como Interpol o Europol, continúen aumentando el número de detenciones y *takedowns* de mercados ilegales, como lleva ocurriendo los últimos años.

Tendencias observadas

1 Segmentación geográfica de las medidas regulatorias con respecto a la inteligencia artificial.

2 Aumento de la cantidad de detenciones y *takedowns* de foros del *underground* gracias a la colaboración entre entidades policiales.

BeDisruptive™

Medioambiente

06

Si bien puede parecer que el medioambiente no tiene una relación directa con la ciberseguridad, existen dos aspectos que se han de tener en cuenta.

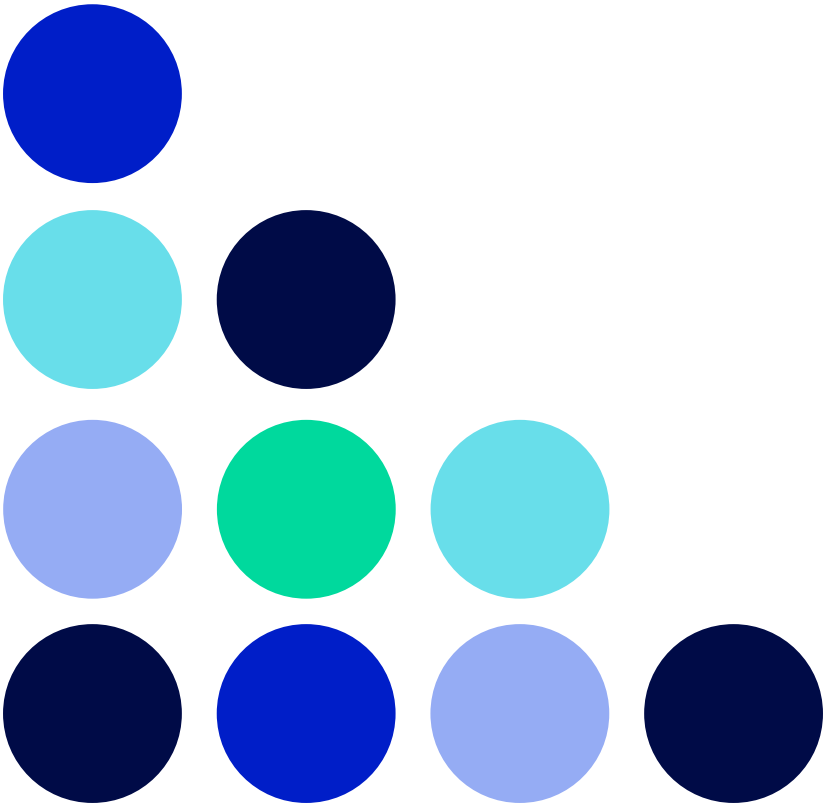
- **Cambio climático**. En primer lugar, el cambio climático está provocando un aumento de los fenómenos climáticos de adversidad extrema, tales como tormentas eléctricas que provocan incendios, huracanes, erupciones volcánicas o grandes inundaciones, entre otros.

  Estas condiciones han de ser tenidas en cuenta a la hora de operar y securizar sistemas tecnológicos.

Cada catástrofe ecológica da lugar a campañas de fraude suplantando ONGs en busca de donativos.

A mayor número de catástrofes, mayor número de campañas de recaudación de fondos y mayor beneficio en campañas de fraude para los cibercriminales.

- **Auge de energías renovables**. Por otro lado, el auge de las energías renovables, la transición energética actual y los conflictos armados, promoverán que, en 2024, muy probablemente el número de ataques contra sistemas renovables aumente, como ha ocurrido en los últimos años. Esta será una tendencia consolidada y en auge que habrá de tenerse en cuenta.



Tendencias observadas

1 Aumento de eventos climáticos adversos y fraudes relacionados a estos.

2 Aumento del número de ataques contra empresas y elementos propios de las energías renovables.

BeDisruptive™

Previsiones regionales 2024

07

América Latina

En 2024, la expansión económica de América Latina se reducirá a una cifra muy inferior a la media mundial, debido a la persistente inestabilidad política y a la falta general de competitividad económica frente a otros mercados emergentes. América Latina atraviesa un periodo de cambio político sustancial con los nuevos gobiernos asentados. Aunque la incertidumbre política disminuirá en 2024, persistirán riesgos como el retroceso democrático y la agitación social.

La previsión de crecimiento para 2024 es del 2,3%, indicando un retroceso a los bajos niveles de crecimiento previos a la pandemia. La región también sufrirá los efectos adversos a nivel global, como la disminución de los precios de productos básicos, el aumento de las tasas de interés en los países del G7 y la frágil recuperación de China.

El impacto de El Niño y otros desastres naturales son un riesgo clave para la agricultura y la minería, esenciales para la región.

El cambio climático afectará la región, causando pérdidas económicas y sociales: catástrofes meteorológicas serán más frecuentes, y se estima que 17 millones de personas podrían verse obligadas a abandonar sus hogares.

Las oportunidades de crecimiento verde, en forma de electricidad renovable - solar, eólica y geotérmica - y el vasto capital natural - agua, árboles, biodiversidad - representan el potencial para nuevas industrias en la región.

Otras oportunidades surgen de políticas a largo plazo, como la reducción de riesgos sistémicos, la promoción de inversiones en infraestructura tradicional y digital, y la mejora del capital humano.

Ciberseguridad en América Latina

En este contexto, el tamaño del mercado de ciberseguridad en América Latina se espera que crezca de 8.340 millones de dólares en 2023 a 11.670 millones de dólares para 2028, con una tasa de crecimiento anual compuesta del 6,95%. La creciente penetración digital en la región, respaldada por el uso de Internet y el desarrollo móvil, genera una creciente demanda de ciberseguridad, esencial para la realización de la transformación digital.

Sin embargo, los mercados emergentes latinoamericanos están especialmente expuestos a cibercriminales y brechas de seguridad, lo que requiere una base más sólida para defender el futuro de las empresas. La creciente preferencia de los consumidores latinoamericanos por los pagos móviles amplifica la necesidad de seguridad de aplicaciones, ya que los pagos basados en aplicaciones se vuelven más comunes.

La región necesita más profesionales con habilidades específicas en el sector de la ciberseguridad.
Según el Foro Económico Mundial, la demanda de especialistas en ciberseguridad ha crecido un 350% desde el año 2013, mientras que en 2025 el déficit de profesionales en la especialidad alcanzará los 3,5 millones.

En resumen, América Latina enfrenta desafíos y oportunidades en el campo de la ciberseguridad, con la necesidad de una base más sólida para proteger su crecimiento digital y enfrentar amenazas emergentes, especialmente en un contexto post COVID-19.

Los impulsores clave de la industria de ciberseguridad en América Latina provienen de la adopción de nuevas tecnologías como el IoT, Big Data e inteligencia cognitiva, junto con el uso generalizado de servicios gestionados en la nube.

Europa

La economía de Europa central y oriental se proyecta hacia un crecimiento más rápido en 2024, respaldada por la moderación de la inflación y la disminución de los tipos de interés. La recuperación de Alemania desempeñará un papel crucial al respaldar las exportaciones y la producción industrial en la región. No obstante, factores como la evolución de la guerra en Ucrania y los precios de las materias primas deben tenerse en cuenta, ya que podrían impactar el panorama económico.

Las empresas europeas han demostrado resistencia durante la crisis energética, aunque la producción industrial ha disminuido, generando preocupaciones sobre subvenciones que podrían comprometer el mercado único de la UE.

Las políticas coordinadas, que incluyen inversiones públicas para la transición verde, son consideradas cruciales en este contexto.

Las proyecciones indican una orientación restrictiva de las políticas fiscales en la zona euro, influenciada por el aumento del gasto militar y las inversiones del programa "*Next Generation EU*".

El BCE ha endurecido la política monetaria, previendo que las tasas se mantendrán altas hasta 2025 para reducir las presiones inflacionarias.

Sin embargo, existen riesgos a la baja, como precios energéticos inestables, tensiones comerciales y riesgos para la estabilidad financiera, mientras que un alivio geopolítico o una recuperación en China podrían mitigar los impactos negativos.

Ciberseguridad en Europa

El tamaño del mercado de ciberseguridad en Europa se espera que crezca de 32.430 millones de dólares en 2023 a 57.750 millones de dólares para 2028, con una tasa de crecimiento anual compuesta del 12,23% durante el período de pronóstico (2023-2028).

La adopción de soluciones de ciberseguridad aumentará con la creciente penetración de Internet en los principales países de Europa, mientras que la expansión de la red inalámbrica ha aumentado la vulnerabilidad de los datos.

La implementación de la legislación de la Unión Europea y las acciones derivadas del Marco Nacional y el Plan Nacional de Ciberseguridad se espera que faciliten el crecimiento del mercado en la región.

Además, inversiones significativas, como los 1.600 millones de euros comprometidos por la UE, impulsan la implementación generalizada de infraestructuras y tecnologías de ciberseguridad en la UE.

Los dispositivos conectados, incluyendo máquinas, sensores y redes que conforman el Internet de las Cosas (IoT), junto con la ciberseguridad, jugarán un papel clave en el futuro digital de Europa.

La escasez de trabajadores capacitados en ciberseguridad es un desafío clave, especialmente en un contexto de aumento de la presencia en línea durante la epidemia de COVID-19, donde los cibercriminales se centraron en el comercio electrónico, las empresas de pago en línea y el sistema de salud.

Asia

En Asia se espera experimentar un sólido crecimiento en 2024, a pesar de la desaceleración económica en China y las tensiones geopolíticas regionales. El panorama político estará marcado por elecciones en economías estratégicas como India, Indonesia y Taiwán.

El crecimiento regional debería acelerarse en 2024 con respecto a la proyección de este año, impulsado por la reducción de las tasas de interés, el enfriamiento de la inflación y la recuperación de las exportaciones.

La industria de energía verde será destacada, ya que los mercados buscan alternativas regionales frente a la oferta china.

Sin embargo, la lenta recuperación de China y el fenómeno meteorológico de "El Niño" pesarán sobre el crecimiento en toda la ASEAN.

Una recesión prolongada en el sector electrónico mundial y condiciones climáticas extremas plantean riesgos a la baja.

Corea y Taiwán deberían acelerar gracias a la recuperación de sus sectores industriales orientados a la exportación, mientras que Mongolia seguirá siendo el país con mejor desempeño de la región.

Ciberseguridad en Asia

En este contexto, el tamaño del mercado de ciberseguridad en Asia-Pacífico se proyecta en un crecimiento significativo, aumentando de 57.410 millones de dólares en 2023 a 109.100 millones de dólares para 2028, con una tasa de crecimiento anual compuesta del 13,7% durante el período de pronóstico (2023-2028). Este crecimiento se atribuye a la creciente adopción de soluciones de ciberseguridad impulsada por la expansión del uso de Internet y las redes inalámbricas, junto con un impacto mayor de los ciberataques.

Muchos países, como India, China, Singapur y Japón, enfrentan problemas crecientes relacionados con la ciberseguridad. India ocupa el tercer lugar en la cantidad de secuestros de DNS, indicando un fuerte aumento en los registros de cibercrimen.

Según el Índice de Inteligencia de Amenazas de IBM Security X-Force de 2023, Asia recibió el 26% de todos los ataques a nivel mundial en 2021, convirtiéndola en la región más atacada globalmente, con India encabezando la lista de los países más atacados en la región.

La investigación reciente de la Red de Crecimiento de la Seguridad Cibernética de Australia sugiere que el sector de la ciberseguridad podría triplicar su tamaño en la próxima década.

La baja preparación y la alta dependencia de técnicas de autenticación convencionales representan un desafío en términos de identidad digital. En un entorno de mercado donde los profesionales de seguridad recomiendan soluciones de gestión de identidad robusta como el reconocimiento facial y la identificación biométrica, más del 80% de las organizaciones aún confían únicamente en nombres de usuario y contraseñas para el inicio de sesión, lo que podría desafiar el crecimiento.

Norteamérica

Aunque las elecciones presidenciales de EE.UU. en noviembre dominarán el panorama para América del Norte el próximo año, la región también deberá enfrentar los efectos de mayores costos de endeudamiento.

La economía de Estados Unidos se recuperó fuertemente de las profundidades de la recesión pandémica, gracias a una respuesta gubernamental amplia y duradera.

Sin embargo, la guerra de Rusia contra Ucrania y las fuertes presiones inflacionarias han afectado las perspectivas económicas.

A pesar de los esfuerzos de la Administración por mejorar el bienestar público mediante inversiones en infraestructura y la transición climática, se prevé una presión fiscal, debido al envejecimiento de la población. En respuesta, se deben centrar más esfuerzos en ampliar la base imponible y mejorar la eficiencia del gasto público, especialmente en las áreas de salud e infraestructura.

En Canadá, el aumento global de los precios ha afectado a la economía justo cuando el desempleo alcanzaba mínimos históricos, en medio de una fuerte recuperación de la pandemia. Los responsables de la política del país enfrentan el desafío de frenar la inflación sin causar una recesión. Canadá tiene como objetivo eliminar sus emisiones netas de gases de efecto invernadero para 2050, lo que requiere fuertes incentivos para eliminar el uso de combustibles fósiles y fomentar el ahorro de energía y el desarrollo de energías renovables.

Para impulsar la descarbonización, la estrategia climática federal utiliza una combinación de fijación de precios de emisiones, apoyo a la energía verde y nuevas regulaciones.

Ciberseguridad en Norteamérica

Estos desafíos económicos y medioambientales se entrelazan con la importancia de la ciberseguridad en la región, donde se estima que el mercado crecerá de 85.070 millones de dólares en 2023 a 127.980 millones de dólares para 2028.

América del Norte es una de las regiones digitales líderes en el mundo, y en los próximos años, se anticipan cambios significativos impulsados por la tecnología.

El aumento de la digitalización, con desarrollos tecnológicos como la robótica, la tecnología de sensores, la impresión 3D, el Big Data y la inteligencia artificial, plantea la necesidad de aumentar la seguridad de los datos en la región.

La proliferación de Internet y la expansión de las redes inalámbricas han impulsado un aumento en la adopción de soluciones de ciberseguridad.

La amenaza persistente de ciberataques cada vez más frecuentes y sofisticados resalta la necesidad imperante de implementar medidas eficaces para asegurar la integridad digital en este entorno desafiante.

África

África experimentará un notable crecimiento económico en 2024, impulsado por el sector de servicios, especialmente destacado en África Oriental.

Sin embargo, persisten amenazas como la seguridad, la inestabilidad política y las cargas de pago, que constituirán riesgos a considerar en el próximo año. El conflicto armado en el Sahel seguirá siendo una preocupación para la seguridad, y las elecciones en el continente presentarán desafíos socioeconómicos y posibles disturbios civiles.

En cuanto a la economía, las perspectivas estarán influidas por las obligaciones de pago de la deuda y la depreciación de la moneda.

Las presiones inflacionarias, aún presentes en África, continuarán afectando el rendimiento económico a corto y medio plazo. La inflación actual ha sido impulsada principalmente por *shocks* en la oferta agrícola, el aumento de la inflación importada debido a la debilidad de las monedas locales, los precios relativamente altos de las materias primas y la persistencia del dominio fiscal en varios países africanos. Se estima que la inflación africana promediará el 17,1% en 2024.

La desaceleración del crecimiento económico en China también afectará a los países africanos, especialmente aquellos dependientes del mercado chino para las exportaciones de materias primas.

Medio Oriente

La persistente guerra entre Israel y Hamás seguirá resonando en el año 2024, exacerbando el resentimiento hacia Israel y sus aliados occidentales.

Este prolongado conflicto presenta desafíos significativos para las relaciones árabe-israelíes, generando tensiones que pueden tener implicaciones más allá de la región inmediata.

Las relaciones internacionales se verán sometidas a prueba: este conflicto no solo afecta directamente a la región, sino que también tiene ramificaciones globales, especialmente dada la participación de actores occidentales en la situación.

En el ámbito de las alianzas geoestratégicas, se anticipa que los Estados del Consejo de Cooperación del Golfo (CCG) se beneficiarán de estrategias destinadas a diversificar tanto el comercio como las inversiones.

El CCG podría desempeñar un papel clave en la mitigación de los impactos económicos derivados de la inestabilidad en otras partes del Medio Oriente.

La inseguridad regional derivada de estos conflictos tendrá un impacto en las perspectivas para el sistema de "petrodólares", afectando potencialmente la estabilidad económica de la región.

La volatilidad en los precios del petróleo y la incertidumbre geopolítica podrían influir en las decisiones económicas y de inversión en los países de la región, así como en aquellos que dependen de sus recursos energéticos.

El panorama geopolítico del Medio Oriente en 2024 está marcado por tensiones persistentes, desafíos para las relaciones internacionales y posibles implicaciones económicas.

Las alianzas estratégicas, la seguridad regional y el sistema de petrodólares están interconectados en esta compleja red de dinámicas, que requerirá una gestión cuidadosa y una diplomacia efectiva para abordar sus múltiples facetas.

Ciberseguridad en Medio Oriente y África

El mercado de ciberseguridad en Medio Oriente y África se estima en 2.590 millones de dólares en 2023 y se espera que alcance los 4.650 millones de dólares para el 2028, con tasa de crecimiento anual del 12,42%.

En la situación actual del mercado, los conglomerados de ciberseguridad pueden crecer de manera orgánica o desarrollarse a través de acciones intencionales, a menudo tomadas por los gobiernos locales, y la regulaciones y políticas gubernamentales desempeñan un papel significativo en su desarrollo. Muchas empresas privadas están trasladando sus operaciones a plataformas en la nube.

Arabia Saudita, con una economía basada en el petróleo, es la nación más grande de la región del Golfo y tiene como objetivo ser el mercado de tecnologías de la información más destacado.

Diversas iniciativas gubernamentales, como el Programa de Transformación Nacional (NTP), han respaldado el rápido desarrollo de las tecnologías de la información en la región.

Arabia Saudita es un objetivo popular para los ciberdelincuentes, debido a sus pozos petroleros y su ocupación en un área con tensiones geopolíticas.

La región de Medio Oriente y África cuenta con un número reducido de profesionales en ciberseguridad, pero teniendo en cuenta la alta actividad empresarial en la región, se posiciona como una de las regiones más atractivas para los ciberataques.

La creciente adopción del teletrabajo durante la pandemia ha aumentado el número de ataques.

Esto es un factor clave, ya que los incidentes de ciberseguridad asociados al trabajo remoto tuvieron un coste promedio de 1,05 millones de dólares más que en las demás.

Esta región requiere profesionales más experimentados para enfrentar la intensidad de las amenazas cibernéticas entrantes.

BeDisruptive™

Actores de amenazas

08

El panorama de amenazas no solo se ve condicionado por los ámbitos ya analizados. Además, los grupos de cibercrimen están cambiando su forma de actuar recurriendo a TTPs que anteriormente no correspondían a sus motivaciones.

Un ejemplo de esto es el caso del hacktivismo "nacional", en el que un Estado nación tiene su propio grupo hacktivista con el fin de llevar a cabo una campaña reputacional o de desprestigio hacia un adversario, mediante el uso de ataques de denegación de servicio o incluso de ataques de *ransomware*.

Con esa información, es importante tener en cuenta que para el año 2024 el panorama cambiará aún más y las diferencias entre los tipos de actores serán más difusas.

PREVISIÓN DE ACTORES MÁS ACTIVOS DURANTE EL AÑO 2024

Actores con motivación de espionaje

ASIA Amenazas persistentes avanzadas (APTs)

Centrando sus objetivos principalmente en gobiernos y sectores clave como tecnología, telecomunicaciones y salud, las APTs chinas han dirigido su enfoque hacia nuevas familias de *malware*, entre las que destacan IISBd6 y MQTTRat.

En la actualidad, las APTs originarias de este país se posicionan como la amenaza de ciberespionaje más amplia, activa y persistente para las redes tanto gubernamentales como del sector privado en Estados Unidos. La ODNI (Office of the Director of National Intelligence) subraya sus capacidades altamente probables para interrumpir servicios esenciales en infraestructuras críticas, incluyendo oleoductos, gasoductos y sistemas ferroviarios.

Frente a la presencia de otros grupos APT chinos, como EvilEYE y Mustang Panda, emerge un nuevo actor conocido como Vanguard Panda. Este grupo se distingue por la aplicación de técnicas de explotación de vulnerabilidades, la persistencia mediante *webshells* y estrategias "*Living off-the-Land*" (LotL), evidenciando una presencia considerable en Estados Unidos.

En cuanto a esta última táctica, su objetivo principal es operar aprovechando *software* y funciones legítimas disponibles en el sistema para llevar a cabo acciones maliciosas.

RUSIA Amenazas persistentes avanzadas (APTs)

Parece previsible que, en 2024, la actividad de las APTs rusas continúe teniendo a Ucrania como foco principal y, además, se lleven a cabo campañas relativas a las elecciones rusas, como ya ha ocurrido en comicios previos.

Las víctimas serán, previsiblemente, Ucrania, Estados Unidos y las naciones con mayor implicación en el conflicto. De estas víctimas, los principales objetivos serán el sector público, las infraestructuras críticas y los organismos militares.

Fancy Bear, también conocido como APT28 y presumiblemente vinculado al Servicio de Inteligencia Militar de Rusia (GRU), ha refinado significativamente sus Tácticas, Técnicas y Procedimientos (TTPs).

Este actor de amenaza ha alcanzado un mayor nivel de sofisticación, al buscar obtener acceso inicial sobre los sistemas de sus víctimas mediante una combinación entre la explotación de vulnerabilidades y la ejecución de campañas de *spear phishing*.

Estas tácticas se dirigen específicamente a organismos gubernamentales y militares, revelando un enfoque selectivo y altamente dirigido en sus operaciones.

Otro actor, presuntamente vinculado también con el Servicio de Inteligencia Militar de Rusia (GRU), que merece atención es SandWorm/Voodoo Bear.

Este grupo se distingue por llevar a cabo operaciones a gran escala con motivaciones geopolíticas, participando activamente en campañas de *malware* destructivo, incluido el desarrollo y la explotación de amenazas dirigidas a dispositivos Android. Sus objetivos abarcan organismos gubernamentales, militares e infraestructuras críticas, marcando un perfil distintivo en el panorama de las ciberamenazas.

IRÁN Amenazas persistentes avanzadas (APTs)

Los grupos APTs iraníes en 2023 se han centrado en el sector de las telecomunicaciones y en el ámbito regional. Las víctimas de los ataques se encontraban en Oriente Medio y el Norte de África principalmente, regiones en la que Irán pretende mantener su posición de influencia. Fuera de esta región, se han registrado campañas en EE.UU. contra entidades gubernamentales.

El conflicto que se inició entre Israel y Hamas en el pasado mes de octubre de 2023, acapara completamente en la actualidad y, seguramente en el futuro próximo, los esfuerzos de parte de las APTs iraníes. El apoyo cibernético a la causa Palestina es un recurso más de los que Irán es sospechosa de estar utilizando actualmente para conseguir desestabilizar militar y políticamente a Israel sin proporcionar ayuda militar directa en Palestina, lo que podría desencadenar una escalada de tensión en la región y la intervención de otras potencias regionales e internacionales, con la subsiguiente escalada del conflicto.

En relación con algunos de los grupos con actividad más reciente durante este 2023, cabe destacar a Imperial Kitten, Charming Kitten y Static Kitten. Respecto al grupo Imperial Kitten, caracterizados por la ingeniería social, se sospecha una conexión con el Islamic Revolutionary Guard Corps (IRGC), puesto que cumple de forma muy probable los requisitos de inteligencia estratégica para las operaciones asociadas al IRGC.

Además, actúan utilizando técnicas SWC y utilizan el *malware* IMAPLoader en la mayoría de ataques contra los sistemas infectados.

COREA DEL NORTE Amenazas persistentes avanzadas (APTs)

Existen numerosos grupos cibercriminales desde el país norcoreano haciendo uso de sus propias APTs como método de financiación y contrapeso a las sanciones internacionales a las que está sometido. Para ello, está llevando a cabo ataques con motivación económica contra empresas del sector financiero, en concreto contra las llamadas Fintech y empresas de intercambio de criptomonedas o *exchanges*.

Esta financiación se reinvierte en el programa nuclear del país. No se han registrado grandes cambios en las TTPs de los actores y no se espera que lo hagan en el próximo 2024. En todo caso, aumentarán la actividad contra las criptomonedas aprovechando la recuperación del mercado.

Siendo Lazarus Group sin duda el grupo más predominante de origen norcoreano, este grupo se ha visto envuelto en ataques a diversos sectores. Los más afectados son el sector sanitario, de educación o de manufactura, entre otros. Como principal método de actuación, se conoce que Lazarus Group ataca a los fabricantes de soluciones con el fin de recopilar cualquier tipo de información disponible que sea sensible para obtener beneficio directo.

De acuerdo con Talos, recientemente se ha descubierto una nueva campaña por parte de este grupo llamada “Operation Blacksmith”. En concreto, esta campaña está siendo utilizada contra empresas de los sectores de fabricación, seguridad física y manufactura. Además, se conoce que se está haciendo uso de tres nuevas familias de *malware* basadas en Dlang; siendo dos de estos troyanos RAT que usan bots y canales de Telegram.

_ Actores con motivación ideológica_

HACKTIVISMO

El hacktivismo ha sufrido una mutación desde hace dos años, desde antes del inicio de la guerra en Ucrania. A los hacktivistas "tradicionales" se les han sumado hacktivistas que defienden las causas de una nación, lo que llamaremos de ahora en adelante, hacktivismo estatal.

En este sentido, el principal actor de hacktivismo estatal desde que se inició la guerra en Ucrania es NoName057(16), un grupo prorruso que ataca con denegaciones de servicio a naciones y empresas que se posicionan públicamente a favor de los intereses de Ucrania. Durante 2024 y el tiempo que dure el conflicto, lo más probable es que este actor seguirá presente y atacará principalmente a empresas e instituciones de Estados Unidos, Canadá y Europa.

A NoName057(16) se le ha sumado el actor Anonymous Sudan, que parece defender los ideales del islam y de Rusia. Este actor ha participado activamente en el conflicto entre Israel y Hamas, con la principal motivación de dejar inoperativos los servicios esenciales del adversario a través de ataques DDoS, principalmente.

Se habría de tener en cuenta que, cada vez con más frecuencia, se atribuirán campañas de desinformación a grupos hacktivistas, dado que ya en algunos conflictos, como en el de Israel y Palestina, se están observando campañas de propaganda y desinformación.

En 2024, este nuevo tipo de hacktivismo, que se dio a conocer en la guerra de Ucrania en 2022, se verá consolidado con el conflicto entre Palestina e Israel y es posible que traslade sus TTPs a las elecciones previstas para 2024.

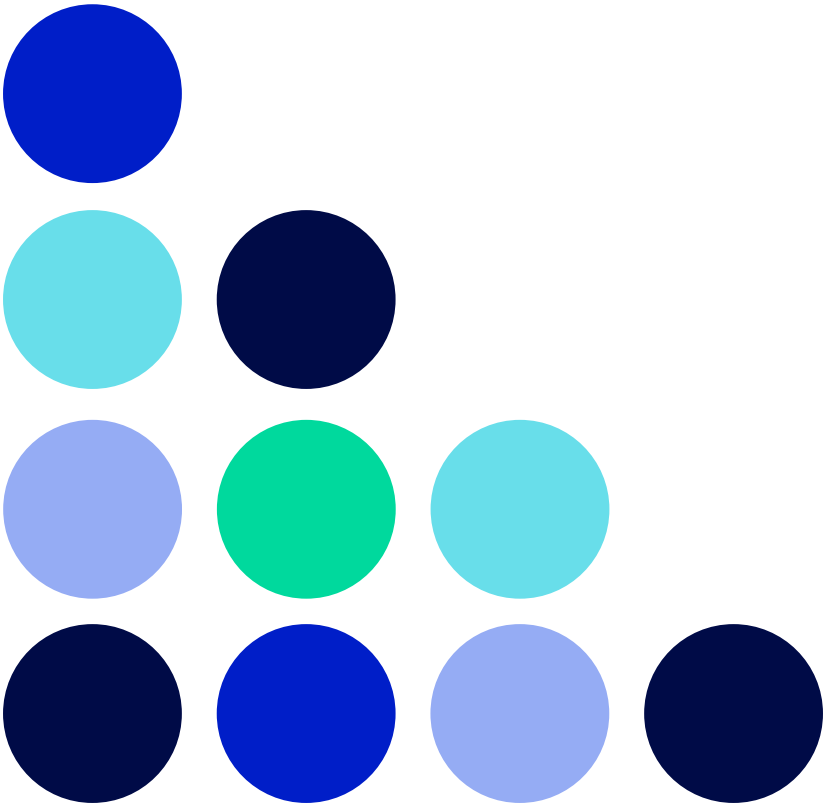
_ Actores con motivación económica o reputacional _

ACCESS BROKERS

Cada vez es más sencillo acceder a esta “profesión” del cibercrimen con poca cualificación, dada la accesibilidad a grupos cibercriminales que proporciona Telegram como nuevo gran foro de la Darknet.

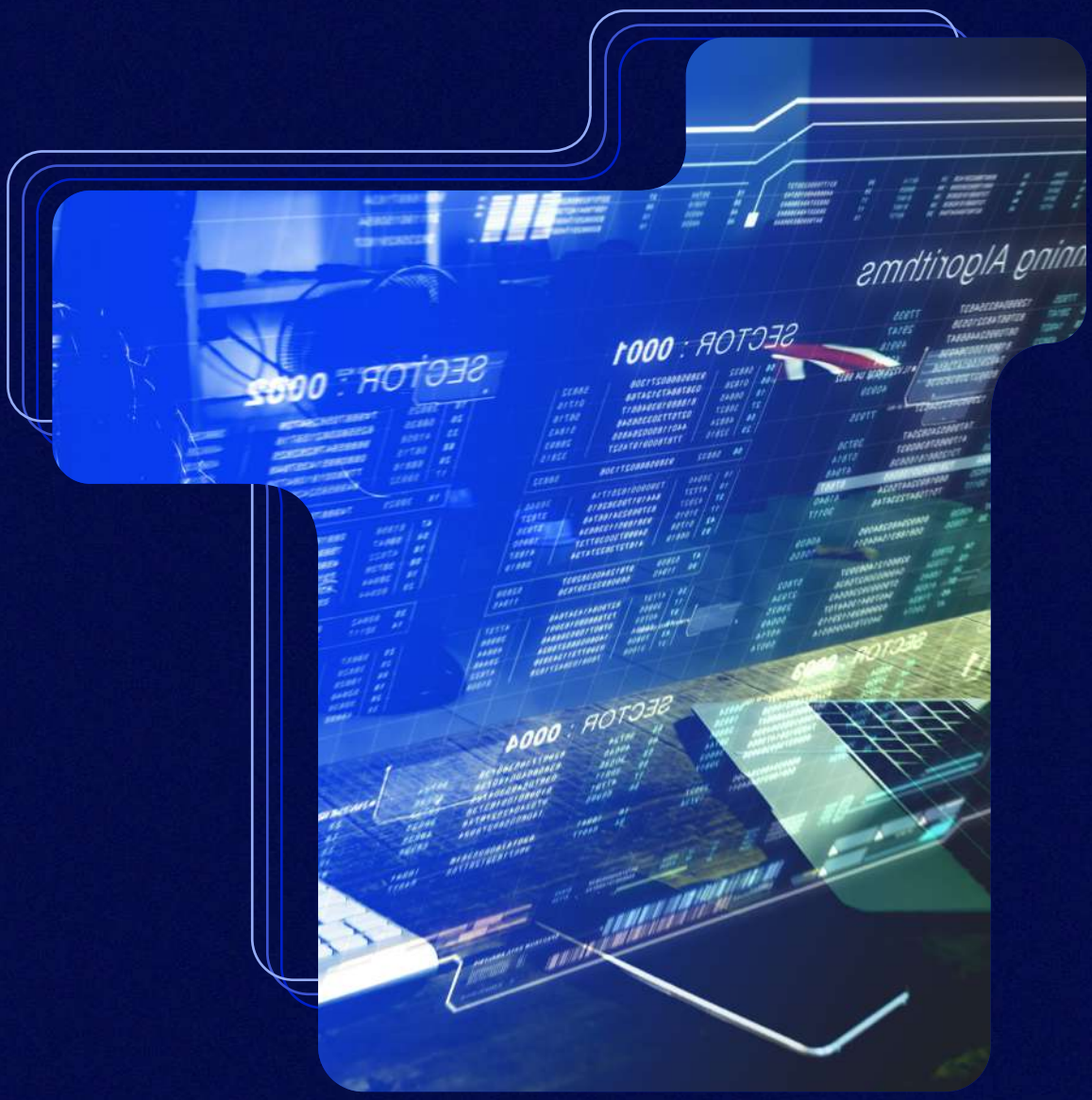
Como añadido, la información disponible en Internet y la ayuda de chats con IA, facilitan el acceso y la formación necesaria para desempeñar estos roles.

Además, a estos factores se le ha de añadir que la inestabilidad económica ya descrita es un motivador más para que un mayor número de personas se involucre en estas actividades.



BeDisruptive™

Grupos de *ransomware*



09

En este 2023 el *ransomware* no se queda atrás. Estados Unidos se ha visto fuertemente afectado con un 40% más de casos de *ransomware* de doble extorsión.

Tras conocer que este país ha sido uno de los principales objetivos, también se han visto afectados otros países como Canadá, Reino Unido y Alemania, los cuales han sufrido *data breaches*, pérdidas financieras e interrupciones operativas, atacando tanto a individuos como a organizaciones de mayor tamaño.

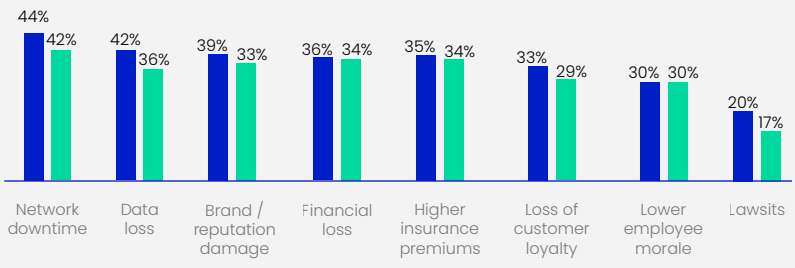
Cabe destacar que América Latina se encuentra entre las regiones más afectadas a causa de *ransomware*, *phishing* y troyanos bancarios durante 2023. Sin embargo, es notable la eficaz y diligente colaboración entre dichos países y las entidades privadas en consecuencia del alto riesgo de incidentes de ciberseguridad.

Las organizaciones gubernamentales de la región están en procesos intermedios para llevar adelante nuevas y resilientes estrategias de ciberseguridad con el fin de mitigar los daños ocasionados y proteger a la ciudadanía a causa de los incidentes de ciberseguridad.

Entre los sectores más atacados se destaca el sector salud, puesto que la abundancia de información sensible y la propia interconexión de los sistemas, unido a la transición digital, genera que este sector sean un blanco estratégico para los ciberdelincuentes. Junto a estas cifras, se suma que el sector cultural y de ocio aumentó el número de ataques de *ransomware* en un 430%, según ThreatLabz.

Se han identificado 25 nuevas familias de *ransomware* de doble extorsión o de extorsión sin cifrado. Esta tendencia de aumento en el número de ataques y en el número de familias de *ransomware* está consolidada y en 2024 muy probablemente se mantendrá.

Impacto de ciberataques de *ransomware*



Fuente: The State of Segmentation 2023

Actores principales de *ransomware* 2023

Si bien es conocido que 2023 ha sido un año donde se han visto afectados un amplio abanico de sectores a raíz del *ransomware*, esta amenaza ha destacado todavía aún más la necesidad urgente de fortalecer las medidas de ciberseguridad, junto a la adopción de estrategias robustas para evitar incidentes críticos en su mayor medida.

También se da por sentado que durante este 2024 se experimentará un fuerte incremento del "*ransomware* de baja cualificación" contra pequeñas y medianas empresas cuya resiliencia digital sea baja o nula.

CONTI

Aunque el grupo de *ransomware* Conti ha experimentado en su mayoría una disolución, se ha observado una veloz redistribución de sus integrantes en diversos grupos. Un ejemplo relevante es la presencia de estos actores en los grupos BlackBasta ó Karakurt.

Cl0p

Conocido por difundir altas cantidades de *phishing* y poseer una amplia gama de *malware* discreto, Cl0p se ha convertido en uno de los grupos más observados este año. Además, tras conocerse la reciente vulnerabilidad de MOVEit, se descubrió que Cl0p fue uno de los mayores explotadores de dicha brecha de seguridad.

Este grupo, con motivación financiera se conoce que ha afectado a diversos sectores tras sus ciberataques como por ejemplo la Administración Pública, la sanidad y la educación, entre otros.

Como punto a destacar, se ha descubierto recientemente que Cl0p está haciendo uso de Amadey Trojan Bot, el cual es utilizado para realizar el robo de datos e instalar *malware* malicioso en los dispositivos de la víctima.

BlackCat (ALPHV)

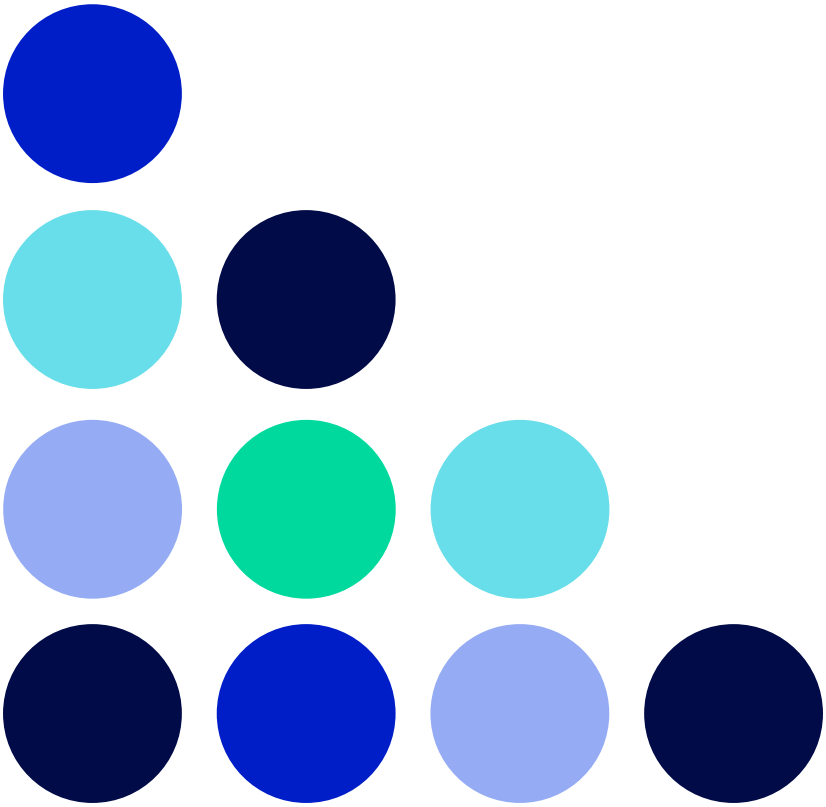
El principal vector de ataque inicial caracterizado por este grupo es el uso de anuncios de Google y Bing con el fin de promocionar sitios web falsos con carga útil de troyanos personalizados y comerciales.

Se conoce, que ALPHV ha afectado a los sectores sanitario, manufacturero y tecnológico, entre otros. Asimismo, es necesario destacar que recientemente han agregado la integración de APT60 a su web de *leaks* y han realizado la actualización de su cifrador de ficheros.

LOCKBIT

Conocido anteriormente como ABCD, LockBit ha evolucionado hasta convertirse en una subclase de *ransomware* o crypto-clase, debido a sus peticiones de rescate ante los incidentes de *ransomware* de doble extorsión.

Habiendo sido puesto como punto de mira por varias organizaciones de bajo y alto perfil, este grupo se posiciona como uno de los principales en el panorama del *ransomware* en 2023, acumulando +522 víctimas alrededor del mundo, según Trend Micro.



BeDisruptive™

Previsiones 2024 en el panorama de la ciberdelincuencia

10

La evolución del panorama cibernético presenta una serie de tendencias al alza que delinean los próximos desafíos en materia de la ciberseguridad de las organizaciones.

1 Desincronización entre motivación, actor y tipología de ataque, junto con cambios en el modus operandi de los diversos actores.

2 Consolidación de Telegram como el principal foro del cibercrimen, sirviendo de antesala a los foros más restringidos de la Darknet.

3 Aumento de vulnerabilidades en IoT, especialmente en el sector salud, debido a la rápida adopción de nuevos dispositivos interconectados y tecnologías.

4 Incremento en el uso de la inteligencia artificial.

5 Crecimiento del *ransomware*, con ataques dirigidos a vulnerabilidades en productos recién lanzados y en productos más antiguos.

6 Aumento en el empleo de ingeniería social y *phishing* para incrementar la efectividad de ciberataques.

7 Mayor énfasis en el control y gestión de puntos finales (*endpoints*) como medida preventiva frente a ataques, forzando a las entidades a adoptar un modelo SASE de ciberseguridad.

8 Creación de subgrupos de *ransomware* en respuesta a los *takedowns* de instituciones que combaten la ciberdelincuencia.

9 Incremento en el número de personas que ingresan al ámbito cibercriminal debido a la combinación de la IA y la presencia de actividades cibercriminales en Telegram, más accesible que las tradicionales en la DarkNet.

Bibliografía

- https://www.cnbc.com/2023/11/07/putin-looks-set-to-run-for-president-in-2024-and-theres-no-opposition.html
- https://carnegieendowment.org/politika/90753
- https://www.realinstitutoelcano.org/blog/la-nueva-politica-exterior-de-rusia/
- https://pages.eiu.com/rs/753-RIQ-438/images/EIU-Europe-outlook-2024.pdf?version=0&mkt_tok=NzUzLVJJUS00MzgAAAGPdnV6gf20tbv6CZ-Sn3inlVFNgr_ygz04mEjnR2Q-8sQYdliFaMlcCDV5lUaHuuBq7zOvxoRCyHalgAOgBjlIJlewgM91QD9pLR0l9s58Te9HOQ
- https://www.controlrisks.com/our-thinking/geopolitical-calendar?utm_referrer=https://www.google.es
- https://socradar.io/possible-cyber-threats-in-the-2024-olympics/
- https://www.american.edu/sis/global-election-tracker.cfm#south-america
- https://rm.coe.int/disinformation-and-electoral-campaigns/16809fa91f
- https://www.weforum.org/agenda/2023/09/global-economy-outlook-september-2023-chief-economists-outlook/
- https://pages.eiu.com/rs/753-RIQ-438/images/Financial-report-V5.pdf?mkt_tok=NzUzLVJJUS00MzgAAAGPR_6mGVBDf3F-cV-IBHH_IzOrhjwX4PUvhEsUsetdrAVEY3v6E_qymbiSqppD0_sk6kKr4MWJZg_6StBBRevLDOXC2Ab-jil5AmPHNol0FA0N5A
- https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
- https://www3.weforum.org/docs/WEF_Chief_Economists_Outlook_May2023.pdf
- https://pages.eiu.com/rs/753-RIQ-438/images/EIU-Europe-outlook-2024.pdf?version=0&mkt_tok=NzUzLVJJUS00MzgAAAGPdnV6gf20tbv6CZ-Sn3inlVFNgr_ygz04mEjnR2Q-8sQYdliFaMlcCDV5lUaHuuBq7zOvxoRCyHalgAOgBjlIJlewgM91QD9pLR0l9s58Te9HOQ
- https://www.bbvaresearch.com/publicaciones/situacion-espana-octubre-2023/
- https://unctad.org/es/publication/informe-sobre-el-comercio-y-el-desarrollo-2023
- https://www.imf.org/en/Publications/WEO/Issues/2023/10/10/world-economic-outlook-october-2023
- https://www.kroll.com/en/insights/publications/cyber/2023-geopolitical-and-economic-risks-davos
- https://purplesec.us/resources/cyber-security-statistics/#Crypto
- https://cincodias.elpais.com/cincodias/2022/01/22/mercados/1642849267_129516.html
- https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf
- https://ransomware.org/blog/mobile-phone-ransomware-a-primer/
- https://www.itsitio.com/seguridad/qbot-es-el-malware-mas-prevalente-en-2023-y-el-troyano-para-moviles-spinok-hace-su-debut-en-mas-de-100-aplicaciones-android-con-421-millones-de-descargas/
- https://securelist.com/it-threat-evolution-q1-2023-mobile-statistics/109893/
- https://www.varonis.com/blog/ransomware-statistics#mobile
- https://www.forbes.com/sites/bernardmarr/2023/11/01/the-top-5-artificial-intelligence-trends-for-2024/?sh=d5f53c62c349
- https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf
- https://www.forbes.com/sites/forbesbooksauthors/2023/08/04/artificial-intelligence-generative-ai-in-cyber-should-worry-us-heres-why/?sh=2684d81b204f
- https://emt.gartnerweb.com/ngw/globalassets/intl-es/information-technology/documents/las-principales-tendencias-tecnologicas-estrategicas-de-gartner-2024-ebook-es.pdf?_gl=1*1ppx5v1*_ga*NjY1ODMwNjQ1LjE3MDA2NDQ5MzE.*_ga_R1W5CE5FEV*MTcwMDY0NDkzMC4xLjEuMTcwMDY0NTAwOC40OS4wLjA
- https://www.boe.es/doue/2022/333/L00080-00152.pdf
- https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962
- https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
- https://www2.deloitte.com/content/dam/Deloitte/us/Documents/energy-resources/us-eri-renewable-energy-outlook-2023.pdf
- https://www.microsoft.com/en-us/security/blog/2023/07/25/cryptojacking-understanding-and-defending-against-cloud-compute-resource-abuse/
- https://www.zscaler.es/press/zscalers-ransomware-report-2023-shows-global-ransomware-attack-growth-of-nearly-40-percent
- https://www.welivesecurity.com/es/cibercrimen/5-grupos-ransomware-activos-america-latina-2023/
- https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/
- https://www.obrela.com/advisory/lockbit-3-0-increased-ransomware-attacks/
- https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/threat-intelligence-report-nov/Blackberry-Global-Threat-Intelligence-Report-November-2023.pdf
- https://techhq.com/2023/10/what-we-know-about-lockbit-ransomware/
- https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-clop-prevail-as-top-raas-groups-for-1h-2023
- https://blog.qualys.com/qualys-insights/2023/09/26/qualys-survey-of-top-10-exploited-vulnerabilities-in-2023
- https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
- https://securityscorecard.com/blog/top-5-security-vulnerabilities-of-2023/
- https://go.checkpoint.com/2023-cyber-security-report/chapter-03.php
- https://firewalltimes.com/recent-data-breaches/
- https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#top-data-breach-stats
- https://vulnera.com/2023/01/03/vulnerability-statistics-for-2023/
- https://www.getastra.com/blog/security-audit/data-breach-statistics/#
- https://www.picussecurity.com/hubfs/Red%20Report%202023/RedReport2023-Picus.pdf?hsCtaTracking=a6b9f00e-0309-4be1-9d07-ec3bbd7ffe4c%7Ce5400384-e2ec-4a46-97ac-bbdfedf8c6e2
- https://any.run/cybersecurity-blog/malware-trends-q1-2023/
- https://any.run/cybersecurity-blog/malware-trends-q2-2023/#top-mitre-attck-techniques-in-q2-2023-5406
- https://any.run/cybersecurity-blog/malware-trends-q3-2023/
- https://blog.checkpoint.com/security/hacktivism-in-2023-from-grassroots-movements-to-state-sponsored-threats/
- https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/
- https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/
  https://thehackernews.com/2023/11/iran-linked-imperial-kitten-cyber-group.html
- https://socradar.io/apt-profile-who-is-lazarus-group/
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations
- https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/
- https://www.csoonline.com/article/650413/north-koreas-lazarus-group-hits-organizations-with-two-new-rats.html
- https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/
- https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia
- https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china
- https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3676-2023-annual-threat-assessment-of-the-u-s-intelligence-community
- https://www.isaca.org/resources/reports/state-of-cybersecurity-2023
- https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
- https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
- https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
- https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF
- https://www.flashpoint.io/blog/risk-intelligence-year-in-review/
- https://www.ibm.com/downloads/cas/DB4GL8YM
- https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2023.pdf
- https://redcanary.com/resources/guides/threat-detection-report/
- https://www.mandiant.com/resources/reports/get-your-copy-m-trends-2023-today
- https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/rethinking-tactics-annual-cybersecurity-roundup-2022
- https://www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023-latam/
- https://www.checkpoint.com/about-us/investor-relations/annual-reports/
- https://www.cyberark.com/resources/ebooks/cyberark-2023-identity-security-threat-landscape-report
- https://www.recordedfuture.com/2022-annual-report
- https://www.kelacyber.com/wp-content/uploads/2023/01/KELA-RESEARCH_THE-CYBERCRIME-INFERNO_2022-ANNUAL-REPORT.pdf
- https://intel471.com/resources/whitepapers/the-471-cyber-threat-report-2023
- https://media.telefonicatech.com/telefonicatech/uploads/2021/1/164343_security-status-report-2022-h2-es.pdf
- https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023
- https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file?format=html
- https://s2grupo.es/noticias-y-publicaciones/page/4/
- https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2023-cyber-threat-report.pdf
- https://www.s2lsec.com/es/threat-landscape-report-2023-01/
- https://www-silicon-es.cdn.ampproject.org/c/s/www.silicon.es/la-ue-aprueba-una-historica-primera-ley-sobre-inteligencia-artificial-2491811/amp

BeDisruptive™

It's an attitude

Limiting threats for an unlimited future.

Paseo de la Castellana 259C, Plta.33, Madrid

Contáctanos en info@bedisruptive.com

Llámanos al +34 911 91 10 90

www.bedisruptive.com