ágoraSIC Centro de Conocimiento en Ciberseguridad

Los quebrantaversos salen de caza

Amenazas y ciberataques en 2023: ¿cuáles serán los más complejos y de gran impacto, se esperen o no?

SUMARIO

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

LOS QUEBRANTAVERSOS

La sociedad ya atesora una cierta experiencia en el padecimiento de ciberataques. Y a la hora de vaticinar lo que nos espera este año, los expertos han dejado patente que las acciones y los artefactos técnico-sociales principales (*phishing*, *ransomware*, *malware*, denegaciones de servicio, suplantación de identidad...) y las tipologías delictivas en las que se materializan (robo, extorsión, fraudes variados, tráficos ilícitos de personas y bienes, financiación de organizaciones y actividades delictivas...), van a seguir creciendo durante este año. Al tiempo vislumbran

"En 2023 habrá más de 45.000 millones de dispositivos IoT en todo el mundo. La potencial amenaza es su grado de inseguridad, considerando la gran cantidad de información que almacenan. Mitigar este riego no es actualmente la prioridad de los fabricantes".

"Vamos a ver un aumento de incidentes por filtración de datos desde la Nube por error del usuario. Ya sea por deficiencias de diseño de la arquitectura de servicio como por configuración insegura de los servicios, como por errores en la operación diaria".

"Aumento de 'Ciberataques en los Metaversos' (modificación de código, secuestros de perfiles de usuarios, etc.): industrial, compras, juegos, socialización, medicina, finanzas, etc.".

"Los Seguros de Ciber riesgos empiezan a incluir restricciones de cobertura a los ataques a la cadena de suministro, como anteriormente introdujeron limitaciones al *ransomware*".

"Se espera que el *malware* generado por IA se generalice. La suplantación de voz con IA para fines fraudulentos va a ser una amenaza creciente".

"Algunos países europeos pueden exigir la notificación de los pagos de rescates por *ransonware*".

"Es previsible que continuemos con una tendencia de ataques al sector 'cripto'".

"Crece el apetito por los Cyber Phisical Systems (CPS) y el presupuesto de los gobiernos a los "ciberejércitos" (defensivos y ofensivos)".

"El propio sector de la ciberseguridad se está saboteando al contribuir al problema de la falta de talento, amenazando su sostenibilidad sin necesidad de ataques externos".

"Será bastante común ver cómo algunas organizaciones son comprometidas debido al compromiso previo de alguno de sus proveedores o productos (incluidos productos de seguridad)".

... SALEN DE CAZA

–más allá del uso de la IA para el "mal"– la evolución de ideas creativas en la cada vez más engrasada maquinaria de la ciberdelincuencia (organizada mucho o poco) para encontrar nuevos y cómodos caladeros y, también, para sacarle mayor partido a las necesidades de algunos estados para fomentar trifulcas y conflictos a todos los niveles. Esta ha sido la pregunta de SIC: "Amenazas y ciberataques en 2023: ¿cuáles serán los más complejos y de gran impacto, se esperen o no?" Y aquí están las respuestas. Nada menos que de 272 actores, sin duda el muestreo más grande jamás hecho en España.

"La privacidad seguirá quebrada mientras no se erradique la actividad, no reglada cuando no abiertamente ilegal, de los 'corredores de datos' y el creciente mercadeo en la Darknet".

"Entendiendo el ransomware como una denegación de servicio de acceso (disponibilidad), lo siguiente es pensar en ataques a la Integridad semántica de los sistemas".

"Se espera un aumento de ciberataques con motivaciones políticas y el enfoque de grupos de ransomware en datos médicos y personales".

"Va a ser el año del cibercrimen a sueldo: el *ransomware*, el *phishing* o los ataques DDoS estarán disponibles *as a Service*, todo ello unido a la triple extorsión (cifrado de sistemas, publicación de datos y ataques de denegación de servicio).

"La amenaza más importante en el futuro más cercano es el acercamiento del crimen organizado tradicional al cibercrimen. Por este motivo, aparecerán operativas criminales de mayor gravedad, principalmente en la forma de ciberextorsiones".

"Incremento notable de ciberataques y ciberamenazas en el área de los 'Gemelos Digitales' (MITM, fuga de información, manipulaciones, DDoS, vulnerabilidades, etc.) en todos sus espacios: físico-digital-comunicaciones, por ejemplo, en los ecosistemas de producción industrial (plantas, productos, procesos)".

"Si los ciberdelincuentes son listos, no veremos ningún ataque que pueda hacernos reaccionar como sociedad de manera más decidida".

"Seguirán apareciendo vulnerabilidades en pequeños módulos de software que, inexplicablemente, utilizan la mayoría de las aplicaciones y que desarrolló, desinteresadamente, un programador de...".

"Muchas organizaciones no cuentan con un inventario de los sistemas criptográficos empleados, ni utilizan el paradigma de agilidad criptográfica (*crypto-agility*)".

UNIÓN EUROPEA

COMISIÓN EUROPEA

Josep Borrell
Alto Representante de la UE
y Vice-presidente de la Comisión Europea

"La guerra cibernética y los ciberataques se han convertido en una parte integral de la guerra moderna. (…) Estamos proponiendo acciones para aumentar nuestra capacidad de prevenir, detectar, disuadir los ataques cibernéticos y defendernos de ellos. (…). La Comisión Europea está haciendo mucho en el aspecto civil de la ciberdefensa y en el ámbito militar. Tenemos que unir estos dos lados. Debemos crear las estructuras y mecanismos de cooperación entre los actores militares para mejorar la conciencia situacional, la detección, la preparación y la respuesta. Por eso, proponemos en este plan crear un Centro de Coordinación de Ciberdefensa de la UE. Actuaría como un nodo central para recopilar, analizar y distribuir información de defensa cibernética. Además, estableceremos una red operativa de Equipos Militares de Respuesta a Emergencias Informáticas con la Agencia Europea de Defensa actuando como secretaría. También, ampliaremos nuestros Equipos de Rápida Reacción Cibernética y ejercicios de ciberdefensa. Del mismo modo, debemos abordar las brechas en la fuerza laboral de defensa cibernética. (…). Y también intensificaremos nuestro trabajo en apoyo del desarrollo de capacidades de defensa cibernética de nuestros socios. (…).
Estamos presentando estas soluciones concretas, cumpliendo compromisos y ambiciones que ya anunciamos cuando aprobamos la brújula estratégica. Estoy seguro de que esto hará de la Unión Europea un actor mundial más fuerte en materia de seguridad y defensa".

**En su discurso durante la rueda de prensa sobre el Paquete de Seguridad y Defensa. 10 de noviembre de 2022.*

COMISIÓN EUROPEA

Thierry Breton
Comisario Europeo de Mercado Interior

"En lo que respecta a la ciberseguridad, Europa es tan fuerte como su eslabón más débil: ya sea un Estado miembro vulnerable o un producto inseguro a lo largo de la cadena de suministro. Ordenadores, teléfonos, electrodomésticos, dispositivos de asistencia virtual, coches, juguetes… todos y cada uno de estos cientos de millones de productos conectados son un posible punto de entrada para un ciberataque y, sin embargo, hoy en día la mayoría de los productos de hardware y software no están sujetos a ninguna obligación de ciberseguridad. Introduciendo la ciberseguridad por diseño, la Ley de Resiliencia Cibernética ayudará a proteger la economía de Europa y nuestra seguridad colectiva".

**Durante la presentación de la propuesta para una nueva Ley de Resiliencia Cibernética. Estado de la Unión. 15 de septiembre de 2022.*

EUROPOL

Philipp Amann
Head of Strategy, European Cybercrime Centre

"Es seguro asumir que los ciberataques continuarán intensificándose y el *ransomware* seguirá siendo una amenaza clave para las empresas, facilitado por un modelo maduro de *Crime-as-a-Service*. Los delincuentes seguirán adaptándose y empleando nuevos métodos, por ejemplo, mediante el uso de *deepfakes* para mejorar los ataques de ingeniería social. A medida que la *'IA-as-a-Service'* continue creciendo con servicios como ChatGPT o Stable Diffusion, los delincuentes buscarán formas de abusar de ellos en áreas como el CEO o el fraude de inversiones.
Con la adopción más amplia de las finanzas descentralizadas, también se espera que aumenten los ataques contra los servicios y las herramientas DeFi (*Decentralized Finance*). Así pues, las empresas deben continuar invirtiendo en medidas de ciberseguridad y capacitación del personal; no solo para mitigar las amenazas, sino también para prepararse para una nueva legislación, como NIS2".

BANCO CENTRAL EUROPEO

Kerstin af Jochnick y Mario Quagliariello
Miembro del Consejo de Supervisión del BCE
y Director de Estrategia y Riesgo Supervisor,
respectivamente

"La seguridad de TI/el riesgo cibernético y los riesgos relacionados con el clima y medioambientales son algunos de los retos más importantes para los bancos y seguirán estando entre nuestras prioridades de supervisión.
Con respecto al primero de estos factores, la transformación digital en el sector bancario y la mayor dependencia de las nuevas tecnologías y los proveedores de servicios externos han aumentado la complejidad y la interconectividad en el sistema financiero. Los ciberataques, en particular, se han convertido en los últimos años en un desafío importante para la resiliencia operativa de los bancos, y son especialmente difíciles de gestionar debido tanto a la creciente complejidad y la naturaleza cambiante de las amenazas, como a su dimensión transfronteriza.
La situación geopolítica actual plantea nuevos retos, a este respecto. Si bien la amenaza de ciberataques masivos al sector bancario europeo en respuesta a las sanciones impuestas a Rusia por la Unión Europea y otras economías avanzadas aún no

se ha materializado, el número de ciberincidentes comunicados por las entidades supervisadas siguió creciendo en 2022. Sin embargo, el número total de estos ciberincidentes, que parece relativamente estable, es similar al observado en 2021, y su impacto real ha sido contenido hasta ahora.

Ello requiere extrema prudencia y un mayor control tanto por parte de los bancos, como de los supervisores. Seguiremos colaborando estrechamente y de forma individualizada con los bancos, mediante revisiones horizontales e inspecciones in situ, con el objetivo de fortalecer sus marcos de seguridad informática y resiliencia cibernética".

** Basado en el artículo publicado en el Blog de Supervisión del 12 de diciembre de 2022*

CENTRO EUROPEO DE COMPETENCIA EN CIBERSEGURIDAD (ECCC)

Miguel González Sancho

Director Ejecutivo interino

"En 2023 cabe esperar que algunas de las grandes amenazas de ciberseguridad actuales se mantengan, las cuales a menudo están relacionadas. En particular los ataques que afectan a infraestructuras críticas, a la cadena de aprovisionamiento y a vulnerabilidades de software. También que muchas más pymes se vean afectadas y que la extensión de las aplicaciones de inteligencia artificial conlleve un aumento de los ciberataques en ese ámbito. Creo que ello podría tener como efecto positivo una mayor exigencia del cumplimiento de normas de seguridad ('*compliance*'), por ejemplo, a los proveedores de ciertas empresas, así como fomentar la evaluación y certificación de la conformidad con dichas normas por parte de organizaciones, servicios y productos. La normativa europea reciente de ciberseguridad va en ese sentido, por ejemplo, la revisión de la Directiva "NIS" y la propuesta de la Comisión sobre el "Acta para la Cyber Resiliencia".

ENISA

Vicente González Pedros

Research and Innovation Team

"El último informe anual de Enisa que analiza el Panorama de Amenazas (*Enisa Threat Landscape 2022- ETL*) y que este año llega a su décima edición destaca el impacto de la geopolítica en el panorama de amenazas a la ciberseguridad y considera las vulnerabilidades Zero-Day como el nuevo recurso de los astutos actores de amenazas para lograr su objetivo. Además, el *ransomware* y los ataques contra la disponibilidad ocupan los primeros lugares durante el período del informe. Hemos detectado que más de 10 terabytes de datos son robados mensualmente en ataques de *ransomware*. No faltan las amenazas novedosas, híbridas y emergentes están marcando el panorama de amenazas con un alto impacto.

Comprender las tendencias relacionadas con los actores de las amenazas, sus motivaciones y sus objetivos ayuda en gran medida a planificar las defensas de ciberseguridad y las estrategias de mitigación. Así, se consideran las siguientes cuatro categorías de actores de amenazas a la ciberseguridad: los patrocinados por el estado, el cibercrimen, ciberdelincuentes a sueldo, hakctivistas… De cualquier forma, ENISA mantiene un análisis continuo de tendencias, patrones e información de cada una de las amenazas que se presentan en el informe.

AGENCIA ESPACIAL EUROPEA (ESA)

Massimo Mercatti

Autoridad de Seguridad de la ESA y Jefe de la Oficina de Seguridad

"La evolución del panorama de amenazas aplicadas al dominio espacial está mostrando en los últimos diez años una curva exponencial, justificada con la introducción de nuevas tecnologías, y enfocada en detrimento del servicio que produce el dominio espacial. De hecho, el dominio espacial se ha convertido en un pilar clave para la economía, la seguridad y el aspecto civil de Europa. Cualquier ataque dirigido en perjuicio del dominio espacial tendría un impacto directo en la economía, la seguridad y el aspecto civil del país europeo. Pensemos en un ataque al sistema Galileo enfocado a comprometer la señal del servicio abierto. El impacto a nivel político y económico sería realmente perjudicial. Además, un ataque a la seguridad puede enfocarse también para comprometer la integridad de la fase de diseño, falsificando el diseño y los requisitos de los Programas Espaciales Principales.

La ESA con su Oficina de Seguridad en los últimos dos años ha trabajado arduamente para coordinar dos corrientes principales de actividad. Por un lado, la Resiliencia Cibernética de ESA que aborda la capacidad distribuida de ESA para monitorizar un Sistema Espacial desde la fase de diseño hasta la fase operativa, detectando cualquier tipo de ataque desde tierra o desde el espacio. De hecho, la primera configuración de resiliencia cibernética distribuida entre ESEC-ESOC-ESRIN estará operativa en 2024. Por otro, la actividad de investigación y desarrollo de Seguridad Cibernética de la ESA, coordinada por ESO (*ESA Security Office)* en sinergia con TEC, TI, OPS, representa el núcleo de un conjunto de nuevos proyectos de tecnología cibernética que abordan la protección del satélite, la protección de la misión terrestre y el segmento de control, y la verificación y certificación de seguridad de tecnología cuántica y post cuántica aplicada al dominio espacial.

ESO está construyendo alrededor de la ESA una capacidad cibernética única, en términos de resiliencia e I+D, con el objetivo de tener una red cibernética europea liderada por la ESA y respaldada por todos los activos cibernéticos de los Estados miembros".

UCRANIA

SERVICIO ESTATAL DE COMUNICACIONES ESPECIALES Y PROTECCIÓN DE LA INFORMACIÓN DE UCRANIA

Victor Zhora
Chief Digital Transformation Officer

"Ucrania ha estado en estado de guerra durante los últimos 9 años, desde que las tropas rusas que vestían uniformes sin ninguna insignia comenzaron a tomar edificios administrativos en Crimea, lo que resultó en la anexión de la península por parte de la federación rusa. Desde 2014, hemos sufrido numerosos ataques cibernéticos a la infraestructura de información de Ucrania, llevados a cabo por piratas informáticos afiliados al ejército ruso. Durante esos 9 años, tenemos suficiente información sobre las estrategias, métodos y herramientas que utilizan los rusos para sus ciberataques. Este conocimiento nos permite predecir el comportamiento del enemigo.

Comencemos con una pregunta fácil de lo que NO esperamos: definitivamente no esperamos que cesen los ataques cibernéticos. El componente cibernético se ha convertido en una parte importante de la guerra híbrida en curso contra Ucrania. Los ciberataques complementan tanto las ofensivas terrestres del enemigo como las operaciones psicológicas. Esto se desprende del estudio de ciberataques que nuestro Servicio ha realizado junto con nuestros socios. Está disponible como archivo descargable debajo de la información vinculada: **https://cip.gov.ua/en/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi**

El régimen de Putin se ha fijado el objetivo inequívoco de destruir Ucrania, los ucranianos y todo lo relacionado con el idioma y la cultura ucraniana. Utilizan todas las herramientas disponibles, incluidos los ciberataques, para lograr este objetivo. Además, es probable que nos enfrentemos a nuevos ciberataques complejos y bien preparados en el futuro. Tras la oleada de poderosos ataques que tuvieron lugar antes de la invasión militar a gran escala de Rusia en Ucrania y en los primeros meses de la guerra, la cantidad de ataques graves ha disminuido ligeramente desde el verano hasta el final del año. La preparación para nuevos ataques cibernéticos de alta complejidad puede ser una de las razones detrás de eso.

Por lo tanto, nuestra tarea es estar lo más preparados posible para contrarrestarlos. Tenemos varios escenarios posibles y estamos mejorando sistemáticamente nuestra resiliencia cibernética, considerando los menos optimistas.

Otra tendencia de 2022 que no cambiará en este año y los siguientes se basa en el hecho de que el ciberespacio no tiene fronteras, a diferencia del espacio físico. Los piratas informáticos militares rusos se han aprovechado de esto repetidamente para atacar los recursos de información de los países que apoyan a Ucrania, enviarnos ayuda humanitaria, armas u otros equipos. Sin duda, el número de ataques a las democracias maduras seguirá aumentando. Esto debería alentar a todo el mundo democrático a revisar la actitud hacia los delitos cibernéticos y su evaluación legal. Así como para crear un sistema de defensa colectiva en el ciberespacio, ya que las amenazas cibernéticas aumentan y el mundo necesita estar preparado para enfrentarlas antes de que sea demasiado tarde. Estamos listos para compartir la información que tenemos con nuestros socios para contribuir a un mundo digital más seguro".

ACTORES INTERNACIONALES RELEVANTES

AGENCIA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFRAESTRUCTURA, EN EE.UU. (CISA)

Jen Easterly
Directora

"Los gobiernos y las empresas de todo el mundo dependen cada vez más de la tecnología, una revolución digital que ha creado enormes recompensas y riesgos inimaginables.

A medida que nos adentramos en 2023, el panorama de las amenazas cibernéticas es más complejo y diverso que nunca, y abarca desde estados nacionales sofisticados hasta ciberdelincuentes cada vez más capaces.

Si queremos tener la oportunidad de interrumpir la trayectoria de esta amenaza, en particular la que plantean las naciones adversarias que no están restringidas por las normas y los valores apreciados por las democracias de todo el mundo, necesitamos un nuevo modelo de ciberseguridad sostenible, uno en el que los incentivos se realinean para favorecer las inversiones a largo plazo en la seguridad y la resiliencia de nuestro ecosistema tecnológico, y donde las naciones afines reconozcan una responsabilidad compartida para nuestra ciberdefensa colectiva".

ANDORRA DIGITAL

Jordi Ubach
AD National Cybersecurity Agency of Andorra

"En 2023 habrá más de 45.000 millones de dispositivos IoT en todo el mundo. Dispositivos personales, maquinaria industrial, *smart cities*... son gran parte de la variedad tecnológica a proteger de forma segura. En este contexto, remarcar que la potencial amenaza es la Inseguridad, considerando la gran cantidad de información que se acaba almacenando en los propios dispositivos. Mitigar esta potencial amenaza no es actualmente la prioridad de los fabricantes, como por ejemplo aplicando actualizaciones o parches en el *firmware*. Estas vulnerabilidades, y la falta en general de seguridad, derivan en puertas traseras con acceso ilícito al dispositivo, o a la red interna del usuario o empresa, aspectos que raramente se solucionan. Nuevas iniciativas internacionales van en la dirección correcta y obligarán a que los fabricantes apliquen una capa de seguridad extra en sus dispositivos, simplemente para proteger el bien más preciado: la protección del usuario final".

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE) ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

Alison August Treppel
Secretaria Ejecutiva

"En un mundo donde se invierten millones de dólares anualmente para digitalizar y automatizar los servicios, la mayor amenaza para 2023 sería que los responsables de la toma de decisiones del sector público y privado no presupuesten los recursos necesarios, incluidos los recursos humanos, para responder a incidentes cibernéticos. La línea de amenazas ha crecido exponencialmente, y sin personal capacitado y dedicado la ventana de oportunidad para la minería de datos a gran escala o las interrupciones del servicio se abre aún más. Dado el panorama político cambiante en las Américas, anticipamos que este desafío se agudizará en nuestra región, con posibles brechas en la transferencia de habilidades entre los gobiernos en transición".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

FIRST
Sherif Hashem
Chair

"En los últimos años, el *ransomware* dirigido se ha convertido en la principal amenaza cibernética visible. Del mismo modo, existe una creciente preocupación por la propagación de ataques cibernéticos sofisticados dirigidos a la infraestructura y las cadenas de suministro en sectores críticos, incluidos los sectores de energía, telecomunicaciones, finanzas, atención médica y servicios gubernamentales. Los ataques cibernéticos avanzados a menudo están motivados por ganancias financieras, pero a veces están impulsados por fines políticos y de espionaje. Los equipos de seguridad están mejorando en la defensa contra tales ataques cibernéticos. La adopción de principios y modelos de confianza cero en las soluciones y herramientas de seguridad puede mejorar aún más la resiliencia cibernética. Sin embargo, la cooperación global y regional son esenciales para defenderse de ataques cibernéticos avanzados y lograr plataformas digitales seguras y confiables".

FORO ECONÓMICO MUNDIAL
Filipe Beato
Lead, Centre for Cybersecurity

"La seguridad cibernética sigue siendo el riesgo tecnológico mejor clasificado y los ataques cibernéticos a la infraestructura crítica son el impacto más grave para las economías globales, según el informe 'Global Risks'. Los conocimientos recientes en Davos sugieren que asegurar la infraestructura crítica sigue siendo una prioridad debido a los ataques cibernéticos sofisticados con la capacidad de escalar a diferentes entornos e industrias mientras navegan por sus complejas cadenas de suministro. Si bien el 86 % de los líderes empresariales y el 93 % de los líderes cibernéticos creen que un ciberataque global es inminente en los próximos dos años, eso podría tener un impacto catastrófico".

NATIONAL SECURITY AGENCY DE EE.UU. (NSA)
Rob Joyce
Director

"No alentaría a nadie a ser complaciente o despreocupado por las amenazas al sector energético a nivel mundial. A medida que avanza la guerra [de Ucrania], ciertamente existen oportunidades para aumentar la presión sobre Rusia a nivel táctico, lo que hará que reevalúen, prueben diferentes estrategias para liberarse".

OFICINA FEDERAL PARA LA SEGURIDAD DE LA INFORMACIÓN DE ALEMANIA (BSI)

Gerhard Schabhüser
Vice President of the Federal Office for Information Security

"Los ataques de *ransomware* han sido la mayor amenaza operativa en 2022. Además de eso, se observaron incidentes y campañas de *hacktivismo* como DDoS en el contexto de la guerra rusa contra Ucrania. También continuó el agravamiento de los métodos de extorsión digital, así como los ataques de amenazas persistentes avanzadas. En 2023, el *ransomware* seguirá siendo una de las mayores amenazas operativas, especialmente contra organizaciones más grandes para obtener el rescate más alto posible. El aumento de la interconectividad digital y las dependencias de las cadenas de suministro contribuyen a una superficie de ataque posiblemente mayor. Finalmente, la guerra rusa contra Ucrania podría conducir a un *hacktivismo* continuo y otros incidentes cibernéticos. Por lo tanto, BSI espera que la situación no mejore, sino que se vuelva aún más volátil".

OTAN
Jens Stoltenberg
Secretario General

"Parte de la agresión de Rusia es una guerra invisible en el ciberespacio. En las horas inmediatamente anteriores a que las fuerzas rusas cruzaran la frontera, los ciberataques afectaron a los departamentos del gobierno, el ejército y los servicios de emergencia de Ucrania. La red satelital ViaSat fue forzada fuera de línea. (…) Los ataques de 'borrado de datos' se han dirigido a los sectores gubernamental, comercial y energético ucranianos. Y un ciberataque al sistema ferroviario intentó interrumpir no solo el transporte de suministros militares al frente, sino también la evacuación de los ciudadanos ucranianos. (…) El ciberespacio no debería ser un 'Salvaje Oeste' libre para todos. Todos los aliados están de acuerdo en que los derechos fundamentales y el derecho internacional se aplican tanto en línea, como *off line*. (…) La amenaza del ciberespacio es real y está creciendo. Es por eso que nuestro Compromiso de Defensa Cibernética es tan importante. Así que hago un llamado a los aliados para que vuelvan a comprometerse con la ciberdefensa, con más inversión, más experiencia y una mayor cooperación".*

** Durante su intervención en la Conferencia de Compromiso de Ciberdefensa de la OTAN en Italia. 10 de noviembre de 2022.*

ONU
Dra. Camino Kavanagh
Investigadora Visitante Senior, King's College London / Consultora Naciones Unidas y otras entidades internacionales

"Este 2023 será un año, otra vez, de mucha actividad multilateral llevada a cabo en un entorno geopolíticamente complejo. Inicia enero con la primera sesión del Grupo Ad-Hoc de la ONU sobre el 'borrador negociador para un tratado internacional sobre el cibercrimen'. El documento consolida las presentaciones anteriores de los estados miembros, que en buena parte reflejan el contenido del Convenio sobre la Ciberdelincuencia del Consejo de Europa y el Convenio de la ONU sobre el Crimen Organizado. Aun así, son varios los temas que frenarán la posibilidad de un consenso rápido en los diferentes grupos de trabajo sobre provisiones generales, criminalización, y medidas de procedimiento y aplicación de la ley.

Por otro lado, el Grupo de Trabajo de Composición Abierta (OEWG) de la ONU sobre las TIC y la seguridad internacional tendrá dos sesiones este año, en marzo y julio, respectivamente. Cómo no, las negociaciones se pintan complejas, incluso sobre propuestas como el establecimiento de un directorio global de puntos de contacto gubernamentales para el intercambio de información y la cooperación en caso de incidentes, propuesta apoyada por España mientras sea una medida voluntaria, que contribuya a la implementación de medidas de confianza y normas existentes, que no duplique los esfuerzos de otras organizaciones y que sea practicable. Otro tema que se discutirá acaloradamente este año es la propuesta de Egipto y Francia para una plataforma permanente de dialogo y acción sobre las TIC en el seno de la ONU, el llamado Programa de Acción. Mientras la propuesta fue aprobada con una mayoría significativa en el primer comité de la Asamblea General a finales del 2022, queda mucho camino para que vea la luz del día".

AUTORIDADES PÚBLICAS COMPETENTES Y DEPARTAMENTOS DE LA AGE

CCN – CENTRO CRIPTOLÓGICO NACIONAL

Carlos Abad
Jefe del Área de Sistemas de Alerta y Respuesta a Incidentes del CCN

"Aunque en 2022 hubo cierta inquietud a que, por la guerra Ucrania-Rusia, España sufriera ciberataques disruptivos directos o colaterales (por *wipers*, ataques a servicios satelitales o DDoS), el hecho es que sólo se detectaron algunas acciones menores de grupos *hacktivistas* prorrusos contra nuestro país. La situación actual de la guerra no hace prever un cambio de tendencia, aunque habrá que mantenerse vigilantes.

En líneas generales, el fraude/estafa digital seguirá siendo el que gane en número de incidentes (mediante *phishing*, *smishing*, *vishing*, etc..), pero por complejidad e impacto tanto el ciberespionaje como el cibercrimen, especialmente el *ransomware*, seguirán siendo el dolor de cabeza de las organizaciones.

En particular, los sospechosos habituales del ciberespionaje como APT28, APT29, TURLA, los PANDA, Lazarus u otros actores sin etiquetar aún, seguirán trabajando en el robo de información y propiedad intelectual. Se basarán en la explotación de accesos remotos y de servicios expuestos (como el correo o la nube en general), a lo que se une recientemente los intentos de infiltración en *routers* de comunicaciones, para creación de túneles y descifrado de comunicaciones internas.

Por su parte, los grupos de *ransomware*, a pesar de peleas internas (véase Conti Leaks) o de operaciones policiales en el pasado con detenciones y desmantelamiento de infraestructuras (Revil, Emotet, ...), gozan de buena salud y se readaptan con cierta facilidad. La estrategia de doble extorsión, cifrado y exfiltración, ya es dominante. Es de esperar que los ataques de mayor impacto sean causados por este tipo de actores de la amenaza.

Además, el mercado negro en *Darkweb* de compra/venta de accesos es cada vez más maduro y opera con facilidad en múltiples canales, más seguros y anónimos.

La superficie de exposición y vulnerabilidad, a pesar de los esfuerzos, sigue siendo amplia, especialmente si incluimos también la de la cadena de suministro (proveedores de servicio IT, Cloud y componentes *open source* comunes en tecnologías de amplio espectro, etc.) o sistemas ciberfísicos (automóvil autónomo, red eléctrica inteligente, dispositivos médicos, etc.). Por no hablar de la debilidad de los dispositivos móviles, de difícil gestión y defensa ante las amenazas mencionadas.

Todo este escenario nos hace replantearnos la necesidad de incorporar a las tradicionales medidas de seguridad otras de Defensa Activa que nos den más oportunidades ante los atacantes".

DSN – DEPARTAMENTO DE SEGURIDAD NACIONAL

Marina Rodríguez Díaz
Jefa de Unidad de Ciberseguridad y lucha contra la desinformación

"Desde el DSN se considera que el año 2023 vendrá marcado en parte por la tendencia en ciberataques ya vivida en 2022, especialmente en la segunda mitad de este último, a lo que habría que añadir condicionantes específicos del año ya en curso.

El riesgo elevado de sufrir ciberataques en 2023 se mantendrá, tanto en el ámbito de la Administración pública como en el sector privado, debido principalmente a la mejora en las técnicas desplegadas por los atacantes, que incluyen una mayor dificultad de detección, y a su alto nivel de persistencia. Es previsible un aumento del *ciberhacktivismo*, principalmente en la modalidad de denegación de servicios, así como ciber espionaje, especialmente a través de Amenazas Persistentes Avanzadas (APTs).

La actual situación geopolítica presidida por la invasión rusa de Ucrania y lo que podría calificarse de "neutralidad pro china", condicionan la citada movilización del *hacktivismo*, y la intervención de grupos cibercriminales - Estado en la ejecución de los ataques.

Desde el punto de vista de la seguridad nacional preocupan especialmente las acciones de ciber espionaje silenciosas, desplegadas por actores – Estado, sin motivación económica aparente o inicial, que pueden llegar a pasar inadvertidas largo tiempo en sectores estratégicos de la Administración Pública y sector privado. Estas operaciones, de desarrollo a medio largo plazo, se centran en recabar información masiva que, de por sí o en relación con otra obtenida de forma complementaria, podría contribuir en un futuro a comprometer de múltiples formas la seguridad/estabilidad del país.

En el ámbito del cibercrimen con motivación económica, durante 2023 se pueden esperar en España, en el corto medio plazo, campañas masivas y/o selectivas de ataques tipo *phishing*, estafas y otros delitos patrimoniales a resultas de la combinación de datos de carácter personal extraídos durante 2022 a través de distintos ciberataques.

Tanto el sector público como el privado son conscientes de los elevados costes económicos y reputacionales que ocasionan los ciberataques, especialmente los de tipo *ransomware*, en alza imparable en los últimos años. Durante 2023 previsiblemente esta modalidad seguirá siendo una grave preocupación, si bien el conjunto de medidas específicas, preventivas y correctivas, desplegadas en ambos sectores durante los años anteriores, deberían comenzar a demostrar su efectividad.

El año 2023 trae consigo ciertos acontecimientos que no hacen sino incrementar el ya de por sí elevado riesgo de ciberataques críticos en nuestro país. Concretamente se deberá prestar especial

atención a posible actividad cibercriminal ligada a los distintos procesos electorales que se desarrollarán a lo largo del año, bien en forma de campañas de desinformación o en forma de ciberataques de denegación de servicio o de otro tipo propagandístico, con la finalidad, en ambos casos, de socavar la confianza de la ciudadanía en la fiabilidad y transparencia de dichos procesos. En esta misma línea de desafío nacional se sitúa la Presidencia española del Consejo UE que dará comienzo en septiembre 2023. Para ambos supuestos y siguiendo el ejemplo del éxito cosechado con ocasión de la organización y cobertura de la Cumbre OTAN, alojada en Madrid en junio 2022, la experiencia demuestra la eficacia de aplicar una adecuada fórmula anticipativa y de coordinación/colaboración de capacidades de todas las instituciones públicas nacionales competentes en ciberseguridad incluyendo la experiencia y capacidades del sector privado español.

Desde el punto de vista estratégico en Ciberseguridad, desde este DSN se recuerda que durante este 2023 se deberán sentar las bases para el desarrollo de un sistema nacional que permita no sólo trasponer de forma ordenada, coherente y en plazo la Directiva NIS2 (Directiva 2022/2555) publicada el pasado 27 de Diciembre 2022, sino también adaptar las capacidades de los distintos actores ciber nacionales, públicos y privados para llevar a cabo el cumplimiento de las nuevas obligaciones que esta recoge, así como hacer frente a la importante ampliación de sectores y entidades que pasarán por primer vez a quedar incluidas bajo el paraguas de esta nueva Directiva, cuya finalidad última es mejorar y sobre todo armonizar la ciberseguridad de los países UE al objeto de conseguir un ciberespacio común más protegido.

En este sentido durante 2022 se detectó un incremento en el número de ciberataques llevados a cabo contra la cadena de suministro en la que sin duda se ubican los eslabones más débiles de la ciberseguridad de las más importantes entidades públicas y privadas de nuestro país.

En 2023 es previsible que la tendencia en ciberataques en este sector continúe al alza. En el ámbito de la Administración Pública este sector se contempla en el Esquema Nacional de Seguridad (ENS). La NIS2 prevé el reforzamiento de la ciberseguridad de la cadena de suministro como prioridad.

Finalmente, desde DSN, en el ámbito estratégico y en consonancia con los departamentos ministeriales competentes en la materia, se significa la importancia del dato, cada vez más entendido desde el punto de vista nacional y europeo como activo estratégico y empresarial. España podría llegar a consolidarse como "hub" internacional y destino de los flujos de información y almacenamiento de datos en la nube de manera segura. La Economía del dato cada vez debería tener un peso mayor en el ecosistema productivo español y europeo. Estas reflexiones apuntan hacia importantes oportunidades como país y ciudadanos españoles, a la vez que presentan desafíos a los que enfrentarse desde los sectores público y privado a través principalmente del impulso de políticas fiables, estables y coordinadas en ciberseguridad".

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

Marcos Gómez
Subdirector INCIBE-CERT. CISO de INCIBE

"El 2022 fue un año complejo, aún por la finalización de la pandemia y su impacto en el ámbito digital, pero también por el comienzo de un nuevo conflicto bélico trasladado al ciberespacio, hecho no singular, pero sí más mediático debido a la madurez de un ecosistema más dependiente de las TIC. Así INCIBE gestionó nuevos incidentes en las empresas españolas y ciudadanía, catalogando ataques e intentos de ataques a sistemas vulnerables o deficientemente protegidos, con más de un 45%; o el fraude electrónico en sus diferentes tipologías, incluyendo el *ransomware*, con más de un 28%; Estas dos tipologías fueron las más utilizadas por los cibercriminales. Una vez más la amenaza de mayor impacto por su alcance en la disponibilidad de los sistemas, redes y servicios o por su perjuicio económico ha sido el *ransomware*, pero la sombra del *hacktivismo* ha permanecido vigente durante buena parte del 2022. Además, el 50% de las empresas y ciudadanos se pusieron en contacto con la Línea de Ayuda de Ciberseguridad, el 017 de INCIBE, en busca de asesoramiento preventivo, tanto frente a nuevas ciberamenazas como sobre el uso de nuevas tecnologías, dispositivos y servicios de la Red.

El 2023 se presenta como un año también complejo, y lleno de incertidumbres: ¿será de nuevo un año marcado por este tipo de ciberataques cuando la tendencia habitual era el fraude informático frente a otras tipologías, como el *malware* o los sistemas vulnerables? ¿Veremos más *hacktivismo* relacionado con el conflicto aún vigente o con situaciones sociales y políticas que marcarán el año como la presidencia de España, de la UE o las futuras elecciones municipales y generales planificadas? ¿Se consolidará la nueva-vieja tendencia de proteger nuestros servicios y sistemas con la filosofía de confianza cero o zero trust? ¿Qué nuevo impacto tendrán las regulaciones recién aprobadas y en pleno proceso de transposición, como la Directiva Europea de Seguridad de los Sistemas de Información (NIS 2), la Directiva de Resiliencia en el Sector Financiero (DORA), la Ley de Ciberresiliencia (Cyber Resilience Act) o la Ley de Ciberseguridad en 5G? ¿Qué beneficios podremos ya notar de la inversión inyectada por el Gobierno en materia de ciberseguridad canalizada hacia la sociedad principalmente a través de INCIBE? Un año, sin duda, muy interesante. Veremos qué ocurre…".

AUTORIDADES PÚBLICAS COMPETENTES Y DEPARTAMENTOS DE LA AGE

MCCE – MANDO CONJUNTO DEL CIBERESPACIO

Francisco Marín
Teniente Coronel
Responsable Área Inteligencia de ciberamenazas

"En 2022 el conflicto en Ucrania configuró el panorama de las ciberamenazas, afectando tanto a las naciones enfrentadas como a las actividades de APTs y a un rejuvenecido *hacktivismo*. Se estima que para 2023 los APTs llevarán a cabo ataques cada vez más disruptivos contra infraestructuras críticas. También se espera que algunos utilicen credenciales adquiridas a grupos especializados (*initial access brokers*) para facilitar su acceso a organizaciones. La actual guerra evidencia que se perfeccionará la integración de los efectos en los ámbitos tradicionales o físicos con los ejecutados en el ciberespacio y el entorno cognitivo (desinformación). Igualmente, un *hacktivismo* renovado continuará siendo utilizado como *proxy* por los estados para alcanzar sus objetivos ocultando su atribución, y también es posible que lleve a cabo acciones destructivas sin otra finalidad que la venganza. Y respecto al conflicto no debemos olvidar la tradicional amenaza de los *insiders*, que ya son señalados como futura herramienta de ataque a los grandes proveedores de servicios que apoyan a Ucrania."

Mº DE ASUNTOS EXTERIORES

Nicolás Pascual de la Parte
Embajador en Misión Especial para Ciberseguridad y Amenazas Híbridas
Dirección General de Política Exterior y de Seguridad

"Durante el presente 2023 se espera, en línea con lo acaecido en el pasado año, que las amenazas y ciberataques más complejos y con un mayor impacto potencial procedan de la Federación de Rusia, la República Popular China e Irán. El desarrollo de la guerra de Ucrania será un factor determinante en el despliegue de la estrategia rusa de campañas de desinformación masiva, amenazas híbridas y ciberincidentes. Si bien es cierto que no se materializó en nuestro país, tal como se temía, un incremento notable de la cantidad y peligrosidad de los ciberataques rusos con ocasión de la guerra de agresión a Ucrania, estamos bien preparados para prevenir, mitigar y reaccionar a posibles ciberincidentes dirigidos contra nuestras infraestructuras críticas y el suministro de servicios esenciales.

Por su lado, es de prever que China continúe ejerciendo sus malos usos y prácticas en el ciberespacio, así como en la aplicación de nuevas tecnologías disruptivas que implican una vulneración de derechos humanos, y están encaminadas a la apropiación ilegal de propiedad intelectual e inteligencia industrial y al espionaje tecnológico".

OCC – OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

Guillermo Fernández López
Jefe de la OCC
Secretaría de Estado de Seguridad
Mº del Interior

"En el actual contexto geopolítico, aprovechado negativamente por estructuras estatales o paraestatales maliciosas o sus *proxies*, por cibercriminales, etc., el nivel de alerta frente a posibles amenazas es importante, tanto para Operadores de Servicios Esenciales como para pymes y ciudadanos.

El *ransomware*, por su impacto, el fraude al CEO y otras estafas, por su rentabilidad ilícita, continuarán, sofisticando sus TTP y recurriendo a la inteligencia artificial.

La ciber higiene, la seguridad de operaciones, la protección de la cadena de suministro y del dato serán esenciales para su prevención, así como dar una adecuada respuesta en los ámbitos penal y diplomático, a nivel nacional e internacional, aumentar la coordinación y promover un cambio en la cultura de gestión de riesgos".

FISCALÍA GENERAL DEL ESTADO Y FSE (INVESTIGACIÓN)

FISCALÍA GENERAL DEL ESTADO

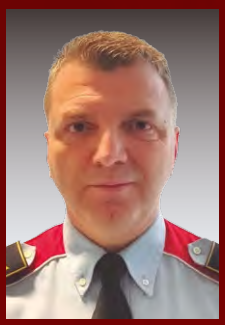
Elvira Tejada de la Fuente
Fiscal de Sala contra la criminalidad informática

"Continúa el incremento progresivo de la actividad ilícita en la red que previsiblemente se mantendrá en 2023. Especialmente llamativa es la intensidad y frecuencia de todo tipo de ataques informáticos con exfiltración de datos de carácter personal para su uso fraudulento, muchas veces con suplantación *on-line* de identidad ajena, cuyas perversas consecuencias cada vez afectan a más ciudadanos. Afrontar esta amenaza requiere impulsar la cooperación interinstitucional y con el sector privado para proteger los intereses de las víctimas y optimizar la investigación criminal, significativamente complicada por el creciente uso de criptomonedas como medio para desarrollar el *iter criminis* o blanquear los beneficios ilícitos obtenidos. Siguen preocupando las ciberagresiones contra intereses personalísimos –libertad, seguridad, intimidad, indemnidad sexual– y el consiguiente aumento de expedientes judiciales como consecuencia de la profunda penetración de las tecnologías en las relaciones interpersonales.
No obstante, los avances en distintos ámbitos como el importante paquete legislativo de la UE; la publicación del 2º Protocolo Adicional a la Convención de Budapest (COE) o las diversas iniciativas nacionales e internaciones para fomentar la colaboración entre operadores diversos auguran mejoras significativas en la respuesta del Estado de Derecho frente a estas amenazas".

GUARDIA CIVIL

Juan Antonio Rodríguez Álvarez de Sotomayor
Teniente Coronel.
Jefe del Dpto. Contra el Cibercrimen
UCO-Unidad Central Operativa
Policía Judicial

"La amenaza más importante en el futuro más cercano es el acercamiento del crimen organizado tradicional al cibercrimen. Por este motivo, aparecerán operativas criminales de mayor gravedad, principalmente en la forma de ciberextorsiones, ya sea con la aparición de estructuras complejas detrás de nuevas formas extorsivas mediante *ransomware*, pero también veremos como regresan las extorsiones por ataques del tipo DDoS a través de plataformas de venta de servicios cibercriminales. Igualmente, esta convergencia del crimen organizado resultará en un aumento del uso delictivo de todo tipo de *malware*, así como la aparición de nuevas redes de BOT dedicadas a ofrecer una amplia gama de nuevos servicios orientados a facilitar la operativa criminal en el ciberespacio."



MOSSOS D'ESQUADRA

Ricard Doña
Subinspector
Jefe de la Unidad Central de Delitos Informáticos
Divisió d'Investigació Criminal
Policia de la Generalitat - Mossos d'Esquadra

"Los ciberataques se han convertido en una de las principales preocupaciones de los estados. Pese a su baja repercusión en cifras globales del cibercrimen, constituyen un gran problema para las instituciones y las empresas, generando una gran alarma social. Para el 2023 se espera la línea al alza de los últimos años. Los ciberataques seguirán amenazando los servicios esenciales (*ransomware* y DDos) y la cadena de suministro. Se esperan ataques más sofisticados, no solo por el conocido objetivo económico sino también como parte de estrategia de lucha geopolítica amparada en la protección que ofrecen algunos estados a los cibercriminales. La cooperación internacional y la ciberresiliencia serán claves para combatir esta amenaza, en tanto que mejorar la capacidad de anticipación y de resistencia al ataque, será determinante para evolucionar a modelos de ciberseguridad más eficientes".

ERTZAINTZA

Íñigo Pascual
Jefe de Sección Central de Delitos en Tecnologías de la Información

"La consolidación del cibercrimen como modelo negocio augura un incremento de los ciberataques. Los ciberdelicuentes experimentados comercializarán, incluso en la modalidad de suscripción y bajo coste, cada vez más herramientas y servicios de fácil uso para la comisión de delitos a través de la red. La inteligencia artificial aplicada a la ciberdelincuencia facilitará la labor a los delincuentes sobre todo en el ámbito de la suplantación de la identidad (*deepfakes*) aportando un plus de credibilidad a sus acciones. La progresiva implantación del 5G, aún con su seguridad integrada en diseño, implicará unos riesgos añadidos que provienen principalmente de sus propias capacidades (velocidad, latencia, ancho de banda, número de dispositivos conectados).

FISCALÍA GENERAL DEL ESTADO Y FSE (INVESTIGACIÓN)

En cuanto a impacto y complejidad mencionaría los ciberataques dirigidos a infraestructuras críticas y cadena de suministros como principal preocupación.
A nivel empresarial, el lucrativo *Ransomware* seguirá adaptándose a las medidas en materia de ciberseguridad implementadas por las empresas y aprovechando cualquier nueva vulnerabilidad. Se confirmará la disminución del número de ataques aunque éstos estarán cada vez más dirigidos a grandes empresas y organizaciones por la posibilidad de doble o triple extorsión que presentan. En cuanto a particulares el *Smishing* seguirá siendo una de las mayores amenazas.
Seguimos apostando por la difusión de noticias, consejos y técnicas como medida preventiva contra la victimización, ya que, a día de hoy, el usuario sigue siendo el eslabón más débil de la cadena de la seguridad informática".

POLICÍA FORAL DE NAVARRA
Miguel Ruiz Marfany
Jefe de la Brigada de Delitos Económicos y Contra el Patrimonio

"Tal y como afirmamos el año anterior, en 2022 se iba a producir un aumento importante de los ataques de *Ransomware*, dirigido especialmente a pequeñas y medianas empresas, la mayoría de las cuales no cuentan con un departamento de Ciberseguridad, las cifras que manejamos demuestran que así ha sido y que, desgraciadamente, este tipo de ataques van a continuar este año. Desde Policía Foral hemos observado también que han crecido los ataques a empresas mediante ingeniería social, hechos con una complicada investigación policial, ya que en la mayoría de los casos, la única línea de investigación es un número de teléfono extranjero y medios de pago difícilmente rastreables (plataformas de envío de dinero, tarjetas Google o Apple, etc.). No sería de extrañar que en este 2023 la Inteligencia Artificial sea utilizada por los ciberdelincuentes para mejorar estos ataques dirigidos, pudiendo falsear conversaciones, imágenes, vídeos, documentos, etc...
Me gustaría, nuevamente, recalcar la necesaria implicación de todos los agentes que trabajamos en este 'mundillo', no hay más remedio que poner el mayor número de trabas posibles a los ciberdelincuentes, tanto a la hora de abrir cuentas bancarias fraudulentas, contratar líneas telefónicas o beneficiarse del dinero obtenido, por lo que es fundamental la colaboración de entidades bancarias, prestadoras de servicios de telecomunicaciones, Exchanges de Criptomonedas, etc".

POLICÍA NACIONAL
María Piedad Álvarez de Arriba
Comisaria Principal
Jefa de la Unidad Central de Ciberdelincuencia
Comisaría General de Policía Judicial

"Las principales ciberamenazas a las que nos enfrentaremos en 2023 serán, como es natural, una evolución de las heredadas el año anterior, caracterizado por el aumento imparable de los delitos contra el patrimonio, especialmente fraudes informáticos, cada más sofisticados que trataran de vencer lo aprendido por las víctimas. *Phishing* previo, fraude al CEO, a la Banca *Online* y aquellas relativas a inversiones en criptovalores, serán los modus operandi más empleados por las organizaciones criminales que poco a poco tienden a la especialización delictiva (*Crime as a Service*).
Malware avanzado, *Ransom* y accesos llegítimos con exfiltración de datos para su posterior venta o para cometer extorsiones, serán los ataques más importantes que sufrirá el ámbito empresarial e institucional.
Igual tendencia experimentarán los ciberdelitos que tienen como objetivo mismo los propios internautas, especialmente las extorsiones con contenido sexual o la distribución de pornografía infantil, a través de las Redes Sociales mediante utilización de nuevas técnicas de anonimización como *Deepfake* o IA para alterar y falsificar imágenes, ya detectado en esta UCC durante el año pasado".

ENTIDADES AUTONÓMICAS Y LOCALES

AGENCIA DE CIBERSEGURETAT DE CATALUNYA

Pedro Lendínez
Director de SOC

"Derivado del contexto económico y de la bajada del BitCoin, se producirán más ataques de menor complejidad y monetización rápida (*smishing*, vishing, *DeepFake*, BEC), siendo las empresas de la cadena de suministro y los sectores estratégicos objetivos principales. Los principales APT's seguirán evolucionado sus ataques, y se incrementarán los ataques de explotación de vulnerabilidades, dotando de mayor peso a los servicios de *Threat Intel*".

AGENCIA DIGITAL DE ANDALUCÍA

Eloy Rafael Sanz
Jefe del Servicio de Ciberseguridad

"¿Complejos y de gran impacto? Suena a infraestructuras críticas, y con el recrudecimiento de la situación en Ucrania, ese podría ser el escenario. Las explotaciones de vulnerabilidades de día cero, de credenciales de acceso remoto y de vulnerabilidades en la cadena de suministro seguirán siendo fuente de nubosidad y chubascos. Sin embargo, y no siendo necesariamente complejos, los ciberincidentes con motivación económica seguramente sean este año los de más impacto. Todo esto se parece mucho a la predicción del año pasado, en una especie de día de la marmota cibersegura".

GENERALITAT VALENCIANA

Lourdes Herrero
Jefa de servicio de Confianza Digital (DGTIC)
Conselleria de Hacienda y Modelo Económico

"Entrando de lleno en año electoral, aumentarán las campañas de desinformación, continuarán los ataques de denegación de servicio, y las desfiguraciones de no excesiva complejidad contra las administraciones públicas, al tiempo que seguirá creciendo el *ransomware* de triple extorsión hacia ellas, objetivos blandos y de bajo perfil, donde la ya pasada pandemia dejó en herencia configuraciones de seguridad más laxas de lo deseable. El uso malicioso de la inteligencia artificial, que ya ha dado sus primeros frutos al incorporarse a la elaboración del *ransomware*, seguirá creciendo en sofisticación y alcance. Estará presente en los ataques más complejos, facilitando, además, que actores de bajo perfil amplifiquen sus daños gracias a su uso".

BASQUE CYBERSECURITY CENTRE (BCSC)

Asier Martínez
Responsable del CERT

«Se acrecentarán los fraudes BEC como consecuencia de la baja complejidad técnica y el rápido y gran beneficio que suponen. Continuarán los ataques a proveedores de ciberseguridad con el objetivo de comprometer masivamente a sus clientes por la cadena de suministro. Y la nueva regulación europea será determinante para incrementar la resiliencia en ciberseguridad de multitud de empresas.»

XUNTA DE GALICIA – AMTEGA

Gustavo Herva
Jefe Subárea de Seguridad de la Agencia para la Modernización Tecnológica de Galicia

"Creo que pueden tener mucho impacto, como ya hemos visto en el pasado, los ataques a la cadena de suministro, en particular en lo relativo a las dependencias del software de terceros, será algo que habrá que vigilar bien. Por otra parte, también habrá que estar pendiente de lo que depare el desarrollo de la inteligencia artificial y lo usos imaginativos que hagan de ella los atacantes".

INFORMÁTICA DEL AYTO. MADRID (IAM)

José Ángel Álvarez
Director del Centro de Ciberseguridad

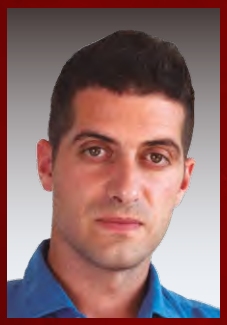
"Los grupos organizados de cibercriminales intensificarán su actividad, optando por un tipo de ataque lo más sencillo posible, con el que obtener beneficios rápidos, evitando escenarios mediáticos que puedan ponerles en el punto de mira de países con capacidad de pasar 'al ataque' y desmantelar sus operaciones. En una gran ciudad, atacantes más sofisticados podrían llevar a cabo acciones cuyo objetivo sea la interrupción de los servicios públicos (educación, sanidad y similares) y la afectación de sus infraestructuras críticas (suministros o transporte, entre otros), tal y como ya vimos en USA con Colonial Pipeline. El Ayuntamiento de Madrid, con la creación del Centro de Ciberseguridad (CCMAD) apuesta por el refuerzo de las capacidades de protección, monitorización y respuesta".

ASOCIACIONES Y ANALISTAS

AENOR

Boris Delgado
Director de Soluciones de Digitalización y Tecnología

"Podríamos decir que estamos en el circo de la era digital; somos espectadores y artistas, donde cada año asistimos al: 'más difícil todavía'. En 2023 los ciberataques serán más 'difíciles'; el *ransomware* y el *smishing* se reinventa con Inteligencia Artificial, más convincentes y personalizados a sus víctimas. Los IoT/IIoT + 5G = ambiente propicio para suplantar identidades, vulnerar la cadena de suministro y las infraestructuras críticas. Pero como en todos los circos, los trapecistas trabajan con seguridad. Estos son los estándares de ciberseguridad y resiliencia abiertos actualizados en 2021-2022: ISO 27001, ISO 27002 e ISO 22301; el también actualizado, RD 311/2022 – ENS, que podrán ser la base para el cumplimiento de los actuales NIS2 o DORA".



ANTI-PHISHING WORKING GROUP

Pablo López-Aguilar
Director of Technology

"En un mundo cada vez más conectado y en un contexto donde el teletrabajo parece que ha venido para quedarse, los ataques de *phishing* seguirán predominando como uno de los vectores preferidos por los ciberdelincuentes. Para mitigar su impacto, las campañas de concienciación deberán mejorar su eficacia adecuándose al perfil de cada individuo (no todos somos susceptibles a ser víctimas de los mismos ataques) y no tratar de educar desde una perspectiva tan genérica.
Por otra parte, el uso cada vez más extendido de dispositivos IoT requiere de la implementación de estándares que mejoren su interoperabilidad y garanticen, en todas las fases de su desarrollo, la seguridad de la información. Dichos retos deberán abordarse a todos los niveles (incluyendo instituciones nacionales y también supra nacionales) y considerarse desde una perspectiva técnica, legal, ética y social".

CCI – CENTRO DE CIBERSEGURIDAD INDUSTRIAL

José Valiente
Director

"Serán los ciberataques con origen en la cadena de suministro, especialmente en el ámbito industrial, debido al aumento de la conexión de proveedores externos y la gestión de la operación en terceros debido a la digitalización. Las organizaciones industriales serán objetivo de agentes maliciosos dado el alto número de ellas que no están invirtiendo en medidas de ciberseguridad adecuadas".

CENTRO DE ANÁLISIS E INTERCAMBIO DE INFORMACIÓN DE SERVICIOS FINANCIEROS (FS-ISAC)

Teresa Walsh
Global Head of Intelligence

"La Ley de Resiliencia Operativa Digital (DORA) en Europa entrará en vigor en noviembre y será clave para terceros críticos. En España, TIBER-ES aportará información sobre la resiliencia de los bancos frente a los ciberataques con pruebas de penetración obligatorias.
Es probable que continúen la tendencia alrededor de operadores de *ransomware* que roban datos de empresas sin cifrado. Algunos países europeos pueden exigir la notificación de los pagos de *ransomware*, y es posible que muchas aseguradoras cibernéticas ya no cubran este tipo de ataques.
Las nuevas tecnologías, como ChatGPT, reducirán la barrera de entrada para los estafadores que buscan avanzar en falsificaciones profundas para eludir la autenticación del cliente. Esto conducirá a una mayor presión sobre las empresas financieras para garantizar la autenticidad del cliente".

CLOUD SECURITY ALLIANCE (CSA) ESPAÑA

Mariano J. Benito
Vicepresidente

"2023 verá el aumento de incidentes por filtración de datos desde la Nube por error del usuario. Ya sea por deficiencias de diseño de la arquitectura de servicio como por configuración insegura de los servicios, como por errores en la operación diaria. No pocas organizaciones adoptan la Nube con precipitación y sin análisis de riesgos que detecten y prevengan de estos errores. Todo ello resalta la necesidad de formar recursos propios o contar con terceros especializados. Los recursos que CSA-ES publica también les ayudarán en estas tareas. De cualquier forma, CSA analiza anualmente la evolución del mercado Cloud y siempre es de interés seguir el documento 'Top Threats to Cloud Computing".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

CYBERSECURITY INNOVATION HUB

Tomás Castro
Presidente de la AEI de Ciberseguridad y Tecnologías Avanzadas

"En 2023, se celebrarán elecciones en más de 70 países, por lo que se prevén ciberataques orientados al espionaje y el sabotaje, por ejemplo, mediante campañas de desinformación. Además, cobrará relevancia el *malware* avanzado, una tipología de malware con gran capacidad de adaptación, idóneo para burlar posibles protecciones. También encontraremos IA y *Deep Fakes*, como método para ejecutar suplantaciones de identidad, etc. Además, el ransomware continuará siendo un tipo de ataque habitual, con rescates más caros y modelos de doble o triple extorsión. Lo mismo ocurrirá con el *phishing* y el *smishing*, que emplearán ingeniería social más avanzada. Evitar las autenticaciones multifactor será uno de los principales objetivos de los ciberdelincuentes en las aplicaciones en la nube".

FORRESTER

Tope Olufon
Senior Analyst

"Los ataques MFA serán más comunes y sofisticados. Las empresas deben tratar a MFA como otra herramienta para ayudar a la seguridad y no como una 'bala de plata' para evitar la complacencia.

El *ransomware* se volverá más personalizado. A medida que evoluciona el ecosistema de *ransomware*, se espera que los actores de amenazas creen *ransomware* dirigido a empresas específicas en lugar de usar productos 'COTS'.

Ataques OT más exitosos a medida que más organizaciones aprovechan la nube y las API de terceros en sus operaciones.

Más correos-e de *phishing* vendrán desde dentro, ya que los atacantes se centrarán más en usar direcciones de correo electrónico legítimas en lugar de falsificarlas.

Se espera que el *malware* generado por IA se generalice. Chat GPT ya se ha utilizado para revisiones de código y para generar código posterior a la explotación, algo que se volverá más sofisticado".

ISACA

Vanesa Gil
Presidenta de ISACA Madrid Chapter

"Las empresas deberán enfrentarse a grupos de crimen organizado con técnicas de ataque más sofisticadas y motivaciones muy diversas, desde robo de información a desestabilización de la economía digital. Junto con ataques de *ransomware*, *malware* e ingeniería social, destacarán los dirigidos a entornos Cloud, proveedores de servicios y cadena de suministro. Un enfoque proactivo de gestión de seguridad será imprescindible para garantizar la resiliencia operacional".

KUPPINGERCOLE

Marina Iantorno
Analista

"No podemos predecir el futuro, pero queda una certeza: la cantidad de ciberataques seguirá aumentando en 2023. Los costes de los ciberataques también aumentarán debido a varios factores: inflación mundial, crisis energética, conflictos geopolíticos y expansión de las superficies de ataque de las organizaciones. Por otro lado, las crisis a veces pueden verse como oportunidades, lo que lleva a los proveedores de seguridad a innovar para proporcionar mejores productos y servicios. Además, las organizaciones demandarán soluciones nuevas y más potentes para enfrentar los ataques cibernéticos y reducir los riesgos".

OWASP ESPAÑA

Vicente Aguilera
Presidente del Capítulo

"El robo de datos personales, especialmente los datos médicos, y los ataques a la cadena de suministro tendrán gran impacto. El uso de la IA en la generación de *fake news*, así como en ataques de ingeniería social (*deepfake*, *deep voice*...) se verán incrementados. Asimismo, el metaverso será otro foco importante donde veremos aplicaciones maliciosas que comprometerán nuestra seguridad".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

ASOCIACIONES Y ANALISTAS

SANS INSTITUTE
Jess García
Senior Instructor

"2023 será expansivo en los ataques de extorsión (con o sin *ransomware)*, con nuevos actores, más agresivos y eficaces que se apoyarán en las debilidades de autenticación y la reticencia a 2FA, y con modelos de negocio más eficaces. El año se cebará contra la ciudad sin ley de la Nube, con ataques más silenciosos y sofisticados, y un abuso de las APIs expuestas a Internet".

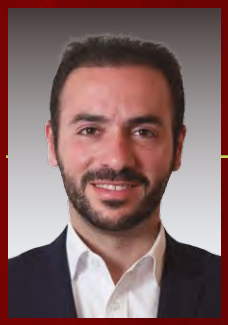
THIBER
Adolfo Hernández
Cofundador

"Es previsible que, a lo largo de 2023, continuemos con una tendencia de ataques al sector cripto, como ha sucedido a lo largo del año pasado con ataques a *exchanges* y *tokens* de forma periódica y con alto impacto.
La potencial recesión a la que las entidades harán frente podría impactar en los presupuestos destinados a ciberseguridad impactando en algunas capacidades, como la formación.
Como ya vaticinamos en 2022, se materializará la tendencia alcista en el coste de las primas de ciber riesgos, y es muy probable que el ecosistema asegurador comience a considerar determinados riesgos ciber como "no asegurables", obligando a los clientes a replantearse la estrategia de gestión del ciber riesgo desde el punto de vista de la transferencia".

ASEGURADORAS

MAPFRE
Andrés Peral
Director de Seguridad en Sistemas de Información

"Ser Nostradamus y predecir cómo serán los ciberataques de 2023, y acertar es, posiblemente, una quimera. No obstante, sí hay algunas certezas. La primera, que el cibercrimen seguirá siendo lucrativo y de poco riesgo, pues siguen faltando medios para perseguirlo. Por eso, seguirá creciendo. La segunda, que las empresas continuarán aumentando su eficiencia. Y con ello su digitalización e integración con terceros, la mayoría pymes que son mucho más fáciles de atacar. Por ello, aumentarán los ataques a través de proveedores y esta vía de entrada será más difícil de resolver.
Si a eso le sumamos una guerra, la cercanía del descifrado cuántico, y la concentración de riesgo en los proveedores de nube, tendremos la tormenta perfecta. ¡Menos mal que tenemos los mejores profesionales de ciberseguridad!".



TOKIO MARINE HCC
José Carlos Jiménez
Cyber Senior Underwriter Southern EMEA & LatAm

"Pronosticamos nuevos ataques de ingeniería social mucho más complejos con nuevos *phishing*, *smishing* más sofisticados, y dirigidos a dispositivos y vías de comunicación más variados. En consecuencia, veremos aumentar el robo de credenciales e información, que se unirán a la aparición de *ransomware* más complejos y agresivos, además de ataques a sistemas industriales e IoT, entre otros".

WTW
Carmen Segovia
Directora de Seguros de Ciber riesgos

"Los ataques de *ransomware* seguirán siendo una de las principales pesadillas, sobre todo porque se sofistican las técnicas por parte de los cibercriminales para eludir los MFA gracias a los *deep fakes* y otras técnicas de *phishing*. También, se seguirá explotando la doble extorsión. Sin embargo, las nuevas sanciones internacionales introducidas este año como consecuencia del conflicto ruso–ucraniano, puede poner a las organizaciones afectadas en una situación delicada, ya que corren el riesgo de enfrentarse a posibles acciones judiciales si pagan rescate a grupos que figuran en las listas de sanciones. Por otro lado, las cadenas de suministro siguen en el punto de mira, con foco en los proveedores de software. Los Seguros de Ciber riesgos empiezan a incluir restricciones de cobertura a los ataques a la cadena de suministro, como anteriormente introdujeron limitaciones al *ransomware*".

CENTROS Y LABORATORIOS DE INVESTIGACIÓN Y EVALUACIÓN

APPLUS+ LABORATORIES

David Hernández García

Director de Dominio Técnico de Circuitos Integrados. Dpt. Cybersecurity & Interop

"El despliegue de la infraestructura 5G prevista para los próximos años será, sin duda, uno de los principales objetivos para los atacantes en 2023. Los ataques de *spoofing* serán, a nuestro entender, los de mayor impacto. Las compañías que reutilicen tecnología (antigua) con el fin de ofrecer nuevos servicios a través de 5G jugarán un papel esencial en la ciberseguridad de estas redes".

DCNC SCIENCES – TECHNOLOGICAL INSTITUTE FOR DATA COMPLEX NETWORKS & CYBERSECURITY SCIENCES

Santiago Moral

Director

"Parece que este año toca hablar de la ciber-guerra y la inteligencia artificial para la generación de ataques. Pero al igual que decía el año pasado a esta misma pregunta, el incidente más grave que esperamos en el sector es el mismo que llevamos acarreando desde el inicio de nuestro oficio: No pasa nada. Nadie asume ninguna responsabilidad. Parece que la UE quiere imponer sanciones a las empresas si no demuestras un interés suficiente por este asunto de la ciber y que después tengan un incidente. Pero no va a pasar nada. Estamos en un modelo de Teoría de Juegos en el que los atacantes están midiendo continuamente nuestra tolerancia máxima al que nos provocan como individuos, como empresas y al conjunto de la sociedad. Los atacantes están muy preocupados y 'ocupados' en no sacarnos de nuestro letargo. Hace poco pudimos ver un poco atónitos, como una plataforma SaaS de *ransomware* se disculpaba porque uno de sus "asociados" había atacado a un hospital infantil. Los dueños de la plataforma SaaS de *ransomware* castigaron al atacante, sentándolo en una esquina de la clase en la silla de pensar para que reflexionara sobre su falta de ética. Le prohibieron el uso de la plataforma de *ransomware*. A veces se nos olvida que los atacantes son inteligentes y que, como cualquier otra industria, están intentando maximizar las inversiones que realizan. Si realmente son listos no veremos ningún ataque que pueda hacernos reaccionar como sociedad de manera más decidida. Aunque como no son perfectos alguno puede medir mal sus fuerzas y generar un incidente que tenga para ellos un efecto boomerang. La nueva facilidad de acceso a la AI para generar ataques puede hacer que algún atacante novato la lie pada y le joda el negocio a los veteranos bien asentados. Esteremos atentos".

EURECAT

Juan Caubet

Director of IT&OT Security Unit

"Para este 2023 se espera que crezcan los casos de *ransomware* personalizados y de triple extorsión, donde ese triple factor estará ligado a empresas y personas relacionadas con las víctimas (clientes, proveedores, pacientes, ciudadanos…). De esta forma los ataques podrán tener un victima principal y múltiples víctimas colaterales si no se paga el rescate, lo cual multiplica su impacto. Por otro lado, al igual que se vio en el último trimestre de 2022, se prevé que sigan creciendo los ataques a empresas del ecosistema cripto, principalmente al sector DeFi, con un gran impacto económico. En estos casos los atacantes buscan sustraer grandes cantidades de capital mediante hackeos. En 2022 se sustrajeron cerca de 3.900 millones de USD, veremos en 2023."

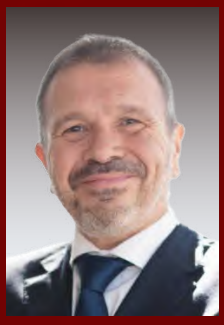
FUNDACIÓN i2CAT

Jordi Guijarro Olivares

CyberSecurity Innovation Director

"El éxito de la Inteligencia Artificial (IA) con soluciones de pronósticos financieros, recomendaciones, reconocimiento imagen/voz, generación de lenguaje,etc, ha llevado a su adopción masiva siendo cada vez más ubicua. En ciberseguridad, una tecnología que puede ser más eficiente para atacar que proteger dónde la disponibilidad de grandes fuentes de información ya permite a los atacantes aprovechar sus herramientas no solo para aumentar la precisión y la eficacia de los ataques, sino también para automatizar sus fases de diseño y personalización. En el horizonte, una evolución de ataques BEC con nuevos enfoques *Business Videoconference Compromise* (BVCC) con *cybertrols* avanzados, más ataques de envenenamiento contra sistemas de protección basados en IA reduciendo su efectividad…¡A por el 2023!

CENTROS Y LABORATORIOS DE INVESTIGACIÓN Y EVALUACIÓN



FUNDITEC

Miguel Rego
Director General

"La inteligencia artificial está creando enormes oportunidades para todos los sectores productivos. La automatización inteligente de la información permite la transformación operacional, comprender y predecir el comportamiento de los clientes y, aplicado al campo de la gestión de los riesgos cibernéticos, una mejor caracterización de la amenaza y capacidad predictiva de los ataques.

El mercado global de IA se expande rápidamente. Entre 2023 y 2030, la adopción de IA por parte de las empresas crecerá a una tasa anual del 38,1%, generando oportunidades de negocio de hasta 180 mil millones de dólares al año.

El despliegue de soluciones basadas en IA y su integración con procesos críticos de negocio, la convierte en un objetivo claro de los cibercriminales. Los ataques adversariales hacen que los modelos aprendan incorrectamente y generen decisiones incorrectas. Las técnicas de envenenamiento introducen datos manipulados a voluntad. El robo de modelos de IA o la extracción de la información que alimenta el sistema, son otras de las posibles consecuencias. ¿Cabe pensar que se están abordando los proyectos de desarrollo, implantación y operación de entornos IA teniendo en cuenta los ciber riesgos? ¡Qué *deja vu*…! Por favor, ¡qué venga pronto la regulación!

GRADIANT

Juan González Martínez
Director del Área de Seguridad y Privacidad

"El pasado año advertimos sobre el peligro de una gran vulnerabilidad en el campo de la criptografía. Aunque finalmente no llegó a suceder, el equipo de OpenSSL anunció en octubre una vulnerabilidad crítica en su código, que posteriormente se clasificó como alta debido a su dificultad de explotación. Esto nos hizo a todos temer lo peor. Sin embargo, es crucial estar preparados para gestionar rápidamente cambios en las librerías criptográficas que utilizamos, debido a la complejidad e impacto de una vulnerabilidad de este tipo. Muchas organizaciones no están preparadas para ello y no cuentan con un inventario de los sistemas criptográficos empleados, ni utilizan el paradigma de agilidad criptográfica (*crypto-agility*) que les permitiría responder de manera ágil y ser resilientes ante incidentes de estas características, que podrían producirse, quizás, en 2023".

GRUPO DE INVESTIGACIÓN REDES Y SISTEMAS

Javier Areitio
Director
Facultad de Ingeniería
UNIVERSIDAD DE DEUSTO

"El panorama para este año muestra un incremento de superficies de ciber-ataque, un aumento inquietante de vulnerabilidades/multivectores, el uso de acciones perversas y comportamientos insidiosos potenciados y automatizados por IA, cada vez más complejos y de mayor impacto, con técnicas de ocultación muy elaboradas. Los ciberataques a la "Tecnología IoT: IIoT-IoCT-IoMT-IoAIT" (como DDoS, PitM/*Person-in-the-Middle*, fuerza-bruta, etc.) relacionados con la digitalización caótica/frenética, serán cada vez más comunes ya que los ciber-atacantes han encontrado numerosas fisuras (APPs/APIs explotables, cuentas comprometidas, correos infectados, etc.) que les permite actuar despiadadamente sobre sus superficies de ciber-ataque. Las "Cadenas de Suministro" que incluso abarcan infraestructuras críticas OT/IT serán cada vez más objetivos de ciberataques y lo más perverso es que en la mayoría de los casos no se detectarán lo que permitirá diseminar *malware* durmiente en los elementos de las cadenas de suministro esperando actuar, ubicadas incluso en el sector público. El "CaaS(*Cybercrime-as-a-Service*)"/*MaaS(Malware-as-a-Service*) incrementará el volumen y efectividad de los ciber-ataques. Se empoderarán, crecerán y sofisticarán las "Campañas de *Phishing* potenciados con IA" utilizando modelos de lenguaje como GPT-4. El uso de la "Tecnología Web3" (aplicaciones financieras, criptomonedas, etc.) aún inmadura desde la perspectiva de la ciberseguridad aumentará los ciberataques con éxito en muchas áreas. Los "*Spam-bots*" empoderados con IA se usarán para amplificar las campañas MDM (*Misinformation-Disinformation-Malinformation*) con fines perversos (dañar reputación, modificar comportamientos, afectar a la continuidad del negocio, crear deficiencias cognitivas, caos, etc.). Incremento de los ciberataques "API-bots", dañando el núcleo de la economía digital. Crecimiento de la "Explotación de vulnerabilidades sobre el software legítimo" utilizando, por ejemplo, BYOVD (*Bring Your Own Vulnerable Driver*), Secuestro-DLL, etc.) que facilita el saltarse las medidas de protección de los dispositivos finales. Incremento notable de ciber-ataques y ciber-amenazas en el área de los "Gemelos Digitales" (MITM, fuga de información, manipulaciones, DDoS, vulnerabilidades, etc.) en todos sus espacios: físico-digital-comunicaciones, por ejemplo, en los ecosistemas de producción industrial (plantas, productos, procesos). Aumento de "Ciber-ataques en los Metaversos" (modificación de código, secuestros de perfiles de usuarios, etc.):

CENTROS Y LABORATORIOS DE INVESTIGACIÓN Y EVALUACIÓN

industrial, compras, juegos, socialización, medicina, finanzas, etc. Tener la identidad digital y una cantidad cada vez mayor de datos personales almacenada en el móvil incrementarán los ciber-ataques al tener un único punto de actuación/fallo. Crecimiento notable de ciberataques a la identidad (de personas y máquinas) y a los sistemas de autenticación sin contraseña. Incremento importante de ciberataques DDoS usando redes basadas en nubes con fisuras".

IKERLAN
Salvador Trujillo
Responsable de Área
Ciberseguridad Industrial

"El rol de la ciberseguridad en la industria se está convirtiendo en un factor de competitividad clave. Las nuevas normativas europeas que se están definiendo para los fabricantes de equipamiento implicarán un cambio de paradigma donde la seguridad por diseño no va a ser una elección sino una obligación, incrementando la importancia del cumplimiento normativo y la evaluación independiente. Más que nunca las actualizaciones en los sistemas industriales van a ser necesarias y el enfoque integral y evolutivo se convierte en algo central. La rapidez en los tiempos de identificación, detección y respuesta automatizada es crucial, pues impacta en los procesos de los fabricantes de dispositivos industriales conectados.
Los temas de regulación mencionados avanzan en esta senda para hacer de obligado cumplimiento prácticas que anteriormente eran opcionales. Las empresas industriales son cada vez más conscientes de la importancia que tiene la ciberseguridad en sus organizaciones, están apostando más por fortalecer sus líneas de trabajo en este ámbito, y se comienza a considerar un factor de competitividad crucial por los clientes. Gracias a esta creciente concienciación, las empresas están cada vez mejor protegidas y las amenazas recibidas tendrán una menor probabilidad de éxito a la hora de perjudicar su actividad. Desde Ikerlan, continuaremos reforzando nuestras capacidades tecnológicas para seguir colaborando tanto con empresas de productos y servicios de ciberseguridad como con fabricantes industriales de diversos sectores en desarrollar tecnologías de Ciberseguridad industrial".

JTSEC
Javier Tallón
Director Técnico

"Tendremos más de una colaboración generada por ChatGPT, lo que muestra que la IA es ya una herramienta muy poderosa para simular comportamientos humanos, haciendo indistinguible lo real de lo falso con tecnologías como el *deepfake*; los ciberataques se moverán del ciberespacio a los *mass-media* para afectar a la opinión pública y la estabilidad social".

NETWORK INFORMATION AND COMPUTER SECURITY LABORATORY (NICS Lab)
Javier López Muñoz
Director
UNIVERSIDAD DE MÁLAGA

"El año 2023 se va a presentar con grandes retos de investigación, especialmente contra amenazas avanzadas y persistentes que ponen en riesgo la sociedad 5.0 y sus tecnologías emergentes como la inteligencia artificial y los gemelos digitales. En este contexto, el abuso de la información tomará un papel central. Dicho abuso se cristalizará en aspectos como el uso indiscriminado de información obtenida de redes sociales y dispositivos móviles por parte de naciones y grandes empresas, el ciberespionaje industrial con técnicas basadas en IA, la manipulación de las cadenas de suministro del software/hardware haciendo uso de ataques "día cero" para indirectamente tomar el control de infraestructuras críticas, y la explotación de herramientas de generación de contenido textual y visual como GPT-4 y Stable Diffusion para realizar acciones de ingeniería social a nivel individual y social."

SGS BRIGHTSIGHT
Lucio González Jiménez
CyberLab Manager

"Los ataques de *ransomware* (más de 10TBs de datos robados cada mes) junto a DDOS condimentan al principal vector de ataque: la ingeniería social (*phishing* y *smishing*). Sigue aumentando la diversidad de usuarios (privados y profesionales) y su distribución, lo cual los hace más vulnerables especialmente a la ingeniería social. La velocidad de adopción de los principios de *zero trust* es lenta, nos conectamos en cualquier sitio posible haya donde se encuentre una red inalámbrica o móvil para acceder a una infraestructura cloud moderna. El contexto de la guerra en Ucrania traerá nuevas modalidades de ataque, añadiendo la facilidad con la que las redes sociales pueden ser utilizadas sigue

CENTROS Y LABORATORIOS DE INVESTIGACIÓN Y EVALUACIÓN

creciendo. En España, entramos en periodo electoral y habrá que ver o escuchar de todo, mucho de ello falso".

TECNALIA

Ana Ayerbe
Directora Área CORES

"Continuarán los ataques a través de la cadena de suministro software, utilizando tanto el software de proveedores habituales como librerías de código abierto, a la vez que explotando al máximo las vulnerabilidades existentes en los múltiples niveles de los complejos ecosistemas software que pueden encontrarse en las empresas industriales (Edge, IoT, Cloud híbridas, Espacios de Datos, Sistemas de Inteligencia Artificial, …)".

LABORATORIO DE CRIPTOGRAFÍA – LIIS

Jorge Dávila
Director
Facultad de Informática
UNIVERSIDAD POLITÉCNICA DE MADRID

"Esto de vaticinar lo que nos espera en el futuro más cercano es algo realmente difícil y casi siempre erróneo. Este año ya no se nos pide acertar, lo cual relaja mucho la tarea. Si nos piden pensar en los ataques complejos y de gran impacto, en realidad, nos están pidiendo dos cosas. Los ataques complejos probablemente no se den, sean verdaderos cisnes negros, ya que el atacante no suele ser tonto y si encuentra algún frente de ataque más sencillo, seguro que lo probara antes y la probabilidad de éxito sea mayor. Aquí no distinguiría entre agentes nacionales/estatales o de grandes corporaciones, y los del cibercrimen estándar ya que todos ellos juegan en las mismas condiciones de contorno. Si se nos pregunta por los de mayor impacto yo pensaría en ¿qué puede haber después del *ransomware*? Pues bien, entendiendo el *ransomware* como una denegación de servicio de acceso (disponibilidad), lo siguiente es pensar en ataques a la Integridad semántica de los sistemas. Me refiero con ello a todas aquellas modificaciones difíciles de detectar antes de que causen estragos, y que alguien puede intencionadamente plantar en bases de datos, registros, catastros, historiales clínicos, registros civiles, registros transaccionales bancarios, etc. Este tipo de ataques socavarían la confianza colectiva en el sistema y con ello la utilidad de todo el tinglado digital en el que cada día se apoya más nuestra sociedad occidental y avanzada. ¿Cuánto pagaríamos para volver a un estado en el que podamos seguir confiando? ¿Cuánto cuesta volver a nuestra zona de confianza? Lógicamente no podemos saber si alguien puede convertir la siembra de la desconfianza en un negocio boyante como es el *ransomware*, pero si se ha logrado atentando contra la disponibilidad y contra la confidencialidad, que es un clásico, todavía nos quedan la Integridad, la Autenticación y las capacidades de No-Repudio. Se habla mucho del 'Zero Trust', la desconfianza mutua perfecta, pero realmente no se ha pensado con calma lo que eso realmente significa y si eso es posible en una sociedad civil en tiempos de paz y bonanza".

VICOMTECH

Raúl Orduña
Director de Seguridad Digital

"El impacto tiene que ver con la criticidad de los activos afectados, no necesariamente con la complejidad del ataque. Se espera que en 2023 las amenazas más relevantes afecten a la suplantación de identidad para acceder a recursos restringidos de la red, a la explotación de vulnerabilidades de los modelos de *Machine Learning* y a los ataques a sistemas embebidos en entornos críticos.".

ZIUR INDUSTRIAL CYBER SECURITY CENTER

Koldo Pezina
Managing Director

"El proceso de transformación digital en el que está envuelto el sector industrial está provocando que muchas de las organizaciones estén adoptando nuevas tecnologías junto con sus sistemas tradicionales, aumentando conectividad. Este proceso de va a continuar durante 2023. Tendrá especial peso los dispositivos conectados, ya que durante este año entrarán en vigor varias iniciativas para de aumentar la seguridad en los sistemas conectados y los entornos cloud, debido a las amenazas provenientes del cloud. También será determinante la ciberseguridad en el teletrabajo, ya que la mayoría de las organizaciones industriales no estaban preparadas para hacer frente a la conexión de dispositivos no seguros en su red y se encuentran aún en el proceso de identificar y mitigar los riesgos asociados al teletrabajo. También la IA va a ser el motor de ciberataques más inteligentes, convincentes y mejor desarrollados. Y todo ello precisará de realizar campañas de formación y concienciación en materia de ciberseguridad".

INDUSTRIA Y SERVICIOS

ACCENTURE
Myriam Sánchez
CyberDefense Lead de Accenture Security en España

"Continuarán aumentando los que afectan directamente a las operaciones y a la continuidad de negocio de las empresas, buscando como retorno el pago de rescates por devolver el control de la infraestructura, de los datos o por restaurar la operativa normal en las empresas afectadas. Este tipo de ataques afectará por igual a sector público y privado. En relación con el fraude, la tendencia será un aumento de los ataques por *smishing* respecto al *phishing* tradicional, reflejando los intentos de las organizaciones cibercriminales de evitar las políticas de doble factor de autenticación y aumentar el impacto/éxito de sus ataques. La cadena de suministro de las organizaciones seguirá siendo un objetivo claro de los atacantes, que se aprovechan del tamaño y complejidad de éste "ecosistema extendido" de las grandes organizaciones y lo utilizan como vectores indirectos de ataque. Además, continuarán los ataques a las infraestructuras en cloud, donde la gran mayoría de las compañías han ido migrando parte de su infraestructura y servicios esenciales sin que el nivel de madurez en ciberseguridad se haya desarrollado al mismo ritmo. En este sentido, tener conocimiento continuo de cuál es la superficie expuesta de la organización en la nube será un aspecto fundamental a la hora de gestionar el riesgo de exposición. Por último, la situación geopolítica mundial y los diferentes incidentes que ya se llevan sufriendo en los últimos años continuarán impactando en el día a día de este recién comenzado 2023".

ACRONIS
Candid Wüest
VP of Cyber Protection Research

"Hay cinco tendencias principales que probablemente darán forma al panorama de la ciberseguridad en 2023: 1) La autenticación y la gestión de identidades y accesos (IAM) serán atacadas con éxito con una mayor frecuencia; 2) Las filtraciones de datos seguirán causando grandes daños; 3) La automatización de la nube a través de las API podría desencadenar ataques a gran escala; 4) La amenaza del ransomware seguirá siendo importante y evolucionará; 5) Los atacantes intentarán usar las debilidades de la Inteligencia Artificial y el Machine Learning (AI/ML), incluido ChatGPT".

ADVANTIO
Manuel Fernández
Director of Strategic Partnerships

"Estamos asistiendo a la confluencia de revoluciones tecnológicas históricas que tendrán un impacto directo en la evolución de las ciberamenazas y su perímetro de actuación. La puesta en marcha efectiva de las redes de comunicación 5G con el incremento exponencial de dispositivos IoT sofisticados; la explosión de IA que, puesta en manos de una audiencia creciente, ofrecerá desarrollos difíciles de imaginar; la programación 'No Code', cuyo único ingrediente necesario es la creatividad. Todas estas tecnologías incrementan de forma impresionante la cantidad de players en el lado de la ciberdelincuencia y amplían el perímetro a defender. Más a nivel estratégico, seguimos viendo una amenaza importante en la concentración de servicios críticos en *cloud* ante ataques físicos a infraestructuras"

ADVENS
Jose Luis Díaz
Managing Director – Spain & Portugal

"Los ciberataques más complejos y de mayor impacto para 2023 serán: 1) Ciberataques OT/IoT a gran escala con repercusión sobre las personas e infraestructuras críticas; 2) *Deepfakes* avanzadas y utilizadas como ingeniería social; 3) Aumento del uso de IA y chatbots por parte de ciberdelincuentes. Por otro lado, los *ransomware* serán los más habituales y podrían darse de manera masiva durante 2023".

AIUKEN
Juan Miguel Velasco
CEO

"Para nosotros es claro: *Ransomware* (varias formas) y ataques al Cloud público. Como en años anteriores tristemente hemos de colocar el Ransomware en sus 2 variantes más habituales en el top de nuevo en 2023, la razón es por la falta de varios factores, mal parcheo y pésimo actualización, mala protección del endpoint, falta de concienciación y formación y, por último, mala política de *backup* y protección de datos críticos. Esto sigue haciendo vulnerables a las entidades.
Segundo los ataques al Cloud público. Las empresas están adoptando el cloud público de forma masiva sin tomar medidas adecuadas de protección, acceso y cifrado de datos, en una mala conciencia de que los proveedores de Cloud les protegerán por defecto. Esta suposición les llevará sin duda a ser víctimas de todo tipo de robo de datos, pérdida de infraestructuras y daños en el negocio.

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

AJOOMAL

Abraham Vázquez
Service & Support Manager

"Para este 2023 veremos una proliferación en amenazas como el *deepfake*, debido a la creciente popularidad de las IA pudiendo usarse como ingeniería social, o ataques dirigidos a *dispositivos IoT* en base a su continuo crecimiento y falta de controles de seguridad. Por último, tendrán un gran impacto las *filtraciones de datos* puesto que se esperan elecciones políticas en más de 34 países".

AKAMAI TECHNOLOGIES

Francisco Arnau
Vicepresidente Regional para España y Portugal

"Los avances de la IA provocarán un frenesí de suplantación de identidad. De cara al futuro, podemos esperar que los continuos avances en la Inteligencia Artificial (IA), como los que se observan en sistemas como el GPT-3, harán que el *phishing* selectivo sea más convincente, más escalable y común. Estos sistemas serán capaces de escribir millones de mensajes de correo electrónico o SMS, cada uno de ellos personalizado para un destinatario individual, y cada uno con cualidades convincentes similares a las humanas. Esto supondrá un reto importante para las tecnologías *antiphishing* existentes, y hará mucho más difícil que la gente detecte las comunicaciones sospechosas. Se trata de ingeniería social automatizada y ejecutada a escala, y provocará un aumento precipitado de los intentos de *phishing*".

ALL4SEC

Alfonso Franco
CEO & Managing Director

"La Inteligencia Artificial está dando lugar a nuevos modelos de ciberataques. Modernas aplicaciones de interacción con los usuarios están favoreciendo la aparición, por ejemplo, de formas alternativas de *phishing* actuando bajo patrones en apariencia poco sospechosos. De alguna manera, la identidad digital empieza a verse amenazada. Afrontar los retos que suponen la orquestación y automatización de estas amenazas será de enorme importancia particularmente en aquellos entornos de servicios críticos o esenciales".

ÁLVAREZ & MARSAL

Julio San José
Managing Director

"Quizás esta pregunta deberíamos planteársela a esa IA tan famosa en los últimos meses, pero casi mejor que no, no vaya a ser que demos ideas... En lo que respecta a los ciberataques en los últimos años hemos podido asistir a una escalada hacia todo tipo de sectores. Si nos remontamos unos años atrás vemos que han ido ganando no tanto en complejidad como en impacto. Por ejemplo, en 2018 se atacó el sistema de pagos mexicano, en l 2019 se amplió hacia la tercerización con algunas grandes consultoras afectadas a nivel global y finalmente llegamos a lo que creemos que representan ensayos de ataque a nivel global, cuyo claro exponente es Solarwinds.
El contexto geopolítico con la guerra de Ucrania en el centro de todas las tensiones nos lleva a pensar que la tendencia es hacia un impacto global. Aunque ha habido algunos teóricos que han hablado de un 'cyber Pearl Harbour' nosotros nos decantamos hacia un ataque coordinado a infraestructuras básicas (energía-telecomunicaciones-financiero, por ejemplo) y encaminado al bloqueo total del adversario. A nivel de amenazas veremos un mayor crecimiento en las amenazas más tradicionales y la llegada masiva de especialización con ayuda en algún caso de las IA y siempre evitando los nuevos mecanismos de seguridad, especialmente mediante *deepfakes*".

AON

Pablo Montoliú
Chief Information & Innovation Officer

"Hemos contemplado con asombro los recientes avances que han aportado herramientas de Inteligencia Artificial como ChatGPT o DALL-E 2. El reto será poder mitigar el impacto que la adopción de la IA pueda tener sobre la ciberseguridad cuando sea aplicada maliciosamente y seguir explorando casos de uso en los que dichas tecnologías nos puedan ayudar a luchar contra el ciber crimen".

ARMIS

Axel Pérez García
Solution Architect – Iberia Region

"Los ataques en entornos IoT, IoMT y OT serán cada vez más frecuentes y de mayor alcance al aprovechar las vulnerabilidades de dispositivos que, sin contemplar la seguridad desde su diseño, están expuestos a los riesgos de Internet. Los atacantes se valdrán de la IA para automatizar y sofisticar sus ataques, emulando patrones de comportamiento que dificultarán la detección y eludirán las defensas de la red".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

ARROW ECS IBERIA

Ignacio López Monje
Regional Director South EMEA

"En 2023 sufriremos ataques ya conocidos, como el *ransomware*, aunque de manera más dirigida y como servicio (RaaS). También se incrementarán los ataques sobre 5G y de ingeniería para obtener credenciales y evadir el cada vez más implantado MFA. Además, se focalizará más en ataques a servicios web y APIs, así como progresará el incremento de ataques a sistemas ICS/SCADA. Por último, surgirán nuevas amenazas sobre el metaverso y Web3."

ARSYS

Luis Marqueta
Ingeniero Senior de Seguridad

"En 2023 continuarán los ya conocidos ataques de ransomware, pero evolucionarán hacia esquemas de doble y triple extorsión. El complicado contexto económico ayudará al crecimiento del ransomware (y el cibercrimen en general) como servicio. Asimismo, se incrementarán los ataques puramente destructivos, incluyendo infraestructuras críticas; probablemente, con especial énfasis en Europa dada la situación geopolítica actual. Las fórmulas de trabajo remoto o híbrido han llegado para quedarse y esto acelerará la implementación apresurada de estrategias *zero trust*, lo que podría llevar a debilidades que serán explotadas por los cibercriminales. Afortunadamente, los equipos directivos estarán más concienciados y podrán poner más recursos dedicados a ciberseguridad".

ARUBA

Alberto Pérez Cuesta
Southern Europe SDWAN Business Development Manager

"La aplicación de motores AI al *hacking*, tras la explosión de la misma en otros entornos, hará que la captura de insights de una víctima potencial sea masiva, conllevando una explotación de vulnerabilidades más efectiva, sobre todo, en el caso del puesto de trabajo híbrido, aún no correctamente protegido, y donde aplicamos múltiples mecanismos *Zero Trust*, en diferentes niveles (Red, Aplicación, Datos), pero sin orquestación entre sí".

ASTREA La Infopista Jurídica

Dr. Ignacio Alamillo Domingo
Director

"En 2023 veremos un notable incremento en los ataques a los sistemas descentralizados que sustentan la gestión de criptoactivos, especialmente debido a las malas prácticas de gestión de claves asociadas a las carteras de criptoactivos, tanto las autogestionadas por los usuarios, como las gestionadas por proveedores de servicios de criptoactivos, dadas las notables carencias que en este sentido plantea MiCA".

ATALANTA

Isaac Gutiérrez
CEO

"Al igual que el año pasado, en 2023 la inestable situación mundial afecta al ciberespacio. Así, la adopción de la nube seguirá siendo una tendencia creciente y con ello, su seguridad seguirá siendo importante para garantizar la privacidad de los datos. Otro aspecto a destacar será la automatización de las soluciones de ciberseguridad para reaccionar de manera más eficiente y reducir costes. Asimismo, por la forma de desarrollar aplicaciones, cada vez de forma más compleja y con la adopción de DevOps, seguirá creciendo la explotación de vulnerabilidades en todo tipo de aplicaciones, por lo que es importante mejorar la seguridad en su desarrollo, aplicando un enfoque DevSecOps efectivo y sobre todo quien lleve a cabo la Infraestructura como Código. Por último, continuarán incrementándose los ataques dirigidos a dispositivos IoT, especialmente vulnerables dada la multitud de servicios que pueden acceder y unos métodos de autenticación y autorización poco sólidos, de ahí que la gestión de identidades y accesos y las capacidades de Zero Trust seguirá siendo importantes".

ATOS

Arancha Jiménez Martínez
Responsable de Ciberseguridad en Servicios y Productos Atos Iberia

"Esperamos que los ataques de *ransomware* se combinen con otros patrones de ataque buscando un impacto mayor. También esperamos ver aumentar ataques al metaverso (robos de NFTs, identidades de avatares, contraseñas de *wallets*…). Los ataques a la cadena de suministro tomarán aún más relevancia. Aun se necesita aprender mucho en aspectos de control y respuesta, independientemente, de en qué punto del proceso estemos y quién los realice. Los entornos OT e IoT se están expandiendo y son todavía demasiado vulnerables y críticos como para que los atacantes no pongan foco en ello.
Sin duda, la aceleración en la adopción de la nube y las zonas de responsabilidad compartida recibirán más ciberataques. Se necesitará un rediseño y adopción de estrategias de defensa más sólidas. Finalmente, las amenazas tradicionales seguirán siendo un componente central de casi todos los ataques, eso sí, con una mayor sofisticación a través de automatización e IA (*deepfake*)".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

A3SEC
Nacho García Egea
Director Técnico

"Los ataques *malware* sofisticados, *phishing* de nueva generación con IA, campañas masivas de *masquerAds*, y aumento de ataques de *ransomware* a pymes serán el foco de este 2023, donde la clave para la protección viene por la monitorización de nueva generación con inteligencia de amenazas,...".

ÁUDEA
Jesús Sánchez
CEO

"Los ciberataques con foco en el usuario seguirán evolucionando por su compleja solución, que depende de la concienciación de los usuarios. Destacamos una evolución del *phishing* hacía el *spear-phishing* con mensajes elaborados y dirigidos a grupos de población concretos; infecciones *malware* a través de dispositivos externos más sofisticados como ratones, teclados o auriculares; aumento de ataques del tipo Fraude al CEO utilizando técnicas DeepFake".

AUTEK INGENIERÍA
Miguel Ángel Martín
Product Manager

"Los ataques a infraestructuras críticas son los que representan un mayor riesgo por el gran impacto que pueden tener. Aunque se ha producido un cambio de enfoque y se intenta poner el foco en la resiliencia, muchas infraestructuras se han desarrollado sólo con criterios económicos y de facilidad de despliegue y explotación.
Desde el año pasado estamos percibiendo que el sector privado ha incrementado sustancialmente su interés en segmentar sus redes y por lo tanto su necesidad de intercambio seguro de información entre sus dominios de seguridad (cross-domain). Fundamentalmente, empresas estratégicas, cuyos activos de información tienen que preservar su confidencialidad e integridad y garantizar su disponibilidad, como en el caso de las infraestructuras críticas".

AUTHUSB
Jorge Vega Lamas
Socio y CTO

"En 2023 seguirán incrementándose los ataques dirigidos a infraestructuras críticas, así como a las empresas consideradas como esenciales y a las redes productivas. Asistiremos a un incremento de ciberataques a las redes OT, que se verán afectadas por ataques del tipo Zero Day, premeditados y específicamente diseñados, utilizando vías de entrada cada vez más insospechadas, pero de gran recurrencia de uso en este tipo de redes. Ataques que pasen desapercibidos y no puedan ser detectados hasta que el/los delincuentes decidan que es el momento. El impacto puede ser enorme. Hay que prepararse".

AVAST
Luis Corrons
Evangelista de ciberseguridad

"Los ciberdelincuentes se sofisticarán este 2023. En el sector empresarial, el *ransomware* se agravará y las empresas afectadas se enfrentarán también a sanciones mundiales si pagan peticiones de rescate a grupos que figuran en la lista de sanciones. En el terreno consumidor, continuarán las estafas a través de correos electrónicos de *phishing* y la suplantación de cuentas en redes sociales".

BABEL
Mario Casado
Global Head of a Cybersecurity

"Además de los ataques que todos conocemos, el auge de la inteligencia artificial para mejorar los procesos de negocio de todo tipo nos va a llevar a un aumento en ataques de tipo *Data Poisoning*, donde los atacantes inyectan datos corruptos en un sistema de IA, haciendo que el sistema tome decisiones intencionalmente equivocadas. Esto puede ser especialmente importante en entornos OT".

BALBIX
Miguel Cebrián
Solution Sales Engineer – EMEA Lead

"Es difícil predecir los ataques más complejos para este año, ataques respaldados por IA, 'deep fakes', ataques a sistemas biométricos, todos entran dentro de lo posible en 2023. Dada la inestabilidad política, hay una probabilidad alta de ataques provenientes de naciones rivales. Bien como aviso sobre las consecuencias a sufrir si se toma partido o como represalia. La cuestión real desde nuestro punto de vista es cómo minimizar el impacto si un ataque así nos llegara afectar. Aquí Balbix tiene claro los deberes. Comprensión de todo el entorno, inventario. Visibilidad de la postura de seguridad y priorización de los riesgos. Por último, ejecución eficiente del programa de seguridad respaldado con métricas y telemetría que nos ayuden a comunicar eficazmente en la organización.

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

BARRACUDA

Miguel López Calleja
Senior Regional Sales Manager – Iberia

"Dada la situación internacional veremos muy probablemente ataques en el ámbito de la ciberquerra, guerra hibrida y falsa bandera que buscarán desestabilizar al bloque enemigo. La ejecución puede llevarse a cabo de múltiples maneras, algunas más novedosas o menos frecuentes que los habituales *ransomwares* y *wipers*. Podríamos ver algún gran ataque con esta finalidad ejecutado mediante: ataques DDoS, ataques a la cadena de suministro de software, suplantación de identidad y robo de información. Estos ataques utilizarían el vector del correo electrónico y/o los servicios web, contarían con un alto componente de Ingeniería social o incluso Inteligencia artificial para desarrollarlos y estarían dirigidos a infraestructuras críticas, proveedores de servicios esenciales o entornos militares".

BEDISRUPTIVE

Roberto Lara
Spain SOC Director

"El conflicto en Ucrania será una fuente de amenazas cibernéticas en 2023. Se espera que se desarrollen ataques más sofisticados, especialmente en dispositivos industriales (IIoT). Estos pueden interrumpir servicios básicos de infraestructuras críticas y causar inestabilidad en gobiernos y empresas. Los ataques más populares seguirán siendo el *ransomware*, el espionaje y el *phishing*".

BIDAIDEA

Mikel Rufián
Global Managing Director

"La Ciberguerra informativa con IA va a ser el motor de ciberoperaciones más inteligentes, convincentes y mejor desarrollados. Los deepfakes como arma son las principales tendencias de ciberataques que se verán en 2023. Así, los ciberatacantes utilizarán formas sofisticadas para evadir las medidas de detección tradicionales actuales de las organizaciones y se aprovechan de los procesos comunes para introducirse en los sistemas IT-OT-IoT. Especialmente con foco para sistemas ICS/SCADA, cadena de suministro y operaciones disruptivas contra sistemas ciberfisicos. Los ciberdelincuentes también aprovecharán la buena voluntad o la reputación de las organizaciones establecidas en el metaverso para atacar su identidad. Por lo tanto, las transacciones en el metaverso pueden no ser seguras, ya que es difícil determinar la identidad de un usuario. Eso sin dejar de lado los incidentes relacionados con la protección de la cloud. Es necesario una solución en la nube independiente, para unificar la seguridad de todas ellas".

BITDEFENDER

Martin Zugec
Senior Director of Product Management, WW Enterprise Marketing

"Los grupos de RaaS continuarán innovando con lenguajes de programación más exóticos (Go, Rust) que son más difíciles de analizar o admiten una multitud de sistemas operativos. Los actores de amenazas continuarán buscando métodos para eludir las soluciones de detección de puntos finales (EDR) más débiles. El número de ataques híbridos seguirá aumentando. Los ataques comienzan con el uso de escaneo automático para identificar sistemas vulnerables, detectado un sistema vulnerable, se entrega a un actor de amenazas humano para determinar si vale la pena seguir adelante, por ejemplo, si es parte de la cadena de suministro para un objetivo más lucrativo. Este estilo de ataque híbrido aumenta el riesgo para organizaciones de cualquier tamaño. Esto tendrá un impacto dramático en el seguro cibernético: para fines de 2023, el proceso de suscripción será más selectivo y adoptará un enfoque más realista al evaluar los riesgos".

BLACKBERRY

Ismael Valenzuela
Vicepresidente, Investigación de Amenazas e Inteligencia

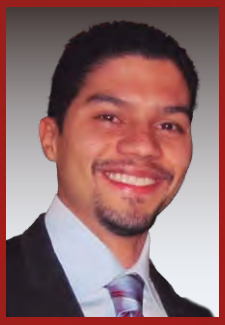
"En 2023 seremos testigos de un uso más dirigido de la IA para la automatización de ataques y para desarrollar ataques avanzados de *deepfake*. El robo de credenciales continuará en auge, y los atacantes incrementarán su interés por las plataformas que cada vez obtienen más datos personales de los usuarios, incluyendo datos biométricos en el caso de plataformas de realidad virtual, con el fin de usarlos en ataques de suplantación de identidad e ingeniería social. Los ataques a instituciones financieras, infraestructura crítica, y agencias de gobierno continuarán contando con alianzas entre actores de amenazas patrocinados por estados y grupos cibercriminales que utilizarán armas cibernéticas más sofisticadas, incluyendo herramientas programadas en lenguajes multiplataforma, para maximizar el impacto y rentabilizar la inversión".

BLUELIV (AN OUTPOST24 COMPANY)

Victor Acin
Labs Manager

"Debido a la posible recesión (o como mínimo estancamiento económico) de 2023, se verá un incremento de los incidentes causados por *insiders*, personas que intentarán utilizar su posición para dar acceso a atacantes a la infraestructura del negocio en el que trabajan. Por otra parte, también veremos la especialización de ataques de *ransomware* enfocados en ICS".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023



BLUEVOYANT INTERNACIONAL

Mario Medina
Director Técnico

"Para 2023, esperamos que más organizaciones den prioridad a la ciberseguridad de la cadena de suministro. Nuestros estudios globales recientes han identificado que el 98% de las empresas habían sufrido un impacto negativo por una debilidad en su cadena de suministro. En lo que respecta al *ransomware*, vimos en 2022 cómo algunos grandes grupos de *ransomware* colapsaron y ahora vemos cómo surgen y se forman nuevos grupos. En 2023, es probable que los ataques se simplifiquen y se dirijan a empresas más pequeñas, objetivos más blandos, con menos probabilidades de atraer la atención de los medios. Esto también proporciona un terreno de pruebas fértil e indulgente para los jóvenes ciberdelincuentes que aprenden a entrar en lo que se ha convertido en el gran negocio del *ransomware*".

BOTECH

Miguel Ángel Rojo
CEO

"Finaliza un año lleno de novedades para la normativa PCI DSS que tendrá en este 2023 su año de transición a su versión 4.0. Un cambio que por fin ve la luz tras casi 8 años desde que se lanzó la 3.0. Esta actualización, cargada de novedades con más de 50 nuevos requisitos de seguridad, nos mantendrá muy ocupados a los expertos en PCI y será, sin duda alguna, uno de los grandes retos de este nuevo año".

BROADCOM

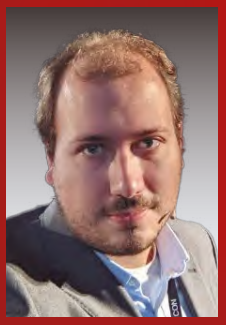
Nur Pulad
Head of Cybersecurity Iberia

"Continuarán los ataques multi-capa, utilizando herramientas legítimas para fines maliciosos. La seguridad requerirá IA para adaptarse rápidamente al entorno de cada organización. La tecnología de detección de comportamiento basada en IA debería ser un componente clave para cualquier organización madura en 2023"

BT

Enrique Martín Gómez
Cybersecurity Sales Specialist en BT Global Services

"Las empresas globales serán objetivo de los ciberataques más complejos en 2023. Los atacantes aprovecharán: fallos de configuración en sistemas multicloud complejos de administrar; cadenas de suministro con mayor exposición al riesgo y sin visibilidad de sus medidas de seguridad; y vulnerabilidades OT del sector manufacturero, que priorizan la disponibilidad frente a la seguridad".



BYRON LABS

Carlos Cilleruelo
CEO

"Se acrecentarán los ataques con gran capacidad de monetización e impacto. El *ransomware* seguirá teniendo un papel central. Aparecerán y crecerán grupos que usen técnicas de doble extorsión. Otra de las amenazas será la relacionada con los ataques a las cadenas de suministros. 2023 ya nos ha traído uno de estos ataques, al haberse visto infectada PyTorch, una librería con más de 200.000 descargas diarias.

CAPGEMINI

Andrés de Benito
Director y responsable de Ciberseguridad en España

"Iría de la mano de la tan famosa IA ChatGPT. El desarrollo de este tipo de IA ha puesto al alcance de todos, herramientas hasta ahora solo a disposición de pocos actores. Este avance permitirá la proliferación en ataques más complejos, que provocarán inquietud en el sector y obligarán a las empresas a reinventarse, dando un salto de madurez en el tipo de tecnologías y defensas desplegadas."

CASTROALONSO

Miguel García-Menéndez
CEO

""La erosión de valor continuará imparable. La Web3 seguirá siendo una de las fuentes de dicha erosión. A ella se sumará la IA generativa. Los efectos negativos de todo ello afectarán a derechos fundamentales; el papel de la ética resultará transcendental. También lo será el de los órganos de administración como responsables del uso que se dé a 'lo digital' en sus organizaciones".

CEFIROS

Ángel Carreras
Director

"Los ataques que más impacto tendrán seguirán siendo los que más lucro generan a los ciberdelincuentes, es decir, aquellos relacionados con el *ransomware* y las nuevas técnicas de ataque que irán

apareciendo, y a ello ayudará en gran medida la evolución de la inteligencia artificial y sobre todo la velocidad de crucero que está tomando la supercomputación cuántica, que permitiría descifrar los algoritmos y cifrados más complejos que conocemos a día de hoy en cuestión de minutos y que nos debería hacer replantear más pronto que tarde como deberían trabajar y protegerse la mayoría de las actuales comunicaciones y dispositivos que usamos en el día a día… Y sin ningún lugar a dudas, con el correo electrónico como principal vector de ataque. ¿Los ataques más complejos? Pues que uno de estos ataques ocurra en alguna de las infraestructuras básicas o servicios básicos como las comunicaciones, energía, sanidad… lo que pondría en jaque a nuestra sociedad de una manera muy seria…".

CGI

Telmo Miguel Ferreira
Red Team Leader para la Unidad de Negocio de España, Italia y Latinoamérica

"Los ciberataques crecerán en frecuencia, complejidad y alcance, centrándose en áreas como el *cloud*, para acceder y exfiltrar datos de estos servicios. Además, los ciberdelincuentes pondrán su foco en las ciberinfraestructuras críticas, buscarán aprovechar las debilidades de seguridad de los dispositivos conectados a IoT, y utilizarán técnicas de IA para automatizar y escalar los ataques".

CHECK POINT

Eusebio Nieva
Director SE para Iberia

"Veremos un crecimiento de los ataques de *ransomware* dirigidos y una evolución del ecosistema de los actores maliciosos con grupos más pequeños y ágiles formados con el propósito de evadir las fuerzas policiales. Habrá un incremento en los ataques dirigidos a las herramientas de colaboración como Slack, Teams, OneDrive y Google Drive sobre todo con intentos de *phishing*. Se vio en 2022 y la previsión es que esta tendencia se consolide: un incremento de *hacktivismo* asociado o esponsorizado por estados, pasando de grupos sociales con parámetros de funcionamiento "fluidos" a otros grupos más organizados, estructurados y sofisticados apoyados por algunos estados. Además, veremos cada vez más vectores de ataque en crecimiento como el uso de *deepfakes* en diferentes contextos (crear opinión, desinformación o como apoyo en ataques tipo timo del CEO) y, por supuesto, relacionados con terceros (*supply chain*), especialmente la perversión de bibliotecas de software de uso común. Todo esto va a generar, por una parte, el encarecimiento y aumento de requisitos de las pólizas de seguro frente a ciberincidentes y que surjan nuevas normas gubernamentales para luchar contra estas amenazas.

CIPHER (A PROSEGUR COMPANY)

Jorge Hurtado
Senior Vice President EMEA

"2023 será el año en que la inteligencia artificial se hará todavía más evidente como el futuro de la tecnología y la ciberseguridad. Si bien desde Cipher llevamos años utilizando estas técnicas en nuestros servicios gestionados, nunca antes se habían visto tan claramente las posibilidades que la IA puede ofrecer. Sin duda este tipo de tecnologías revolucionarán la forma en que gestionamos la ciberseguridad, y debemos todos acelerar el ritmo de adopción para aprovecharlas (y defendernos de ellas)"

CIPHERBIT – GRUPO OESÍA

Alfredo Díez
Director

"IoT: la mayoría de los dispositivos están conectados a Internet, incluso insertados en el cuerpo. Esto irá en aumento, con beneficios, pero también amenazas de ser atacados.
Ordenadores cuánticos: con presencia creciente en sectores clave: banca, sanidad, AAPP. Se hace indispensable garantizar la 'securización' robusta de estos sistemas, por lo que desarrollamos proyectos para esta necesidad".

CISCO

Ángel Ortiz
Director de Ciberseguridad en España

"Con la rápida maduración de los 'kits de herramientas', los atacantes se centran cada vez más en estos kits que incluyen malware modular, con tácticas más dirigidas a los trabajadores y menos a los sistemas. La vulnerabilidad Log4j, el uso de 'commodity loaders' como Qakbot, Emotet, IcedID y Trickbot, la proliferación del *ransomware* como servicio y la explotación de herramientas legítimas como Powershell y de técnicas antiguas como malware USB son los principales ataques detectados por Cisco Talos en 2022, que seguirán afectando a las organizaciones este año. Es así como en 2023 superaremos la era del simple malware; no bastará con detectar el código malicioso. La próxima evolución de la seguridad consiste en detectar anomalías y patrones de comportamiento mediante avances en IA y aprendizaje automático".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

CODEE

Daniel López Sanz
Global Head of Sales and Marketing

"Los ataques seguirán creciendo exponencialmente y uno de los eslabones débiles de la cadena es el SDLC. A pesar de los "movimientos hacia la izquierda" y el número de herramientas existentes, la falta de automatización de las tareas y los objetivos temporales, dominados por negocio, demanda y competencia, obligan a publicar software inmaduro e ineficiente que facilita la labor a los atacantes".

COMMVAULT

Eulalia Flo
Directora General de Iberia

"Nos enfrentamos a un nuevo escenario geopolítico en el que sufriremos un giro en el origen de las ciberamenazas. Además de los kits, que permiten a cualquier ciberdelincuente lanzar un ataque, el uso de la inteligencia artificial y el aprendizaje automático los harán más peligrosos. Las estrategias de ciberengaño tomarán más relevancia y ayudarán a neutralizar ataques mucho antes".

CLOUD SOFTWARE GROUP

Nuno Silveiro
Principal Sales Specialist, Netscaler

"La seguridad del acceso de personas, dispositivos y APIs seguirá bajo una intensa amenaza por el cibercrimen. Estos seguirán explorando distintos vectores de ataque, sea través de los más tradicionales de *phishing* y *ransomware* o las nuevas tendencias de *vishing*, donde se hacen pasar por un centro de contacto para ganar acceso al dispositivo o a las claves de acceso. Seguiremos viendo ataques más evolucionados, combinando distintas técnicas y direccionadas a personas y/u organizaciones, sea por su decisión o por encargo de terceros, en un muy real 'cibercrimen-sob-demanda'. A su vez los consumidores están más conocedores y demandan de sus proveedores acciones para proteger sus datos. Los fallos de seguridad van a generar multas más elevadas y una tangible perdida de reputación".

COMFORTE

Ricardo Escrivà
Client Executive para Iberia

"En nuestra opinión entre las amenazas que se materializarán durante este año están: el uso malicioso de la inteligencia artificial y la identidad digital; y el robo de datos sensibles a gran escala. El uso malicioso de la Inteligencia Artificial conducirá a la industrialización de ciberataques personalizados. La IA ampliará el rango y alcance de los ciberataques mejorando la eficiencia y efectividad de estos. En el caso de la identidad digital, los dobles digitales serán más fidedignos; ya que se recolectará un mayor volumen de información personal y sensible en las redes para los ataques. Los ataques descritos deberán recopilar grandes cantidades de datos sensibles, así que como posibles objetivos estarán las empresas que recopilan grandes volúmenes de información".

CONSIST

Paloma García Piserra
Country Manager de Consist Internacional España y Portugal

"Sin ser conscientes, la IA ha llenado todos los rincones de lo cotidiano (Instagram, YouTube, solicitud de préstamos al banco, etc.). Por eso, creo que tendrá gran impacto el uso de la Inteligencia Artificial como método de intrusión, ya sea para suplantación de identidades, falsificación de documentos… Debemos tener en cuenta que la IA visual gana terreno a la IA puramente numérica, con lo que esto conlleva. Las redes domésticas, que aún tienen pocas técnicas de contención junto con los esquemas híbridos de trabajo, abrirán más brechas de seguridad. Habrá muchos empleados cambiando de lugar de trabajo, abriendo puertas a vulnerabilidades relacionadas con dispositivos de accesos o credenciales comprometidas. El *ransonware* seguirá latente innovando en las tácticas de extorsión y con ataques cada vez más sofisticados".

CONSTELLA

José Luis Fernández
VP of Professional Services

"La difusión de PII en Deep y Dark Web explotará, siendo este el principal vector de iniciación de otros ataques, por lo que se necesitarán mecanismos automatizados basados en IA para identificar de forma temprana y proactiva que un atacante ha robado información (credenciales, direcciones, ID Cards, SIMs, etc.) tanto de nuestros usuarios internos como de nuestros clientes".

CORERO

Álvaro Villalba
Ingeniero Senior de Sistemas

"El espectro de amenazas está variando poco en los últimos años con lo que lo lógico es que siga en la misma línea durante 2023 pero incrementando su sofisticación. Hay dos factores principales que motivan los ataques, los de tipo económicos y los de motivo ideológico / político, con lo que lo más probable es que los

ataques de mayor impacto sean de tipo ransomware bloqueando completamente empresas e instituciones y de DDoS desconectando redes e incluso países enteros".

COUNTERCRAFT

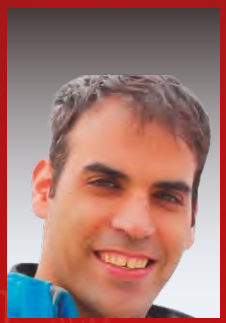
David Barroso
CEO y Fundador

"La aparición de OpenAI y sus aplicaciones como ChatGPT o DALL·E 2 en 2022 nos obliga a intuir que también serán utilizadas en muchos de los incidentes de 2023, y les dará un toque de innovación no visto en los últimos años. No olvidemos que la mayoría de los incidentes más importantes tienen un componente de ingeniería social, y el poder crear textos, imágenes o videos creíbles de forma tan sencilla facilitarán de gran manera el trabajo de los atacantes. También veremos cómo la mayoría de los incidentes pertenece a uno de estos tres tipos: fallos de configuración en servicios en la nube, ingeniería social a empleados, o intrusiones relacionadas con la cadena de suministro. La cadena de suministro seguirá siendo uno de los vectores de ataque más interesantes, y será bastante común ver cómo algunas organizaciones son comprometidas debido al compromiso previo de alguno de sus proveedores o productos (incluidos productos de seguridad). Finalmente, será interesante analizar la evolución de los seguros y pólizas de ciberseguridad, puesto que debido al aumento de incidentes de seguridad cada vez existirán mayores requerimientos a cumplir por parte de las organizaciones, tanto a nivel de políticas como de tecnologías a desplegar (interna y externamente) para minimizar los riesgos de seguridad.

CROWDSTRIKE

Juan Luis Garijo
Director Regional para España y Portugal

"Como novedad en *ransomware*, el mayor riesgo seguirá siendo la doble extorsión desde grupos muy organizados. También crecerá la actividad de los *access brokers* que comercializan credenciales de acceso a sistemas empresariales para su posterior uso por criminales. Y, finalmente, observaremos ataques sofisticados dirigidos desde gobiernos y que atacarán entornos *cloud* sin utilizar *malware*".



CYBERARK

Lavi Lazarovitz
Director del equipo de investigación cibernética de CyberArk Labs

"Los analistas de CyberArk Labs pronostican que la ciberseguridad en 2023 estará marcada por el aumento del robo y la venta de créditos de carbono, la mercantilización de las credenciales a medida que continúan aumentando los ataques a la seguridad de la identidad, las cookies de sesión como objetivo prioritario y el impulso global de Web3 en blockchain, que promete una mayor privacidad".

CYBERPROOF

Manel Álvarez
Country Manager Spain & Sub-Americas

"Los ataques siguen siendo fácilmente evitables y se aprovechan de una ciber higiene deficiente. Los adversarios suelen aprovecharse de una Ciber higiene básica deficiente para obtener el acceso inicial. De hecho, las bandas criminales organizadas atacan a todo el mundo con un enfoque de 'rociar y rociar'. Frente a ello, las empresas luchan por integrar la inteligencia sobre amenazas en sus programas de seguridad. Eso sí, la adopción de la nube pública está impulsando la implantación de nuevas tecnologías de seguridad que satisfacen mejor los requisitos de protección que muchos controles de seguridad tradicionales no cumplen cuando se trata de proteger la computación en nube".

CYBERRES by opentext

Ramsés Gallego
International Chief Technology Officer

"2023 va a ser un año marcado por actores mayúsculos relacionados con la ciberguerra. Ataques orientados a dañar infraestructuras críticas de países en conflicto... o aliados. Experimentaremos ataques 'flexibles' que sabrán optar por una estrategia u otra de penetración en una infraestructura en función de sus diferentes debilidades. Ataques, en consecuencia, 'inteligentes' o programados para variar su aproximación dependiendo de la robustez del sistema en jaque (ya sea por un código débil, una brecha en su configuración o, simplemente, por una vulnerabilidad). En un plano más 'terrenal' veremos muchos ataques orientados a engañar en relación al (Ultra) verso y todas sus dimensiones. Seremos testigos de timos y fraudes en las aplicaciones móviles que dan supuesta entrada a ese multiverso. Todo ello acelerado por un profundo desconocimiento de los usuarios y ayudados por arquitecturas apoyadas en inteligencia artificial y aprendizaje de las máquinas (Machine Learning). Y si dudamos, le podemos preguntar a ChatGPT :)".

CYMULATE

Daniela Kominsky
Country Manager Spain, Portugal and Italy

"Los ciberataques que hay que temer en 2023 son los ataques más comunes que son capaces de evolucionar hacia ataques complejos de varias fases. Veremos que estos implican métodos de ataque probados pero orquestados para ocultar la intención

del atacante. Esto seguirá dando lugar a fugas masivas de datos, costosos pagos por ransomware e interrupciones de negocio sin precedentes. La responsabilidad no puede ser asumida por un único control individual, y las empresas deben validar continuamente sus controles de seguridad para evitar el uso indebido de credenciales, la escalada de privilegios y el movimiento lateral. Los equipos de seguridad también tendrán que aprovechar las simulaciones de amenazas inmediatas para descubrir rápidamente su nivel de riesgo en relación con las amenazas emergentes".

DARKTRACE

José Badía
Country Manager Spain & Portugal

"La IA desempeñará un papel clave en todos los sectores y funciones, también en el 'lado del mal', y también destacará que los ciberdelincuentes se centrarán en MFA. A ello se sumará que el 'hacktivismo' complica la atribución cibernética y las estrategias de seguridad. Y que el *criptojacking* se vuelve peligroso, por el secuestro de recursos informáticos para extraer criptomonedas. Y en 2023, los crypto-jackers se volverán más inteligentes y podríamos comenzar a ver los efectos perjudiciales de lo que generalmente se considera inevitable o insignificante. Asimismo el *ransomware* se 'lanzará' a la nube'. En definitiva, un panorama complejo que requerirá, sumado a la recesión, que los CISO sean francos con la dirección y apuesten, de forma proactiva, por mejorar continuamente su resiliencia cibernética".

DAVINCI

Javier Hijas
Cloud Security Partner

"2022 terminó con los mercadillos navideños de la *dark web* cargados de ofertas *ransomware as a service* por lo que 2023 no nos librará de seguir viendo un incremento en el número de víctimas de estos ataques. Este mercado también ofrece servicios genéricos de *hacking* que una situación económica complicada como la que se avecina y en una situación geopolítica como la que vivimos en Europa con la guerra aumentará el número de ataques dirigidos y complejos. Unas técnicas que evolucionaron en 2022 y que se espera que lleguen a su madurez en este 2023 son los relativos a evasiones de soluciones de EDR, que ya han alcanzado una gran base instalada como solución estándar para proteger los puestos de trabajo. Y sabiendo ahora que en 2022 los asistentes de chatbot demostraron ser capaces de realizar ataques bajo demanda habrá que esperar no sólo un incremento de la actividad maliciosa por la facilidad adicional que estas herramientas ofrecen sino también una nueva familia de ataques que la IA comience a generar por sí misma.

DELINEA

Roger Gallego
Iberia Sales Manager

"Veremos un incremento de amenazas dirigidas a obtener accesos individuales para realizar movimientos laterales dentro de una organización, con el objetivo de causar daños económicos y reputacionales. Contar con una estrategia fuerte de gestión de accesos a los activos de una empresa, apoyada en tecnologías de autenticación multi-factor y gestión de credenciales, será más necesaria que nunca".

DELOITTE

Rubén Frieiro
Consultor de Ciberseguridad y Socio

"No se espera un gran cambio en las amenazas frente a lo vivido en 2022, sino un incremento y sofisticación de las mismas. La tendencia en el uso de ingeniería social y las posibilidades que ofrece la IA propiciarán más ataques y con más éxito a personas. El contexto de inestabilidad geopolítica y de economías en recesión pondrá aún más en el objetivo a organismos públicos".

DEVO

Vincent Laurens
VP Global Security Strategist and General Manager EMEA

"Si basamos nuestra respuesta en los hechos, seguro que algunos ataques tendrán un gran impacto en 2023. Si tuviera que citar solo uno, diría que el ataque *ransomware* en el sector sanitario y hospitalario. Todos sabemos que la evolución en este campo sigue siendo limitada. No porque no estén tratando de contrarrestar a los actores maliciosos sino porque, principalmente, el presupuesto por su parte sigue siendo escaso. Por eso creemos que todo lo que pueda aportar más autonomía/automatización en este campo, como un enfoque de SOC autónomo, puede ser de gran ayuda".

DIGITAL.AI

Mike Woodard
Vicepresidente de Gestión de Productos

"Los ciberdelincuentes se volverán más descarados: Cuando escucho de un pariente sin conocimientos de ciberseguridad que una pequeña clínica que ella frecuenta ha sido pirateada y que sus registros se están reteniendo para pedir un rescate, es muy fácil comprender que los atacantes están buscando cualquier grie-

ta para explotar. Si almacena datos confidenciales, es probable que los atacantes ya estén dando vueltas en busca de su oportunidad. Nuestros datos recientes muestran que, en un período de una semana a partir del 13 de noviembre de 2022, más de la mitad de las aplicaciones que nuestros clientes protegen fueron atacadas. Estos datos indican una clara necesidad de Defensa en profundidad de DevSecOps, en otras palabras, no solo Pruebas de Seguridad de aplicaciones sino, también, ofuscación de código, monitorización y autoprotección de aplicaciones en tiempo de ejecución".

DIGITEL DS
Rubén Fuentes
CISO

"Los nuevos avances en IA van a permitir que este año 2023 empecemos a estar más expuestos a un conjunto nuevo de amenazas inéditas que van a impactar de forma directa en los procesos de validación de identidad a distancia (deepfake: deepfaces, deepvoices), ya que, se hace más difícil identificar y diferenciar entre el 'material real' y el 'material *deepfake*'. En este sentido, se requerirán diseños más robustos, más alineados aún con las mejores prácticas y estándares como el NIST; que evalúan las soluciones de biometría facial, voz, huella dactilar o iris. En concreto, para este tipo de soluciones de validación de identidad, será especialmente relevante la evaluación de la biometría facial que permitirá aumentar el nivel de seguridad técnica para que los sistemas cumplan con los requisitos más exigentes de mercado que minimicen lo más posible los riesgos de suplantación de identidad.

DINOSEC & GUARDEDBOX
Raúl Siles
Founder & Senior Security Analyst

"Los ataques de mayor impacto afectan al acceso y/o manipulación de la información más sensible y confidencial de las organizaciones. Sin embargo, seguimos haciendo uso de tecnologías no lo suficientemente seguras para su gestión y compartición, sin cifrado E2E o sin una correcta verificación de la identidad de los interlocutores, facilitando ataques con una reducida complejidad ¡Cambia!".

DLTCODE
Ricardo Barrasa
Director de Cumplimiento y Riesgo

"Consideramos que los ataques se van a volver más específicos y personalizados. La Inteligencia Artificial y el Machine Learning lo utilizarán tanto los atacantes como los que se defienden. Seguirá proliferando las técnicas de phishing y smishing para conseguir secuestros de datos. El ransomware se va a ensañar con la PYME. Cada día veremos más ataques de gran impacto al cloud".

DOTFORCE
José Luis Pozo
Técnico de preventa

"El éxito de Chat-GPT augura que en 2023 una proliferación de los ataques que utilizan las cualidades conversacionales de las IA, que permitirán elaborar fácilmente ataques de ingeniería social cada vez más realistas y en cualquier idioma, así que las organizaciones de todo tipo deberán aprender a defenderse de estos ataques y utilizar tecnologías de autenticación resistentes al *phishing*".

DXC TECHNOLOGY
Mikel Salazar
Iberia Cybersecurity Country Lead

"En un ecosistema de continuas tensiones geopolíticas, las amenazas crecerán de manera exponencial en un año con más de 70 países celebrando elecciones gubernamentales. Los principales objetivos serán las infraestructuras nacionales críticas, la expansión del metaverso ampliará el riesgo especialmente en identidad y el uso de la IA será usado cada vez más tanto por atacantes como defensores".

DYNATRACE
José Matias
Regional Director Iberia

"2023 estará marcado por la automatización de datos inteligente en entornos colaborativos y multicloud. Esto exige una férrea ciberdefensa para proteger la nube, las herramientas de monitorización, los modelos predictivos, etc. Todo para conseguir una mayor 'observabilidad y conocimiento para la innovación segura de las empresas. Sectores como la banca, seguros, healthcare, entre otros, tendrán que garantizar la seguridad de sus procesos. Para ello, en materia de ciberseguridad va a ser clave la evolución de las estrategias DevOps en DevSecOps y SecDevBizOps. Este enfoque permite madurar las soluciones y estrategias tecnológicas de manera más holística, conduciendo a una mayor inversión en plataformas de observabilidad que puedan respaldar los procesos innovadores de las empresas, garantizando que todos tengan las respuestas necesarias para ser responsables y ofrecer una innovación tecnológica y digital segura".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

EFFICIENTIP

Diego Solís
Sales Director Iberia & LATAM

"La filtración de datos será en 2023 una de las mayores amenazas ya que, al emplear técnicas similares a las utilizadas en la tunelización de DNS, consigue que los atacantes adopten una aproximación de 'nivel bajo y lento' para no despertar sospechas, al no provocar un pico en el tráfico de DNS extrayendo pequeños fragmentos de datos antes de que la empresa lo detecte. Sus consecuencias son el uso fraudulento de la información, pérdida de confianza y multas por incumplimiento de la ley".

ELASTIC

María Campos
Regional Vice President Elastic South

"Es relevante constatar como el *phishing* sigue siendo todavía el método más común para conseguir el acceso inicial. Las cuentas IAM válidas continuarán siendo un objetivo como puerta de entrada y para autenticar recursos *cloud*. Las cuentas de servicio gestionadas por los mayores CSPs (Google, AWS, Microsoft) con permisos erróneos servirán de paso intermedio para un acceso persistente. Las máquinas virtuales Linux utilizadas por DevOps y desplegadas en entornos de nube serán otro objetivo. Los adversarios seguirán utilizando herramientas nativas (p.ej. Rundll32.exe, ficheros LNK) como proxy binario para cargar software malicioso o *payloads* ISO. Las organizaciones que no disponen de capacidades de mitigación centralizada sufrirán para dar una respuesta eficaz ante todo tipo de amenazas."

ENTELGY INNOTEC SECURITY

Jorge Uyá
Director de Operaciones

"Va a ser el año del cibercrimen a sueldo: el *ransomware*, el *phishing* o los ataques DDoS estarán disponibles as a service y podrán ser adquiridos por cualquiera, independientemente de sus conocimientos (con el incremento considerable del riesgo que ello conlleva). Todo ello unido a la triple extorsión que ya se ha empezado a ver en los ataques de *ransomware* (cifrado de sistemas, publicación de datos y ataques de denegación de servicio). Por desgracia, además, las amenazas serán más especializadas y sofisticadas, y habrá que prestar especial atención a los ataques automatizados con inteligencia artificial y al escenario que se plantea a nivel geopolítico derivado de conflictos tan cercanos como el ruso-ucraniano que afecta al territorio digital mundial. No podemos olvidar que los dispositivos móviles serán una de las principales puertas de entrada a las organizaciones para los ciberatacantes, por lo que la concienciación seguirá siendo clave a 360º".

ENTHEC

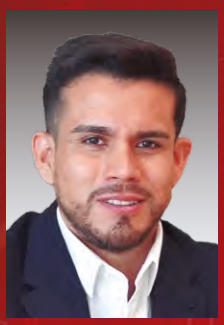
María Rojo Rivas
CEO

"En 2023 veremos cómo los atacantes utilizarán masivamente la Inteligencia Artificial para atacar a empresas y particulares. La IA aprenderá fácilmente sobre ambas mediante la recopilación de toda la información que existe en las redes (y que se desconoce), con la que diseñarán ataques de ingeniería social que se ejecutarán de forma automática, personalizada y dirigida.
Además, en el caso de las empresas, los ataques utilizarán también la información que obtengan de sus terceras partes que forman parte integral de su negocio, pero cuyo nivel de protección y posibles filtraciones de información no pueden controlar. Este nuevo escenario abrirá muchos huecos en los sistemas de defensa actuales que deberán focalizarse en evitar el 'entrenamiento' de los sistemas de IA de los atacantes".

ENTRUST

Rafael Cuenca
Sales Manager IAM South Europe

"Lo vemos como un año de consolidación y readaptación digital. La identidad y la autenticación se configuran claves en la interacción entre sistemas que han de ser resilientes en una realidad híbrida/Multicloud que avanza hacia una nueva dimensión Post Quantum. Vemos una reevaluación de estrategias Zero Trust que requiere la trasformación de los procesos de identidad de la organización".



EPIC BOUNTIES

José Ramón Palanco
CEO

"Se espera que en 2023, comiencen a surgir ataques de ingeniería social de nueva generación que utilicen los últimos avances de inteligencia artificial para lograr un mayor nivel de persuasión y realismo. Debido a esto, los ataques de spearphishing serán más personalizados y efectivos. Si el modelo GPT-3 ya nos ha sorprendido, no se puede negar la posibilidad de una evolución hacia un GPT-4 en 2023, lo que daría lugar a una auténtica revolución en el mundo de la IA y una oportunidad para los atacantes. Todo esto unido a la creación de voz e incluso video con deepfake, convierten a la ingeniería social en uno de los vectores de ataque más peligrosos".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

ESET España

Josep Albors

Director de Investigación y Concienciación

"España ha sido y va a seguir siendo un blanco ideal para el malware relacionado con el robo de información por varios motivos, entre los que se incluyen la facilidad que tienen los delincuentes para seguir explotando técnicas conocidas y la alta rentabilidad que, posteriormente, obtienen con estos ataques. El robo de credenciales es algo constante en las empresas españolas y estas pueden ser usadas en ataques más peligrosos, sin olvidar que el uso creciente de la inteligencia artificial facilita la creación de campañas de *phishing* cada vez más convincentes y que, sin lugar a dudas, vamos a ver como se incrementan en los meses venideros".

EXCLUSIVE NETWORKS

José Manuel Medina

Director de Desarrollo de Negocio para Iberia

"En 2023 se producirán ciberataques más complejos, continuando el factor humano como el eslabón más débil de la organización. Ataques de *malware* avanzando, *ramsonware* más sofisticado, y *phishing* geodirigido. Además, se producirán ataques que utilizarán técnicas que se sirven de redes domésticas (IoT), Inteligencia artificial como **método de intrusión,** y tecnologías de ***deepfake* como** herramienta ideal para engañar a la gente para que crea o haga algo que beneficie a un ciberdelincuente".

EUROCYBCAR

Azucena Hernández

CEO

"2023 es el año en el que "desembarcarán" los primeros vehículos homologados con el certificado de ciberseguridad que exige la normativa UNECE/R155. El propósito de esta normativa es que los fabricantes mitiguen hasta 70 posibles amenazas de ciberseguridad para minimizar el riesgo de un ciberataque contra la privacidad y la vida de las personas que viajan a bordo, así como la integridad de los sistemas del vehículo. ¿Qué se pretende evitar?: que un *cracker* acceda fácilmente a la información privada del propietario –quién es, cuenta bancaria, ubicación…–; manipular datos del vehículo –kilometraje, velocidad de conducción, enviar mensajes e indicaciones falsas al conductor–; de forma remota desbloquear las puertas, frenarlo y/o acelerarlo; introducir un virus que deje inoperativos los sistemas del vehículo; eliminar códigos software del vehículo…".

EVOLUTIO

Ricardo Sanz

Head of Cybersecurity Business

"Seguiremos viendo a los delincuentes confiar en la extorsión, aunque los datos del *ransomware* real puedan disminuir. El incremento y evolución tecnológica de las plataformas de suscripción tipo RaaS (*Ransomware-as-a-service)* y PhaaS (*Phishing as a Service*) permitirán atacar a casi cualquier actor y organización poniendo el foco en la exfiltración de información para dañar la reputación de marca, más allá de la encriptación de datos. En general, los desarrolladores de malware se centrarán en crear herramientas sigilosas, que eviten los sistemas de protección EDR como los del tipo downloader y dropper. Los ataques contra la cadena de suministro seguirán siendo una de las principales puertas de entrada para los cibercriminales. Los ataques contra las APIs seguirán creciendo ya que se está viendo un incremento del tráfico malicioso contra APIs del 681%, lo que ha llevado a que el 95% de las empresas hayan tenido un incidente por un ataque a alguna de sus APIs en los últimos 12 meses. Sin embargo, la identidad es ya más importante que el acceso al dispositivo, de manera que el robo de credenciales y acceso a cuentas de usuario será el principal objetivo este año. Veremos actores intentando robar credenciales mediante una combinación de ingeniería social, *access brokers* y fuentes de datos internas comprometidas. Se usarán estas credenciales robadas y nuevas técnicas para eludir los mecanismos de autenticación mediante MFA o soluciones de IAM".

EY

Jordi Juan Guillem

Socio. Ciberseguridad

"En 2023, las organizaciones criminales seguirán buscando ideas sofisticadas para engañar al usuario, como QR ilegítimos en servicios cotidianos. Así mismo, se seguirán explotando zero-days en aplicaciones muy extendidas, causando grandes daños a las organizaciones que las utilizan. Otro ámbito de preocupación es OT, donde aún existen sistemas muy obsoletos y fáciles de explotar. Como contrapeso, regulaciones como la NIS2 deberán servir para fomentar la seguridad".

FACEPHI

Jorge Félix Iglesias

Director de Seguridad, Calidad y Sistemas

"De los muchos que vendrán, el mayor reto al que nos enfrentamos este año es el aseguramiento de la PII (Personal Identifiable Information) de usuarios y clientes. Garantizar la identidad digital, la confiabilidad y la resiliencia de sistemas y soluciones encargadas de custodiar estos datos como baluarte para el Negocio, será el principal caballo de batalla en el sector".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

FACTUM

David López García
Director de Operaciones

"El traslado de las identidades de los usuarios al *metaverso* traerá consigo una mayor uso de dispositivos de VR, sensores y cámaras conectadas a internet, lo que conllevarán una mayor generación de datos potencialmente vulnerables. El delito de *usurpación de identidad,* por ejemplo, podría llevarse a otro nivel ya que los atacantes podrían suplantar a las víctimas explotando tanto los datos de comportamiento como los biológicos, recopilados por los diferentes dispositivos utilizados. La evolución de las IAs abre un abanico de nuevas oportunidades a los ciberdelincuentes, siendo capaces de crear *exploits* con tan solo pedírselo a *ChatGPT*. Otro claro ejemplo son los *deepfakes*, capaces de engañar tanto a personas como a algoritmos. Por último, el desarrollo de la computación cuántica podría romper fácilmente los algoritmos de cifrado que usamos habitualmente, por lo tanto, será necesario hacer una transición antes de que esta tecnología esté extendida.

FASTLY

Daniel Howe
Senior Presales

"Seguiremos viendo ataques gestionados por bots, pero cada vez serán más complejos y difíciles de identificar. Además, habrá más empresas que ofrezcan servicios de ofuscación de ataques, como VPN, IP, etc., lo que facilitará mucho la contratación de servicios de *scrapping*, *scalping*, *credential cracking* o *stuffing*. A veces, el principal riesgo puede ser interno debido a la falta de formación de la organización o de personal adecuado para hacer frente a las amenazas en evolución. Por tanto, los responsables de las empresas deben considerar el valor de la seguridad interna frente a la eficacia de la externalización para que sus operaciones de seguridad sean lo más eficientes posible y para reducir los riesgos de forma tangible. Dicho esto, si las empresas aplican correctamente los principios fundamentales, serán capaces de defenderse contra la mayoría de las amenazas más comunes".

F5 NETWORKS

Daniel Varela
Ingeniero de soluciones Especialista en Seguridad para el sur de Europa

"Vemos un reto importante alrededor de las APIs y la agilidad que requiere el negocio. La combinación de amenazas y de "Shadow APIS" hace cada vez más necesaria la visibilidad para este tipo de tráfico. Estamos viendo amenazas relacionadas con la autenticación (y más concretamente con los MFA) Es necesario mirar a soluciones que vayan más allá y que garanticen la identificación correcta de los usuarios. Las librerías Open Source serán un objetivo principal de los atacantes, es necesario contar con soluciones que proporcionen visibilidad de los componentes software utilizados y su comportamiento".

FORCEPOINT

José Bavaresco
Channel Sales Engineer EMEA

"El desplome del Bitcoin ha promovido alianzas entre los grandes de la industria de la ciberdelincuencia. Estas "oscuras organizaciones" superan a muchas empresas dedicadas al sector de la ciberseguridad en infraestructura, desarrollo y en capacidad económica, por lo que los secuestros de información cada vez son más sofisticados".

FORGEROCK

Carlos Scott
Digital Risk Consultant en ForgeRock España

"La digitalización del mundo no se ralentizará en 2023. Los *hackers* siempre explotarán la vida *online* de los consumidores. Las credenciales violadas se utilizarán para cometer fraude en los sitios de compras online y entidades financieras, de seguros, entre otros. Las identidades digitales que no se gestionan de forma inteligente son las semillas perfectas para perpetrar nuevas violaciones".

FORENSIC & SECURITY

Santiago Arellano
Cyber account manager

"Vamos a oír hablar y mucho del uso de la AI como principal herramienta de ataque. Todas las tareas que de manera "manual" estaba realizando el ciberatacante, las puede hacer ahora con ayuda de la IA: intrusión, ingeniería social, aprendizaje de usos y costumbres del usuario, robo de credenciales, campañas de *phishing*… Además, la IA se convertirá en propulsora de ciberataques más sofisticados, efectivos y mejor planeados. Es solo el principio y ya nos ha quedado constancia del uso del que comienza a ser célebre, ChatGPT, para realizar ciberataques de gran magnitud".

FORESCOUT

Carlos Moliner
Strategic Accounts Manager

"A medida que IoT y OT continúan convergiendo con la TI tradicional, los actores maliciosos buscarán explotar esta superficie de ataque más amplia y prácticamente todos

los sectores se verán afectados. Por ejemplo, desde Forescout prevemos que en 2023 el sector de la salud verá un aumento notable en el número de ataques, donde la "inseguridad por diseño" presente en muchos dispositivos médicos conectados los convierte en objetivos cada vez más tentadores para los cibercriminales cuyo objetivo será interrumpir la prestación de atención médica. En 2023, los ataques cibernéticos no solo podrían extenderse de forma espontánea a los dispositivos médicos, como fue el caso de varios incidentes de *ransomware* en 2022, sino incluso comenzar a atacarlos directamente".

FORTINET

Acacio Martín

Director Regional para España y Portugal

"2023 vendrá marcado por los ataques avivados por el modelo de Cibercrimen como Servicio (CaaS), así como los nuevos *exploits* en entornos no tradicionales como los dispositivos en el perímetro o los mundos virtuales. Los ciberdelincuentes encuentran más formas de transformar en armas las nuevas tecnologías a escala suficiente para generar una mayor disrupción y destrucción. No sólo atacan la superficie tradicional, sino lo que hay detrás de ella, es decir, tanto fuera como dentro de los entornos de red tradicionales y dedican más tiempo al reconocimiento, para intentar evadir la detección, la inteligencia y los controles. Ante este panorama, las organizaciones deberán disponer de una plataforma de ciberseguridad integrada con las redes, los *endpoints* y la nube que permita una inteligencia de amenazas automatizada y procesable, junto con capacidades avanzadas de detección y respuesta, basadas en el comportamiento"

FUJITSU ESPAÑA

Javier Pérez García

Head of Cybersecurity

"Desde Fujitsu observamos una evolución de los ataques con foco en tecnologías que habilitan la transformación digital. Esto ocurre en ámbitos como la nube, biometría, criptografía, 5G, big data, OT y IoT o ataques contra bancos que prestan servicios de criptomonedas.

Uno de los sectores en el que estamos viendo un mayor incremento del número de amenazas es el sector sanitario. Tanto por aumento de dispositivos conectados (en 2025 se estima que el 68% de los dispositivos médicos estará conectado), el aumento de los ciberataques durante el COVID (incremento del 150% de ciberataques), así como el hecho de que los hospitales se ha convertido en *target* habitual de los ciberataques".

GHENOVA

Enrique Cubeiro

Director de Ciberseguridad

"En mi opinión, este año va a ser el del establido de la inteligencia artificial en apoyo a la actividad ofensiva (creo que a los defensores aún les va a costar unos años incorporar de forma tan decisiva la IA en su beneficio) y, por tanto, un año en el que la brecha entre ataques y defensas va a ser más amplia de lo habitual, con lo que ello supone. Los atacantes explotarán las innumerables posibilidades de la IA para desarrollar *malware* más efectivo y difícil de detectar, ataques más rápidos y sigilosos, campañas de *phishing* y *spoofing* más consistentes y creíbles (y, por tanto, con mayor índice de éxito), ... Va a ser un año tremendamente interesante".

GIESECKE + DEVRIENT

David González

SVP Digital Payments & Smart Cards

"La tecnología *deepfake* se ha hecho lo suficientemente madura para que nos empiece a preocupar la capacidad de alterar audiovisuales y de esa manera aumentar la efectividad de los ataques phishing y BEC. Debemos anticiparnos e invertir en soluciones a prueba de la buena fe de los usuarios y de la ingenierí social para garantizar la privacidad de nuestra información y los servicios digitales".

GMV

Javier Zubieta

Director de Marketing y Comunicación de Secure e-Solutions de GMV

"El propio sector se está saboteando al contribuir al problema de la falta de talento, amenazando su sostenibilidad sin necesidad de ataques externos. La anticipación a los retos del 2023 como la identidad digital en el metaverso, el código fuente vulnerable e inmutable en *smart contracts* o el nuevo paradigma Web3 servirá de poco si no hay IN (Inteligencia Natural) que los gestione".

GOOGLE CLOUD

Héctor Sánchez

National Technology Officer

"Las relaciones de identidad y confianza en y entre los entornos de nube seguirán siendo complejas, abriendo oportunidades a que los atacantes puedan tener un impacto más amplio y profundo en las organizaciones. Observaremos un aumento de los ataques

dirigidos a los sistemas de identidad que permiten autenticaciones cross-plataforma en lugar de directamente a los endpoints. Las dependencias de terceros será un tema importante dado el éxito de incidentes públicos como el que afectó a SolarWinds. Predecimos que al menos un actor de APT utilizará actualizaciones de software aparentemente legítimas para enviar malware a sistemas de terceros en 2023, después de haber comprometido a algún proveedor de software. También es probable que veamos un aumento de ataques dirigidos a interrumpir los servicios y recursos en la nube que respaldan los sistemas de producción de OT a través de ataques de denegación de servicio (DoS), por ejemplo, moviéndose a través de redes segmentadas incorrectamente, implementando *ransomware* o incluso mediante desarrollo de malware personalizado. Predecimos mayor sofisticación de las herramientas de ataque específicas para entornos en nube y observaremos una variedad de *ransomware* que apunte a las copias de seguridad almacenadas en la nube, incluido el historial de revisión."

GRUPO ICA
Alberto Cañadas
Director de Ciberseguridad – Preventa y Desarrollo de Negocio

"Se va a continuar poniendo énfasis en sectores críticos para los estados, polarizando la ciberguerra aún más. Se observan tendencias en nuevos objetivos tras el avance en las amenazas de IT a OT y finalmente a personas, generando un nuevo escenario a proteger por las entidades gobierno, así como por las empresas de servicios de ciberseguridad. La IA representa un salto tanto en la defensa como en el ataque a múltiples objetivos con un coste beneficio cada vez mejor para los actores, por lo que técnicas en la tecnología como el threat hunting automatizado y la automatización/orquestación entre tecnologías diferentes pasa de ser un complemento a una obligación para todo tipo de entidades".

GRUPO TRC
Emilio Rico
Asesor de Ciberseguridad

"Reconozco que se me pasó por la cabeza pedirle a ChatGPT que me redactase esta nota con las predicciones de ciberseguridad para 2023 y es que la aparición de estos modelos de IA ha sido el hecho más llamativo de finales de 2022. No dudo que en 2023, la IA nos deparará grandes sorpresas, a veces miedo, una cuantas alegrías, pero también muchos dolores de cabeza.
Pero aparte de la IA, tendremos otros ciber protagonistas, como los ataques a la cadena de suministro (una técnica traicionera, pero poderosa) la gestión de identidades (aspecto clave en las empresas) y todo tipo de técnicas para eludir la autenticación multifactor (con proxies *de phishing* y captura de tokens), que acabarán con el robo de datos y el temido ransomware (de propina). 2023 será también el año definitivo para adoptar soluciones como SASE y XDR en los end-point. Me preocupa que, ante una posible recesión, algunas empresas dediquen menos recursos y menos presupuestos a su seguridad, quedando más expuestas a las amenazas y reduciendo su capacidad para afrontarlas. Y también será interesante seguir de cerca el debate sobre los ciberseguros, el aumento de las primas y los nuevos requisitos exigibles, que en realidad es el debate entre afrontar el riesgo o transferirlo."

HISPASEC
Fernando Ramírez
CEO

"Detrás de cada gran ataque no es raro encontrar el uso de ingeniería social para conseguir romper esa primera barrera que permite a los atacantes acceder a las grandes corporaciones.
La irrupción de herramientas accesibles y masivas de inteligencia artificial como ChatGPT de OpenAI, serán usadas por los ciberdelincuentes para mejorar sus estrategias de ingeniería social. Esto derivará en una mayor efectividad y por consiguiente, en un mayor número de los ataques que usan esta técnica como son los phishings, el ransomware e incluso ataques tipo APT".

HORNETSECURITY
Félix de la Fuente
Country Manager

"2023 nos traerá más ataques, de todo tipo, explotando nuevas vulnerabilidades. Por ello, contar con un experto que provea de soluciones actualizadas en la nube, *multitenant* e independiente, es fundamental. Frente al mayor número de ataques es fundamental protegerse, formarse y recuperarse ante un incidente. En Hornetsecurity hemos acompañado a empresas e instituciones, dando una respuesta de ciberseguridad experta y con soluciones enfocadas en la creciente dependencia de la nube. En el ámbito de la preacción en la protección, es fundamental formar a los usuarios, receptores a través del mail de los posibles ataques. Además, bajamos la exposición del usuario, filtrando todo el flujo de información hacia él. Y si aun así, el ataque se produce, a través de nuestras soluciones perennes de back-up, recuperamos los datos en minutos".

HP
Carlos Manero
Security & Digital Services BDM

"Esperamos un 2023 continuista respecto a nuestro presagio para 2022, donde poníamos el tándem dispositivo-usuario como principal eslabón débil en la cadena y, por tanto, foco de ataque para el cibercrimen. Si bien en 2022 hablábamos de como de-

bía evolucionar la protección del dispositivo no solo a través de métodos como el EDR sino hacia métodos complementarios como soluciones basadas en el aislamiento, dado que comenzábamos a ver ataques que eran capaces de burlar soluciones de detección y respuesta. En la última parte del año, hemos visto en reportes internos de tipos de ataques, como por primera vez los ficheros de extensión ZIP y RAR han superado a los ficheros de la suite Office como principal método de ataque. No solo es un cambio en el principal tipo de extensión, sino en el tipo de ataque, utilizando una técnica llamada "HTML smuggling" (como en los últimos ataques como QakBot y IceID), lo que da como resultado que las estrategias de protección basadas solo en la detección resulten insuficientes. Además, hemos detectado ataques muy complejos, utilizando una cadena modular que permitía cambiar el ataque dinámicamente entre un spyware, *ransomware* o *keylogger* en mitad del ataque. Todo esto unido a que el cibercrimen es ya un negocio muy rentable nos lleva presagiar más ataques y más complejos, tratando siempre de eludir los métodos de protección, por lo que debemos tratar de complementar con distintas soluciones de seguridad todos los tipos de ataque".

HUAWEI
José Capote
CSPO de Huawei España

"Según el último informe de ENISA, los principales ataques de ciberseguridad estarán relacionados con *ransomware*, malware, robo de datos, ataques de denegación de servicio, amenazas a través de Internet, desinformación y ataques a través de la cadena de suministro. En la misma línea, el Foro Económico Mundial (WEF) indica en su Informe Anual 2023 sobre Riesgos Globales, que los ataques cibernéticos estarán relacionados con *ransomware* y brechas de datos de carácter personal".

IAAS365
Miguel Ángel Arroyo
Director de Ciberseguridad

"La situación geopolítica actual seguirá deparando ciberataques entre los países participantes en el conflicto y que tendrán como objetivo las infraestructuras críticas de dichos países. Además, continuará la proliferación de plataformas de aprendizaje de *hacking* o torneos de CTF (*Capture The Flag*) entre los jóvenes, creciendo la preocupación de que algunos utilicen dichos conocimientos para atacar organizaciones de manera aleatoria. 2023 no será un año de grandes cambios en cuanto a la tipología de las amenazas, pero sí destacará por la evolución de las ya conocidas, que intentarán utilizar nuevas tácticas, técnicas y procedimientos para evadir los mecanismos de seguridad, como por ejemplo HEAT (Highly Evasive Adaptive Threats). Finalmente, no podemos olvidarnos de la IA y su uso para desarrollar y automatizar nuevos ataques. Así, *Deepfake* seguirá evolucionando, intentando desarrollar recursos audiovisuales muy reales que tendrán como objetivo engañar al usuario mediante la suplantación de una identidad".

IBERLAYER
Pedro David Marco
CTO y Fundador

"La ciberdelincuencia sigue moviendo muchísimo dinero a nivel mundial. Pese a la guerra de Ucrania y los desplazamientos de objetivos en grupos rusos y ucranianos, los intentos de phishing, fraude y de *ransomware* siguen al rojo vivo. El usuario sigue siendo el eslabón a romper y dado que los sistemas de 2FA son cada vez más comunes, no son pocos los ataques que veremos contra ellos".

IBERMÁTICA (AN AYESA COMPANY)
Álvaro Fraile
Director, Cybersecurity Services, Global Group

"Los algoritmos de IA se utilizarán para identificar sistemas con seguridad débil o que contengan datos valiosos. Las infraestructuras críticas y el sector público seguirán siendo objetivos atractivos para los ciberatacantes y nos encontraremos con mayores amenazas para el sector sanitario por el crecimiento de los entornos IoT desplegados. La guerra cibernética contará con atacantes internacionales patrocinados por estados que apuntarán tanto a empresas como a gobiernos. Los ataques de *ransomware* serán los más sofisticados conocidos hasta ahora. El Internet de las cosas con tecnología 5G y la seguridad en la nube, requieren todavía mucha investigación para que el sistema sea seguro contra ciberataques externos por lo que serán entornos extremadamente atacados".

IBM
Isabel Tristán
Principal Security Software Sales Manager de IBM Technology en SPGI

"El teletrabajo híbrido será, un año más, el objetivo de los ciberataques a las empresas y la puerta de acceso estará en los *routers* domésticos y las VPN sin parches, la infraestructura de nube de *back-end* y los dispositivos SOHO conectados en los hogares. Otra de las grandes amenazas en 2023 serán las recompensas por fallos llevadas a cabo por grupos maliciosos, como el que pudimos ver el pasado verano con Lockbit 3.0".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

INETUM

Manuel Calderón
Cybersecurity & Digital Identity BU Director Group VP

"Desde el punto de vista de Inetum esperamos que los ataques dirigidos a la cadena de suministro de las empresas y administraciones públicas se están incrementando, según se constata en informes publicados por el CCN o ENISA, que recogen entre las principales amenazas a la ciberseguridad de los próximos años (hasta 2030) la dependencia del software de las cadenas de suministro, viéndose por tanto comprometida su ciberseguridad. Lo que quizás no sea tan esperado o eleve la complejidad de los ataques y pongan a prueba los sistemas de protección, detección y respuesta de las organizaciones, sea el acceso a técnicas más asequibles de IA que permitan que el grado de sofisticación de los ataques sea más elevado, y su potencial uso en vectores que hasta ahora eran detectables o no habíamos considerado, nos obligue a redefinir como enfrentarnos a esta nueva tipología de amenazas".

INFOBLOX

Joaquín Gómez
Cybersecurity Leader para el Sur de Europa

"Las amenazas harán foco en tácticas de evasión ante MFA, EDR e identidad, el malware mutará y aparecerá antes en dominios maliciosos (menos detectables), la monitorización DNS y el CTI para combatirlos será fundamental. Veremos mayor foco en prevención temprana, IA predictiva, automatizaciones e incremento del esfuerzo en ciber resiliencia de cara a minimizar impactos y dar continuidad".

INTERNET SECURITY AUDITORS

Daniel Fernández Bleda
Director Comercial

"Desde el punto de vista de la tecnología no anticipamos el efecto que tendría la apertura a servicios de libre uso de la IA aplicada a la generación de vídeos, audios y textos y, geopolíticamente, no pensamos que se iniciaría una guerra a las puertas de Europa que tendría un efecto tan global. Lo primero abre una puerta a la aplicación al cibercrimen para evadir controles de seguridad humanos. Lo segundo desembocará en pequeños –y no tanto– incidentes de seguridad que van a tener impacto en grandes empresas y organizaciones de ambos lados."

IPM

David López Pacheco
Cybersecurity Product Specialist

"En 2022, vimos cómo las incidencias por APTs (*Advanced Persistent Threats*) fueron evolucionando y son cada vez más sofisticadas, siendo capaces incluso de saltarse los sistemas de MFA por medio del secuestro de las cookies de sesión, que son usadas para acceder a determinados recursos. Si a eso le sumamos el incremento de grupos organizados que se dedican a la ciberdelincuencia, según el último informe de Mitre ATT@CK, nos hace prever un incremento en los ciberataques. Durante estos últimos años, las empresas han evolucionado y mejorado las capas de Protección, Prevención y Respuesta del NIST, pero todavía hay un gran camino que recorrer en la Recuperación, tal y como nos refleja el 'III Indicador de madurez en ciberseguridad' del ISMS Forum, este es el último paso hacia la ciber resiliencia, imprescindible para asegurar una rápida recuperación, minimizar el impacto y reducir las pérdidas económicas, ello será sin duda un importante reto para 2023".

ISDEFE

José Antonio Pérez Rodríguez
Gerente de Seguridad de la Información

"Seguro que habrá más de lo mismo, porque eso demuestra el histórico. También es probable que haya algo peor, porque los atacantes se benefician del avance de la tecnología (como por ejemplo de la IA) y del aumento de la superficie de exposición (transformación digital, migración a la nube, metaverso), y casi seguro que alguna sorpresa hará acto de presencia, porque hay situaciones que no se pueden prever, como hemos podido comprobar con todo lo que ha generado la guerra de Ucrania o la crisis energética de este año, o simplemente surgidas por la introducción de nuevos servicios o tecnologías (5G, web 3) que atraigan el interés de los delincuentes".

JUNIPER NETWORKS

David Noguer
Director de Marketing para Alianzas Estratégicas

"La inestabilidad geopolítica favorece el crecimiento de ataques a empresas, instituciones públicas o infraestructuras básicas. Los gobiernos crean agencias para asesorar a la población en ciberprotección. Se prevé un incremento en la adopción de tecnologías IoT. Los dispositivos IoT y sus servicios en la nube se convierten en nuevos puntos de vulnerabilidad.Otro punto de entrada de nuevos ataques es el modelo de trabajo hibrido que requiere una mayor formación de los teletrabajadores, conexiones seguras y equipos protegidos. Una de las principales novedades tecnoló-

gicas en ciberseguridad, será la entrada de la Inteligencia Artificial en la toma de decisiones gracias a su capacidad de analizar gran cantidad de datos. En 2023 aparecerán los primeros servicios de 5G Network slicing, la micro-segmentación en entornos corporativos y se generaliza SD-WAN".

KASPERSKY

Alfonso Ramírez
Director General de Kaspersky Iberia

"Se espera un aumento de ciberataques con motivaciones políticas y el enfoque de grupos de *ransomware* en datos médicos y personales. La escasez de semiconductores y filtraciones de datos de proveedores de servicios públicos también afectará al tejido empresarial. El *malware* basado en IA también jugará un papel importante este año".

KEYFACTOR

Julio Prada
Sales Director Iberia

"Durante 2023, asistiremos a un aumento de ataques dirigidos a infraestructuras energéticas, incluyendo empresas que gestionan la electricidad y que explotan y suministran combustibles y energía. Además, los ataques a infraestructuras críticas como telecomunicaciones y servicios médicos se volverán más frecuentes y sofisticados. Los dispositivos y sensores IoT, cuyo número seguirá aumentando considerablemente, también serán un objetivo, a pesar de que a menudo descuidamos su seguridad. También veremos un aumento de ataques a empresas de software, donde el objetivo no solo es el código sino también obtener certificados de firma de software, lo que permite a los atacantes distribuir versiones modificadas que aparentan ser completamente legítimas a la seguridad sistemas operativos".

KPMG

Sergi Gil
Socio Technology Risk

"Aproximadamente, el 80% de los incidentes de seguridad en las compañías son provocados por la poca concienciación existente entre los empleados. De estos casos, el 60% no hubieran sido víctimas del engaño si hubieran recibido más formación. En conclusión, la principal amenaza en estos próximos años, añadiendo la rápida evolución y la complejidad de los ataques, van a ser las personas".

KROLL

Juan Carlos Díaz García
Associate Managing Director, Cyber Consulting

"En 2023 los atacantes priorizarán el robo de información y el chantaje frente al despliegue de *ransomware*. Conscientes del daño reputacional, las compañías podrían ver más razonable pagar por evitarlo, que por acceder a los sistemas cifrados. Veremos nuevos servicios de *Ransomware as a Service* orientados a tal fin. Además, sabiendo el valor que tiene la identidad digital de una compañía, veremos nuevas formas de robarlas para acceder a los sistemas sin necesidad de vulnerarlos. Utilizarán la potencia de las IAs para realizar tanto ataques dirigidos muy sofisticados (tipo *deepfakes*), como ataques masivos. Si una IA entrenada en ingeniería social con un claro objetivo puede mantener miles de conversaciones en paralelo, definitivamente la estadística jugará a su favor".

KYNDRYL

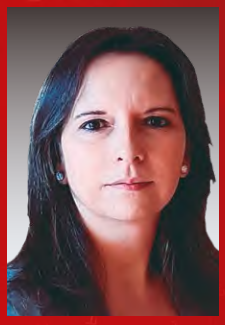
Miguel Ángel Ordóñez
Director de Resiliencia y Ciberseguridad, España y Portugal

"Las empresas deben dar prioridad a los programas de modernización de herramientas e infraestructuras como la nube híbrida, para lograr una transformación empresarial resiliente. La resiliencia operacional da continuidad a las operaciones; sea una caída en red, un problema con los servidores o un ciberataque. Lo importante es ser proactivos y asegurar la continuidad del negocio en todo momento".

LEET SECURITY

Antonio Ramos
CEO

"Dada nuestra visión sobre la seguridad en la cadena de suministro, creemos que este año veremos como se expande la "fusión" entre el *ransomware* y la cadena de valor. Es decir, los criminales intentarán monetizar el *ransomware* no solo con el propio afectado, sino extorsionando a los terceros afectados por el incidente.



LIDERA

Nieves Acebal
Service Manager

"La cadena de suministro, los servicios *cloud* y los usuarios serán los más afectados por los ciberataques en 2023, ya que los ciberatacantes intentarán aprovechar el eslabón más débil, las pequeñas empresas colaboradoras y los usuarios, utilizando vulnerabilidades en las aplicaciones y técnicas como la inteligencia artificial que permitirá crear ataques más precisos y efectivos".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

LIVEACTION

Carlos Ferro
SVP & GM International Region

"La proporción de brechas causadas por *ransomware* creció un 41 % en 2022 y seguirá. El trabajo remoto continuará generando más suplantación de identidad y *phishing* (primer y segundo vector de ataque). El entorno de IoT seguirá siendo objetivo de ataque (+43.000 millones de dispositivos conectados en el mundo) y la continua evolución de la tecnología de IA aumentará la cantidad y sofisticación de los ataques. Aquí es donde lo observabilidad para detectar amenazas y el uso de la IA para analizar patrones de actividad en la red e identificar comportamientos a una velocidad más allá de la humana, se vuelve relevante al eliminar la carga de los equipos de seguridad, al sortear rápidamente el ruido y resaltar las áreas que realmente requieren atención. Las empresas que usan IA y automatización para detectar y responder a las filtraciones ahorran una media de 3 millones de dólares en comparación con las que no lo hacen."

LOGALTY (GRUPO)

Óscar Conesa
CISO

"Las herramientas de Inteligencia Artificial de OpenAI, como DALL-E y ChatGPT, nos han sorprendido con sus capacidades. Es probable que veamos nuevas formas de fraude tecnológico apoyado en ellas en 2023. En breve no podremos saber si una imagen, video, audio o conversación son reales o han sido manipuladas por una IA."

LOGICALIS

Miguel Ángel Cuasante
Security Presales Manager

"Es de esperar que veamos potenciados los ataques centrados en "engañar" a los usuarios como principal vía para entrar en las organizaciones mediante el robo de credenciales y la suplantación de la identidad digital (especialmente mediante correos, whatsapps o SMS's fraudulentos cada vez más elaborados y cercanos a los gustos y aficiones de los destinatarios). Además, debido al paradigma ocasionado por la transformación digital y la 'inmediatez' a la hora de desplegar los aplicativos (cada vez es mayor el número de amenazas relativas a los 'nuevos' entornos DevOps, incluyendo sofisticados ataques a las APIs y a las cadenas de suministro en el ámbito de los microservicios. Por último, no hay que olvidar el escenario de ciberguerra a nivel global en el que nos encontramos inmersos, por lo que cabe suponer que uno de los principales objetivos de los 'hackers' serán las infraestructuras críticas. Aquí los ataques serán más sofisticados y complejos de detectar pero el impacto y la repercusión mediática será potencialmente mayor".

LOOKOUT

Daniel Villaseñor
Cybersecurity Sales engineer

"El *ransomware* continuará siendo una de las amenazas más notorias, evolucionando en dos aspectos: por un lado, se usará como medio de exfiltración directa de datos hacia servidores controlados por el atacante, lo que permitirá a lo cibercriminales obtener un rédito todavía mucho mayor que el conseguido hasta ahora. La segunda principal evolución del *ransomware* será su adaptación a los entornos *cloud* dado su creciente uso. Prevemos igualmente un incremento notable en las amenazas en dispositivos móviles, mucho más expuestos a ataques de ingeniería social dado su uso masivo tanto personal como profesional. La tercera principal amenaza, desde nuestro punto de vista, estará relacionada con la filtración de datos por parte de personal interno tanto intencionada como accidentalmente".

MALTEGO

Carlos Fragoso
DFIR / CTI Princicpal SME

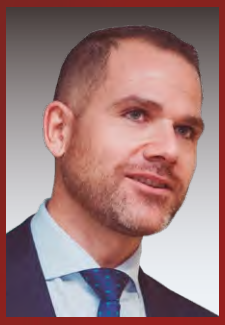
"La fuerte sacudida geopolítica del tablero mundial, junto con la explosiva proliferación tecnológica de los modelos aplicados de la IA, generan un nuevo escenario. Gobierno e industria cuentan con una gran oportunidad para luchar contra el cibercrimen, que intenta valerse de la coyuntura para innovar y evolucionar sus modelos de fraude como servicio, nuevas tipologías de extorsión por *ransomware* y la creatividad del lavado de dinero utilizando tácticas *cross-chain* en criptomoneda."

MDTEL TELECOMUNICACIONES

Francisco Cuesta
Director General Adjunto / CISO MD Secunit

"Veremos ataques de mayor impacto, la sombra de la recesión obliga a muchas compañías a optar por ajustar recursos, lo que tendrá consecuencias operativas en la ciberseguridad, con una automatización todavía pendiente de implantar en muchos casos. Técnicas de ingeniería social más avanzadas y el compromiso de la identidad de usuarios, a pesar del doble factor, serán ataques que continuarán durante este año. Deberemos estar atentos al compromiso de elementos básicos en la cadena de suministro BIOS, UEFI, dispositivos hardware embebidos y como no, en infraestructuras críticas, con una mayor necesidad de convergencia y dónde todavía no se dispone en muchos casos de medidas básicas".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023



MICROSOFT

Carlos Manchado
Responsable de Seguridad, Compliance e Identidad de Microsoft España

"La guerra híbrida, el desafiante escenario geopolítico y las crecientes ciberamenazas a infraestructuras críticas por parte de estados nación seguirán siendo las grandes protagonistas. Adicionalmente, el robo de identidades y las campañas –tanto de ingeniería social como de explotación de vulnerabilidades–, asistidos por sistemas y chatbots de IA, se volverán altamente virales y efectivos".

MNEMO

Roberto Peña
Director Corporativo Ciberseguridad e Inteligencia

"Hemos visto el inicio en la sofisticación del e-Crime, con capacidad de mutación del código y algoritmos de ML entrenados para la detección y evasión de defensas, generando adaptabilidad a ecosistemas cloud y *on-premise*. Este año llegará su madurez, con mercados *As a Service* para su capitalización y servicios avanzados de adaptación, siendo su objetivo las IICC y el sector financiero".

NETSKOPE

Miguel Ángel Martos
Country Manager para Iberia

"En 2023 continuarán usándose servicios legítimos de nube para distribuir malware. La amenaza del r*ansomware* como servicio (RaaS) y de los grupos de extorsión, seguirá intensificándose. Veremos aumentar la sofisticación en operaciones de *phishing* para eludir la autenticación multifactor (MFA). Y por último, esperamos un aumento significativo de ataques a la cadena de suministro de software, especialmente entre los de código abierto".

NETWRIX

Michael Paye
Vicepresidente de Investigación y Desarrollo

"El cibercrimen es ya un verdadero negocio y los actores de las amenazas siguen inventando nuevas tácticas y técnicas de ataque. A los atacantes les interesa hacer más eficiente su 'negocio': prefieren infiltrarse en un proveedor de seguridad y utilizarlo como punto de entrada a los numerosos socios y clientes. Prevemos que los ataques sobre las cadenas de suministros se intensificarán en 2023. En general, las organizaciones se apoyan en sus socios de seguridad de confianza, como socios de canal, integradores de sistemas y proveedores de servicios gestionados; y los atacantes se pueden aprovechar de ello. Para hacer frente a esta amenaza, las organizaciones deben reevaluar sus riesgos periódicamente y tener en cuenta las vulnerabilidades del software o firmware de terceros".

NETWITNESS

Ben Smith
Field CTO

"Cuatro palabras: Crimen como Servicio (CaaS). Reduce la barrera de entrada tanto para los delincuentes como para los gobiernos, donde la falta de experiencia técnica se puede subsanar fácilmente con un pago en efectivo. Una forma de mantenerse al día con esta carrera armamentista es subcontratar estos servicios a un proveedor de detección y respuesta gestionada (MDR), donde los beneficios de visibilidad que ofrece el XDR se combinan con la experiencia humana calificada para ayudarle a luchar en estas batallas de modo más eficaz. No se olvide: el cibercrimen es un negocio y funciona como tal. Y como todas las empresas sanas, los proveedores de CaaS se actualizan constantemente para hacer frente a los nuevos obstáculos erigidos por quienes intentan proteger sus organizaciones y los datos que contienen".

NOVARED

José Miguel Lavín
Director Comercial

"El *ransomware* y el *phishing* serán los principales vectores de ciberataque en 2023 en el mundo. Será necesario *tokenizar* la información para que lo robado carezca de valor en las manos del ciberdelincuente. Los ataques estarán mejor diseñados y dirigidos a grupos específicos, imitando mejor a las empresas para conseguir capturar presas. También será fundamental prestar atención a los componentes o programas de otras compañías, ya que pudieran verse afectadas debido a las cadenas de suministro del software de sus proveedores. Se seguirá utilizando la IA para crear, cambiar o falsificar archivos de audio y vídeo (*Deepfake*…). Los más de 60 mil millones de dispositivos IoT en el mundo que están conectados a Internet, podrían estar bajo ataque para alterar su funcionamiento, robar datos, generar ataques DDoS o incluso espiar a los dueños mediante las cámaras instaladas.

NOZOMI NETWORKS

Adriel Regueira
Regional Sales Engineer

"Seguiremos viendo *ransomware* (en auge) y amenazas de acceso a entornos de infraestructuras críticas con contraseñas y cifrados débiles, seguidas por ataques de fuerza bruta e intentos DDoS. Las herra-

mientas de acceso remoto (RAT) continuarán en la lista de programas maliciosos dirigidos a OT y los programas maliciosos DDoS a los dispositivos IoT con vulnerabilidades conocidas críticas. Desde Nozomi Networks, creemos firmemente que la detección, la transformación digital, la fiabilidad operativa, la interoperabilidad, la gobernanza y las normas serán claves y seguirán impulsando la demanda de la ciberseguridad en entornos OT e IoT. No hay dos ataques a los sistemas OT/ICS iguales, lo que dificulta la respuesta automatizada y la corrección sin un *partner* de confianza".

NTT DATA
Miguel Ángel Thomas
Head of Cybersecurity

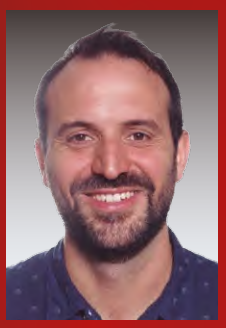
"En 2023 se podrá observar una proliferación en los ataques dirigidos a través del compromiso y suplantación de identidad de sus usuarios, mediante campañas dirigidas como *vishing* y *deepfakes* que harán uso de las técnicas más efectivas logradas mediante IA, tanto por canales profesionales como personales, muy orientados a vulnerar la cadena de suministros de grandes organizaciones".

NUNSYS
Rafael Vidal
Director de Seguridad y Gobierno TIC

"A nivel macro, esperamos un recrudecimiento de ataques de espionaje entre países y grupos de interés, emulando los tiempos de la guerra fría, con nuevas versiones de Pegasus, intervención de cuentas de correo, etc. para intervenir procesos democráticos, elecciones, etc. A nivel micro, la profesionalización de los ciberdelincuentes llevará a ataques a infraestructuras críticas: Hospitales, Puertos, Centrales de energía (gas, electricidad, energías limpias…) se verán amenazadas y requerirán CyberSOCs cada ver más verticales, que entiendan el negocio y puedan detectar y actuar con mayor eficacia".

OKTA
Felipe San Román
Ingeniero preventa

"Los intentos de registros de usuarios fraudulentos continuarán incrementándose en sectores como las finanzas y servicios públicos en general. Otra amenaza creciente es la reutilización de credenciales de cuentas robadas. Hoy mismo, en algunos sectores como el comercio minorista, representan la mayoría de los intentos de autenticación. También, más orientado a los empleados, la fatiga MFA."



ONE eSECURITY
Toño Díaz
Director Global de Respuesta

"El contexto geopoíitico, el suministro eléctrico y la escasez de semiconductores marcarán la tendencia de 2023. La cadena de suministro se convertirá en un objetivo más atractivo para campañas de *ransomware* dirigidas, aunque el número total de ataques de este tipo puede verse reducido. La extorsión y el espionaje alcanzarán un mayor grado de sofisticación. Irrumpirán nuevos actores no patrocinados por estados".

ONE IDENTITY
Daniel Gaspar
Team leader for Iberia

"Ciberataques basados en la identidad. Ciberdelincuentes con acceso no autorizado a redes propietarias a través de estrategias sofisticadas y múltiples para robar datos confidenciales e información de cuentas. Estas estrategias de *hacking* habituales (*malware*, *phishing*, *ransomware*, ingeniería social, etc.) no van a cambiar como tal durante el 2023, y en todo caso evolucionarán para ser menos detectables y más eficientes para los hackers delincuentes. Todo esto significa que el perímetro tradicional ya no es suficiente para proteger las organizaciones. No se puede proteger todo. Seguridad basada en la identidad, las organizaciones deben cambiar su enfoque de tratar de proteger todo a asumir que una infracción es inevitable. Minimizar de manera efectiva el radio de exposición".

ONESEQ BY ALHAMBRA
José María Ochoa
Cybersecurity Area Manager

"En la fiesta del cibercrimen para 2023 creemos que se incrementarán los impactos en administraciones públicas perimetrales (locales) con el fin perseguido de paralizar los servicios en los mismos y generar más sensación de vulnerabilidad, sin ser con ello muy complejos y especializados. Creemos que los impactos que se produjeron durante 2022 en estos contextos, han señalado dicha cadena de entrada más debilitada que otras y por ello sí esperamos un incremento en ese plano"

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

ORACLE

Marcos Alvarado
EMEA Cloud Security Architect

"La capacidad de estados maliciosos de usar plataformas sociales para extender campañas de desinformación es cada vez más sofisticada y precede a otro tipo de ataques, siendo el sector público español un objetivo importante, impactando la continuidad del servicio. La tendencia continuará en el 2023 y la creciente explotación de vulnerabilidades críticas de día cero, motivada por la necesidad de encontrar nuevas vías de entrada en entornos de la nube seguros".

ORANGE

José Ramón Monleón
Manager Seguridad Información Corporativa

"En 2023 el *ransomware* continuará siendo el principal problema para las organizaciones, si bien la cuestión que habrá que resolver es cómo se introducen en las mismas. Cubrir los vectores de ataque evitará tanto su entrada como otras amenazas o consecuencias. Para las empresas con un nivel de seguridad razonable, el foco estará en la cadena de suministro, con el objetivo de alcanzar el mismo nivel de seguridad en los servicios que ofrecen terceros. Por otra parte, seguirán apareciendo vulnerabilidades en pequeños módulos de software que, inexplicablemente, utilizan la mayoría de las aplicaciones y que desarrolló, desinteresadamente, un programador de Wisconsin. También será el año de la implantación de múltiples normas que supondrán un reto y que esperemos no quiten el foco de lo que realmente ayude a mejorar la ciberseguridad".

PALO ALTO NETWORKS

Marc Sarrias
Director General para España y Portugal

"Asistiremos a un aumento de la actividad coordinada de los entornos cibernético y físico contra las infraestructuras críticas. Al mismo tiempo, en muchos sectores, incluido el sanitario, la seguridad física de los usuarios frente a ataques coordinados que abusan de los sistemas IoT u OT será una preocupación creciente. Veremos un incremento en los ataques *ransomware* dirigidos aprovechando la IA para crear nuevos ataques ad hoc a la vez que es posible que asistamos a los primeros ataques contra los propios sistemas de IA mediante el envenenamiento de los datos que usan con el objetivo de falsear los resultados. Actualmente, al hablar de ciberseguridad, los 3 ámbitos donde se espera una mayor inversión siguen siendo la seguridad de los datos, en la nube y del IoT. La implementación de estrategias *Zero Trust*, la adopción de SASE, la consolidación de múltiples productos en plataformas y la automatización para la mejora de las operaciones, dada la falta creciente de profesionales cualificados para cubrir la demanda, serán clave en 2023".

PENTERA

Ramón Lucini
Regional Sales Manager Iberia

"Ante la situación mundial que se vive, cada vez se esperan ataques más sofisticados dirigidos a impactar no solo a las empresas, con fines económicos, sino a organismos públicos e infraestructuras críticas. Muchos de estos ataques tendrán el origen en la gran cantidad de información que está expuesta en internet, tanto de forma conocida (Webs, servicios, etc) como en la que ha sido ya exfiltrada y circula por la Deep web".

PRIM'X

Capucine Bardet
Gerente Comercial España

"En Prim'X vemos que el aumento en el uso de datos y su almacenamiento en la nube representan un serio riesgo si no están responsablemente controlados. Otro asunto es la soberanía en cuanto al uso no autorizado de los datos, por parte de un tercero, sea un país, atacante o competidor.
Si bien los proveedores *cloud* tienen propuestas eficientes, se mantiene la necesidad de protección que recae en manos de fabricantes expertos, lo que potencia ambos servicios. Conocemos casos de datos alojados en la nube sin suficiente resguardo ni segmentación, que generaron graves daños a los afectados y a los responsables. Por eso, Prim'X considera que el cifrado es un gran aliado para garantizar la confidencialidad de los datos, independiente de su ubicación y uso".

PROOFPOINT

Fernando Anaya
Country Manager para Iberia

"En 2023, el *ransomware* se desplegará agresivamente con doble o triple extorsión y la cadena de suministro será vector de ataque crítico. Los atacantes no dejarán de explotar las vulnerabilidades técnicas y humanas, eludiendo el MFA e innovando con deepfakes o kits de hackeo de la dark web. De fondo, las turbulencias en el mundo agravarán el riesgo sistémico y las exigencias de CISOs".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

PwC

Gonzalo Gómez-Abad
Director en el área de Business Security Solutions

"En 2023 se espera un aumento de la actividad de cibercriminales debido al contexto socioeconómico en el que todavía seguimos. Ataques a servicios *cloud* y el *ransomware* serán los ciberincidentes más frecuentes. La modelización por parte de las organizaciones de ciberejercicios sistemáticos en base a ataques reales en sus infraestructuras permitirá la mejora de sus capacidades de respuesta y de sus protocolos de actuación."

QUALYS

Sergio Pedroche
Country Manager España y Portugal

"Las amenazas seguirán la tendencia del año anterior, sin embargo, prácticas que deberían estar erradicadas como el uso de contraseñas inseguras, malas configuraciones y la incorrecta gestión de vulnerabilidades seguirán estando muy presentes. Conocer nuestro nivel de riesgo será fundamental para tomar las medidas adecuadas ya que nuestra superficie de ataque cada vez será más amplia."

RAVENLOOP

Daniel Vidal
CEO

"2023 se perfila como un año de cambios disruptivos: Los avances en el desarrollo de inteligencias artificiales orientadas al desarrollo y la resolución de problemas abstractos plantean la posibilidad de que los atacantes multipliquen sus capacidades ofensivas de forma exponencial gracias a su uso, unida a la sombra de la implantación del 5G y el incremento de la superficie de exposición."

REALSEC BY UTIMACO

Pablo Juan Mejía
Director General

"2023 se perfila para ataques más sofisticados hacia infraestructuras críticas donde la Directiva NIS2 intenta cubrir algunos de los huecos de seguridad existentes.
Con el incremento de dispositivos conectados al IoT, seremos testigos de nuevos ataques y robo de información, incluyendo la pérdida de privacidad para los usuarios, promovido por la debilidad en estándares de seguridad y aumento de APIs. Algo nuevo serán los hackeos a drones con diferentes propósitos maliciosos. En cuanto a industria aérea y espacial, se esperan ataques más sofisticados hacia su infraestructura en tierra e incluso dirigida a los propios aviones o satélites. El concepto de Agilidad Criptográfica Postcuántica formará parte de la estrategia de seguridad 2023 en muchas organizaciones".

RECORDED FUTURE

Pablo Valenzuela
Senior Sales Engineer

"En 2023 se incrementarán los métodos y automatizaciones de los ataques, sobre todo en tres áreas: Proliferación de los *info stealers* y sus industrializaciones para 'bypasear' más fácilmente los sistemas MFA, el incremento del uso y sencillez de plataformas *phishing-as-a-service* y la confirmación de la tendencia en ataques a las dependencias (tanto de software como de empresas proveedoras)"

ROCKWELL AUTOMATION

César Delgado
Business Development Lead Cybersecurity

"Crece el apetito por los Cyber Phisical Systems (CPS) y el presupuesto de los gobiernos a los "ciberejércitos" (defensivos y ofensivos). El *ransomware* azotará a las organizaciones menos concienciadas. Veremos un auge del modelo de triple extorsión (rescate, robo, filtración) para maximizar su monetización, usando la cadena de suministro y el robo de credenciales como principales vectores".

REDTRUST

Daniel Rodríguez
Director General

"Las nuevas amenazas de 2023, al margen de las clásicas que vienen sucediendo en los anteriores años, van a estar centradas en la verificación y protección de la identidad. Estamos viendo la rápida evolución de los sistemas de Inteligencia Artificial, tanto a la hora de generar textos complejos como imágenes creíbles que pueden servir para complementar otro tipo de ataques. Además, la propia Inteligencia Artificial se está utilizando para automatizar ataques y desplegar malware de manera más eficiente. Veremos también una rápida evolución en la combinación de la computación cuántica con la computación clásica para acelerar ataques contra sistemas PKI. Por eso, se vuelve crucial invertir en fortificar la identidad digital tanto de personas, como elementos IoT y todo tipo de dispositivos".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

RISKRECON – MASTERCARD

Vicente de la Morena
Country Leader for Spain and Portugal

"La dramática degradación de las relaciones globales entre los países ha creado un aumento masivo de la ciberdelincuencia y seguirá siendo el principal impulsor de su aumento en 2023 y en los años y décadas siguientes. Específicamente, los gobiernos aliados de Corea del Norte y Rusia patrocinan agresivamente y permiten ataques cibernéticos dirigidos contra países occidentales".

SAILPOINT

Jorge Sendra
Responsable de SailPoint para Iberia

"Los ciberataques y amenazas seguirán creciendo y volviéndose más críticos. Por ello la inversión en seguridad, y particularmente en la identidad digital, seguirá aumentando, aunque los presupuestos tiendan a ajustarse. Esto se verá especialmente reforzado por el hecho de que los CXOs (especialmente los CIOs y CISOs) ahora son más conscientes de lo crítico que es asegurar sus empresas a través de la lente de la identidad, y las consecuencias de no hacerlo son cada vez más claras".

S2 GRUPO

José Miguel Rosell
Socio Director

"A la vista de los acontecimientos acaecidos en 2022 debemos esperar un recrudecimiento de las operaciones de grupos APT contra intereses estratégicos de diferentes países, incluyendo ataques contra infraestructuras críticas que pueden impactar directamente en la sociedad. Seguiremos asistiendo a nuevas variaciones de las TTP de grupos de cibercrimen relacionados con ataques de *ransomware* y asistiendo al crecimiento de operaciones HOR (*ransom* operado). Las pymes son ya un claro objetivo creciente para grupos de cibercrimen, y seguirán siéndolo durante 2023, no solo por ellas mismas, sino como parte de la cadena de suministro de grandes compañías, pudiendo incluso llegar a provocar una sensación colectiva de inestabilidad. Adicionalmente la IA seguirá siendo pieza clave en la ciberseguridad, apoyando a ámbitos como la gestión de incidentes, las capacidades ofensivas o la monitorización de fuentes abiertas."

S21SEC

Igor Unanue
CTO

"Las amenazas que vienen en este 2023 serán derivadas del entorno geopolítico y las bandas organizadas, que cada vez están más preparadas para realizar ataques con beneficio económico. Teniendo en cuenta que el ransomware, junto con la exfiltración de datos robados, están generando rédito económico y que las organizaciones cada vez se protegen mejor, los ataques avanzados serán contra los usuarios".

SECURE&IT

Francisco Valencia
Director General

"Los ataques que más preocupan siguen siendo los asociados al ransomware y, sobre todo, las nuevas evoluciones, que no solamente copian y cifran la información, sino que la utilizan para publicarla en la *darkweb* y hacer chantajes entorno a la propiedad de esos datos.
En cuanto a la complejidad de ataques, debido a su desprotección, seguirán evolucionando aquellos dirigidos al mundo OT e IoT. Estos ataques van a combinar distintas técnicas: inteligencia artificial, ataques informáticos, ingeniería social, etc. El objetivo de los ciberdelincuentes es conseguir ataques cada vez más dirigidos, sofisticados y virulentos. Por ello, las empresas van a tener que estar muy preparadas en materia de ciberseguridad para protegerse ante estos ataques".

SECURÍZAME

Lorenzo Martínez
CTO

"Mientras las empresas sigan sin pensar que por un incidente de seguridad pueden perder parcial o totalmente su capital, seguiremos viendo lo mismo que hasta ahora: *Ransomware* (del de siempre y del "As a Service"), Timos al CEO, manipulación de facturas en los buzones de correo electrónico, *phishing / smishing / vishing* para tener acceso a credenciales, etc., seguirán siendo los platos típicos del menú porque los ciberdelincuentes tienen más claro que las empresas eso de que "Si funciona, no lo toques". Aquellas empresas que no tengan una copia de seguridad "a prueba de *ransomware*" y un nivel de concienciación a "prueba de engaños" en todas personas que integran sus equipos humanos, serán potenciales clientes nuestros en 2023 si se ven inmersos en un incidente de seguridad."

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

SERESCO
Valentín Cabello
Director Comercial Área de Ciberseguridad

"A medida que mejoran las técnicas *DeepFake* de IA para imitar de manera más convincente la comunicación humana, el engaño producido tanto a las personas, como a los algoritmos, aumentará significativamente. El fraude de identidad evolucionará provocando, incluso, que se genere una crisis que vaya más allá de la propia organización, pudiendo tensionar la situación geopolítica, económica o laboral. En un mundo donde todo se mueve a una velocidad de vértigo, sin tiempo para contrastar, siendo las RRSS la plataforma ideal para catapultar los engaños generados a través de *DeepFake*. Paradójicamente, la propia IA será necesaria para contrarrestar estos engaños en tiempo real formando parte de una estrategia más amplia y sofisticada cuya finalidad sea bloquear este tipo de ciberataques antes de producirse".

SENTINELONE
Raúl Benito
Regional Sales Manager Iberia

"La ciberseguridad solo funciona cuando lo hace de 'manera simple'. Por ello, en 2023 con menos presupuesto en seguridad, los productos impulsados por la eficiencia serán los seleccionados. También habrá más organizaciones atacadas, más infraestructura crítica afectada y la economía del cibercrimen seguirá prosperando. El *phishing* continuará siendo un factor principal en el compromiso de las identidades, al igual que la ingeniería social. Asimismo, se esperan más ataques por parte de actores más jóvenes que se niegan a limitar su pensamiento a la forma standard de hacer negocios. A ello se sumará la reasignación de las prioridades de inteligencia para identificar antes y desbaratar las operaciones a largo plazo contra las naciones y las infraestructuras críticas. Por último, también se espera ver a los atacantes apuntar a macOS, con más éxito, y dedicar más esfuerzo a encontrar ventanas de oportunidad".

SIEMENS
Karen Gaines
Global Business Executive Dedicated to Securing Enterprises

"Durante este año 2023 veremos la formalización de la gestión de riesgos con respecto a la cadena de valor. Es más evidente que nunca la vulnerabilidad de las empresas debido a la falta de transparencia en la cadena de suministro y la necesidad de implementar un rígido programa de cumplimiento para proveedores con el objetivo de proteger la reputación empresarial y evitar efectos colaterales de un ciberataque o ser víctima de una vulnerabilidad crítica".

SMART HC
Ignacio Arrese
CEO

"Para afrontar la ciberseguridad en este 2023, debemos tener en cuenta varios aspectos que son diferenciales en este ámbito. El primero es que se evidencia una mayor profesionalización de la ciberdelincuencia, incluso, en el cómo se está sufriendo a causa del conflicto armado en Europa, llegando a niveles de ciberataques entre estados.
El siguiente indicador es el mayor nivel de especialización de los atacantes, que tras la adquisición de experiencia les permite desechar las técnicas y vectores de ataque que no les han reportado el suficiente nivel de éxito en sus ataques, centrándose en los que les son más fructíferos. Esta conlleva la utilización de tecnologías que, aun siendo creadas para la defensa, son extraordinariamente productivas en los ataques, ejemplos claros son la utilización de la Inteligencia para mayor conocimiento de sus objetivos, y de la inteligencia artificial para conseguir mayor efectividad en sus ataques.Además, no debemos dejar de lado la automatización de sus ataques valiéndose de las nuevas técnicas utilizadas, y que precisamente hace que prolifere un mercado "Ad-hoc", para el hampa cibercriminal, que propicia un mercado de servicios dirigidos para un uso delincuencial como puede ser el "Ransom as a Service (RaaS)".

SOLARWINDS
Alberto Arbizu
Territory Director

"Cada día hay más riesgos porque la red está en todas partes y el panorama de las amenazas es mucho más heterogéneo y diverso. Dado que muchas cosas dependen de esta red global, cualquier infracción o incidente menor ya no es una molestia o un simple problema, sino que puede ser catastrófico. Los equipos de seguridad ya no pueden permitirse trabajar en silos; todos los equipos de la organización deben desempeñar un papel activo dentro de una comunidad/departamentos para minimizar las amenazas, que para 2023 prevemos estas tipologías: 1) Aumento de los intentos de ingeniería social y/o *phishing* de forma inofensiva con correos-e; 2) El *ransomware* seguirá existiendo, pero su impacto puede prevenirse fácilmente; 3) Conexiones de Wi-Fi inseguras y que terminan con todos los dispositivos IoT que usamos infectados; 4) Herramientas y servicios gratuitos, ¿alguna vez los usuarios se preguntan por qué son gratuitos?, 5) Amenazas internas malintencionadas".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

SONICWALL

Sergio Martínez
Iberia Country Manager

"En 2023 veremos la explosión de las amenazas encriptadas, las que utilizan los canales cifrados de comunicaciones para alcanzar y comprometer el *endpoint* ante la pasividad de todos los elementos de protección que no pueden analizar ese tráfico por diferentes razones (normalmente, por la falta autorización de certificados digitales). Además, el despliegue de ciertos tipos de protocolos (DNS cifrado, QUICK-UDP, etc.) que potencian la privacidad, pero imposibilitan la ciberseguridad, aumentarán la inseguridad y todo el peso de la defensa se trasladará al endpoint. Por ello, la defensa por capas, la visibilidad y control de la infraestructura, el uso de la IA y los antivirus de nueva generación serán más necesarios que nunca".

SOPHOS

Ricardo Maté
Regional Vicepresident South EMEA & Emerging

"La industria de la ciberdelincuencia como servicio ha alcanzado un nuevo nivel de comercialización y mercantilización, eliminando muchas barreras de entrada para los interesados en la ciberdelincuencia y poniendo las tácticas de amenazas avanzadas en manos de casi cualquier delincuente.
Cada paso de la cadena de ataque –desde la infección inicial hasta la evasión de la detección– está disponible "As-a-Service". Es posible que este cambio vaya en aumento, incluso hasta el punto de que los actores del *ransomware* no sólo adopten un enfoque cada vez más corporativo, sino que algunos empiecen a legitimarse y diversificarse.
Por último, como ya ha ocurrido en otras ocasiones de contexto bélico, gobiernos, organismos públicos y grandes compañías de suministros aparecerán en el punto de mira de los atacantes y la habilidad de las nuevas variantes de *ransomware* de pasar bajo el radar harán imprescindibles los servicios de vigilancia especializada MDR".

SOTHIS

Miguel Monedero
Director de Seguridad de la Información

"Todo parece apuntar a que en 2023 continuaremos con el *ransomware* como la amenaza de mayor impacto, con nuevos actores, nuevas variantes e innovadoras tácticas, técnicas y procedimientos para ejecutarlo. Además, combinado con el robo de información y su uso para la extorsión hacia la víctima. Seguiremos encontrando el uso de vectores de ataque tradicionales como *phishing*, *smishing* o explotación de vulnerabilidades *Zero Day*, de forma unitaria o combinada. Esperamos aumento de ataques vulnerando los sistemas de multifactor y el aprovechamiento del aumento de la exposición digital de las organizaciones, al disponer de un mayor número de dispositivos IT/IoT/OT conectados a la red"

STORMSHIELD

Borja Pérez
Country Manager para Iberia

"Esperamos ver un crecimiento en los ataques de *ransom* y *scam* masivos, con un objetivo en una población de usuarios cada vez más digitalizada, pero con escasos o nulos conocimientos de ciberseguridad. Veremos más ataques al espacio Web3 que, si bien han pasado más desapercibidos para el público general, se estima que hayan costado varios millardos de euros en 2022. Sólo el de Ronin supuso en su momento 615 millones de dólares. En 2023 también empezaremos a ver despliegues, esta vez sí, importantes de 5G. Las capacidades tecnológicas para atacar estas redes tienen que ser altas, pero la oportunidad de negocio para los criminales también lo será. Por último, cabría esperar nuevos ataques a fabricantes y desarrolladores de soluciones de ciberseguridad. Por eso debemos ser especialmente cuidadosos en su desarrollo, poniendo énfasis en la autoprotección y en la separación de microservicios para evitar el impacto de unos en otros. Como señal de la posibilidad de este tipo de ataques podemos hablar de los producidos a librerías de Machine Learning utilizadas por desarrolladores como Pytorch".

TANIUM

Jorge Pascua
Technical Account Management

"La principal amenaza serán los ataques a librerías de código abierto, utilizadas como punto de acceso debido a la incapacidad de las organizaciones para identificar y remediar sus vulnerabilidades. Éstas necesitarán visibilidad a escala y capacidad de inventariar todo, sean aplicaciones de código abierto o terceros, debiéndose proteger con recursos limitados con más frecuencia y rapidez".

TARLOGIC

Alejandro González
Cybersecurity Executive Director

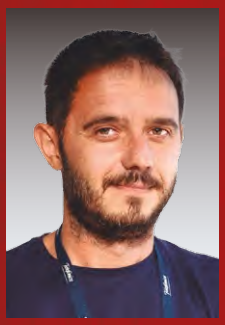
"Con el acceso a inteligencia artificial tipo ChatGPT, esperamos cierta innovación en las técnicas de creación de malware y nuevas técnicas en ciberataques. Por otro lado, continuaremos observando una fuerte tendencia en la generación de ciberataques dirigidos a

la cadena de suministro y otros destinados a generar alto impacto, como lo sucedido en 2022 con vulnerabilidades de tipo log4j".

TD-SYNNEX

Nicanor Pulido
Technical Presales Consultant Security

"Para 2023, en cuanto a ciberseguridad, estos días se habla mucho de los grandes temas: amenazas derivadas de conflictos bélicos activos (invasión de Ucrania y la posibilidad de que se extienda a otras regiones) o políticos (tensión entre Marruecos y Argelia, China y Taiwan, etc.), ataques a infraestructuras críticas de los estados desde estados rivales o pérdidas de servicio y datos personales de clientes en las grandes corporaciones. Sin embargo, lo que nadie espera es que nuestra propia compañía pueda ser objeto de un ataque de características similares a los anteriores, aunque a menor escala. Por ello es necesario mantener el nivel de alerta, revisando y actualizando las políticas de seguridad con los procedimientos y herramientas imprescindibles para ello".



TELEFÓNICA TECH

Sergio de los Santos
Director del área de Innovación y Laboratorio de Ciberseguridad y Cloud

"El FBI confirmaba hace poco la existencia de organizaciones que han ganado hasta 100 millones de dólares en año y medio. Por tanto, en 2023 *el ransomware* enfocado a grandes compañías seguirá arrasando porque el modelo económico está lejos de haberse agotado. Es posible que veamos los primeros usos (para complementar o dar credibilidad a ataques) de las numerosas inteligencias artificiales".

TEHTRIS

Pedro Morcillo
Country Manager Spain

"Vamos a experimentar un aumento de los ciberataques realizados con tecnología basada en IA, que van a sobrepasar los métodos clásicos de protección, causando un grave daño a compañías y empresas que no actualicen su método de protección. Esto deriva en dos consecuencias fundamentalmente: 1ª) No se van a basar en atacar una sola tecnología de Ciberseguridad, sino que va a atacar a todas las que encuentre en su camino hacia su objetivo, y 2ª) El modo de ataque, el vector que utiliza y la manera de comportarse ya no está ideada por un ser humano, con ideas y pensamientos humanos, sino que la IA va a idear nuevos y más complejos métodos de ataque".

TENABLE

Amit Yoran
CEO

"Desde Tenable prevemos: *Ataques de extorsión*: más allá del *ransomware*, la extorsión será aún más disruptiva para las empresas en 2023; *Seguridad OT/IoT*: Las compañías priorizarán la protección de los sistemas críticos industriales; *Brechas en SaaS*: con un modelo de responsabilidad compartida y la limitada supervisión, la gran superficie de ataque es propicia para los atacantes; *Objetivo Cloud MSP*: hay numerosas ventajas de adoptar la nube y subcontratar servicios a un MSP, pero las posibilidades de exposición crecen y serán aprovechadas".

THALES

Alfonso Martínez
Country manager España & Portugal

"La metafrontera de la seguridad de un metauniverso. O sea, anticiparse a las ciberamenazas de un espacio futuro que aún no existe, y que tal vez nunca llegue a existir, es todo un reto. Sin embargo, gracias a la investigación de los fundamentos de la tecnología y al examen del panorama actual de la ciberdelincuencia, podemos imaginar una serie de peligros significativos existentes en el metaverso. Debería aplicarse el mismo nivel de seguridad y escrutinio a la realidad virtual, aumentada y mixta que a las plataformas tradicionales, ya que estas tecnologías plantean graves riesgos de seguridad, como fraudes financieros, ataques ciberfísicos y peligros para la privacidad de los usuarios".

THOUSAND GUARDS

Juanjo Martínez
CISO Advisor

"Se esperan más ataques a los recursos en la nube. Veremos más robos masivos de datos y más multas. Los principales vectores de ataque en la nube serán la explotación de vulnerabilidades, malas configuraciones, activos huérfanos y el robo de credenciales por diversas técnicas, incluyendo ingeniería social y falsos portales de autenticación. Los ataques serán cada vez más personalizados".

TRANSMIT SECURITY

Ángel Nogueras
Solutions Engineer

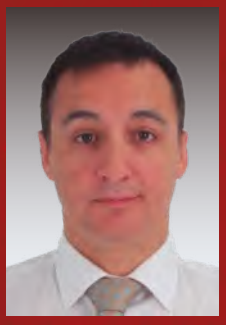
"En 2023, veremos un aumento en la complejidad y el impacto de las amenazas y ciberataques relacionados con la identidad digital. El *phishing* y el robo de datos personales seguirán siendo de enorme preocupación

junto con un esperado aumento en el uso de técnicas de ingeniería social para acceder a cuentas y sistemas protegidos. Contar con las soluciones de protección adecuadas será crítico."

TRANXFER

Alberto Monforte
CEO

"Hay nuevas amenazas en el horizonte en ámbitos como la AI, el Metaverso, o las cripto, pero no hay que descuidar las amenazas que nos vienen acompañando año tras año. La baja concienciación en ciberseguridad y el error humano, causan el 70% de brechas de seguridad, sobre todo con el teletrabajo. La formación de los empleados y las herramientas adecuadas son clave para la ciberseguridad".



TRELLIX

David Baldomero
Senior Systems Engineer

"Las últimas amenazas de ciberseguridad inciden en el auge de los ataques cibernéticos geopolíticos y campañas de desinformación. Dadas las actuales tensiones mundiales, ya estamos viendo un resurgimiento del hacktivismo en 2023, un aumento del uso de herramientas cibernéticas por parte de estos grupos para expresar su ira y causar trastornos. La guerra cibernética evolucionara con ciberamenazas a la infraestructura crítica, con más dispositivos IoT secuestrados. La superficie de ataque será mayor, como satélites comprometidos y otros activos espaciales y se harán más públicos en 2023. Prevemos un aumento significativo de los ataques de suplantación de identidad inversa y más vulnerabilidades de escalado de privilegios de dominio, buscando hacerse con el control total de la red".

TREND MICRO

Raúl Guillén
Strategic Alliances & Partnerships Manager

"Vemos dos grandes bloques de ataque, tanto la adopción de nube como la convergencia OT/ IT con el 5G y la IA como aceleradores, con una brecha importante de recursos y capacidades humanas, la tecnología *blockchain* está en el foco de los ciberdelincuentes y los señuelos de ingeniería social se actualizarán con la lacra de *ransomware* como objetivo en un modelo de múltiple extorsión".

T-SYSTEMS

Laura Hernández
Head of Security Delivery

"Si algo hemos observado en 2022 es que donde hay una debilidad, hay un camino. Esto no es solo una tendencia; las razones siguen siendo: productos vulnerables, disminuyendo el tiempo para que un día cero se convierta en un exploit, procesos de parcheo incompletos que no consideran toda la cadena de suministro dada la dificultad que supone en ocasiones el software open-source/custom sin un SBOM claro, actores de amenazas que se han vuelto colaborativos, con software malicioso y técnicas a su disposición como franquiciados RaaS que nos llevan a un punto en el que los atacantes ahora son independientes de la plataforma y la tecnología, y todo ello sumado a la situación geopolítica que ha hecho que cualquier organización o empresa de la UE sea objetivo indiscriminado de atacantes rusos. La situación no va a cambiar: los ataques serán más grandes, más ruidosos y más rápidos. Más organizaciones serán comprometidas, más infraestructura crítica se verá afectada y la economía del cibercrimen seguirá prosperando."

VARONIS

Julián Domínguez
Iberia Sales Team Leader

"En 2023 esperamos un aumento de la Inteligencia Artificial y el aprendizaje automático, que continuarán integrándose en los sistemas de ciberseguridad, lo que permitirá una detección y prevención más eficientes de las ciberamenazas. Al combinar una IA fuerte y precisa y el aprendizaje automático, veremos la próxima fase en el ciberespacio, es decir, en lugar de confiar en alertas basadas en umbrales, las organizaciones se moverán para aplicar un conjunto de herramientas de aprendizaje automático predictivo que indicaría: "Si el comportamiento de X continúa, el resultado podría parecerse al actor de la amenaza Y". Este cambio mejorará el tiempo de alerta de una empresa y reducirá el tiempo de respuesta. Además, el año pasado anticipamos ver más *ransomware* patrocinado por el estado y, lamentablemente, no esperamos que esto sea cosa del pasado".

VECTRA

Ricardo Hernández
Country Manager España y Portugal

"La Inteligencia Artificial aplicada a los ataques dejará obsoletos muchos tipos de defensas e incrementará las formas de penetrar y explotar las infraestructuras de las víctimas a escala. La aplicación de la Inteligencia Artificial en la detección y respuesta para contrarrestar estos nuevos ataques será fundamental para proveernos de capacidades suficientes en el lado de los defensores".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

VEEAM SOFTWARE

Santiago Campuzano
Country Manager

"La implementación de soluciones en la nube va a hacer que el riesgo de los ataques a los hiperescalares aumente, siendo el objetivo dentro de una guerra cibernética donde se busca un daño más global. Los datos de industrias asociadas a servicios básicos estarán en claro peligro, haciendo que Modern Data Protection, como última línea de defensa, se integre más en el ámbito de la seguridad"

VERIDAS

Gorka Sánchez
Solutions & Deployment Director

"Seguirán creciendo los ataques de tipo *ransomware*, ataques de *phishing*, *malware*, la exploración de vulnerabilidades en los sistemas, los ataques por denegación de servicio y los enfocados a la confidencialidad por fuerza bruta y a los servicios de autenticación".

VINTEGRIS

Victoria Hernández
Chief Information Security Officer & eiDAS Trust Services

"2023 ha llegado con la certeza de que las nuevas regulaciones y la gran inversión en ciberseguridad son piezas claves para que nuestras infraestructuras sean más robustas con el fin de combatir de forma más proactiva la defensa de nuestros servicios. Como en años anteriores, debemos profundizar en las labores de concienciación y formación en materia de ciberseguridad dado que los empleados y las redes domésticas serán unos de los principales vectores de ataque, poniendo especial atención en que la IA aporta técnicas muy sofisticadas para la suplantación de identidad o el Deepfake, y será muy complicado combatir este tipo de ataques que pueden desencadenar importantes brechas de seguridad con pérdida de datos, sanciones económicas y pérdida de confianza en las organizaciones".

VMWARE

Nacho Arrieta
Solutions Engineering Director para Iberia

"Veremos el uso de herramientas como ChatGPT (Inteligencia Artificial de propósito general) para crear *bots* y *phishings* extremadamente realistas que permitirán a los actores maliciosos ganar acceso a nuestros sistemas. También, se usarán estas herramientas para crear software (IA creando código) malicioso. Esto incrementará la frecuencia y el impacto de los incidentes de *ransomware*. Los planes de concienciación frente a amenazas cibernéticas deberán recoger está nueva realidad. También, los planes de contingencia, que se deberán apoyar en capacidades avanzadas y multi-cloud (terceras ubicaciones desconectadas, almacenamiento inmutable, análisis forénicos…) para mejorar la resiliencia de las organizaciones y empresas".

V-VALLEY

Alberto López
Director de División de Seguridad

"Los ataques de denegación de servicio estamos viendo que están afectando directamente a los negocios que concentran una parte importante de su venta en los canales digitales. La exposición y la dependencia que tienen estas empresas es un factor de riesgo importante. No solamente es mantener la disponibilidad de la plataforma, es la imagen digital de las empresas las que está en juego. Otro de las áreas que vemos más evolución es en los ataques persistentes basados en el robo de identidades, donde parte de gestión de la identidad, mediante la integración de soluciones de gestión de credenciales y soluciones ZTNA, serán las plataformas necesarias para proteger a las empresas. Por supuesto el ransomware seguirá presente y más telemetría será necesario para evitar movimientos laterales".

WALLIX

Guillaume Pillon
Sales Manager Iberia y Latinoamérica

"El rápido cambio tecnológico y los efectos de la actual situación geopolítica seguirán haciendo mella en la ciberseguridad de las empresas. También este año los sectores más afectados serán la industria, a causa de las vulnerabilidades asociadas a la cadena de suministro, y el sector público, cuyo principal desafío radicará en la gestión del presupuesto y del riesgo cibernético".

WATCHGUARD

Miguel Carrero
Vicepresidente, Security Service Providers & Strategic Accounts

"2023 verá un gran incremento de ataques con características especiales para evitar entornos de MFA. Veremos una combinación de técnicas de evasión del MFA, nuevas vías de ingeniería social que explotan la mayor adopción de MFA (por ejemplo, *Push bombing*) y variaciones de técnicas "*adversary-in-the-middle*" que tienen en cuenta los procesos de MFA para capturar *tokens* de sesiones de autenticación".

CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2023

WESTCON
Alberto Díez Hernández
Presales Engineer en España

"Estas amenazas estarán presentes en 2023: El *ransomware* dirigido, ataques de autenticación multifactorial, Zero Trust, Phishing, IA, IoT, Deepfake, vulnerabilidades en dispositivos móviles. Existen ciertas razones que contribuyen a que la ciberdelincuencia continúe siendo una amenaza como: la mayor conectividad, el mayor valor de los datos, la dificultad para detectar y prevenir ataques, y la mayor demanda".

WISE SECURITY GLOBAL
Domingo Cardona
CEO

"Los ataques de *ransomware* continuarán siendo la amenaza más relevante, así como los compromisos de jugadores de nube e infraestructuras IoT. La popularización de la IA aumentará esos ataques y se reducirán los tiempos de reacción de los SOC/CSIRT, así como su músculo para con este nuevo volumen. La capacitación en IA de todas las líneas de defensa será clave para seguir presentando batalla."

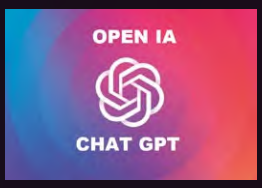
ZEROLYNX
Juan Antonio Calles
Chief Executive Officer

"El reciente lanzamiento de ChatGPT, el sistema de chat basado en el modelo GPT-3 desarrollado por OpenAI, la compañía de investigación californiana, revolucionará nuestro sector a medio plazo. Las primeras pruebas de concepto ya están en marcha, y en breve veremos herramientas generadas por esta IA que podrán sustituir a las tradicionales soluciones SAST. ¡Un avance sin precedentes!".

ZSCALER
Carlos Muñoz
Director de Ingeniería Preventa, España, Portugal e Italia

"Las amenazas continuarán ocultándose en el tráfico cifrado, impulsadas por modelos *as-a-service* que han visto cómo se reducían las trabas técnicas para hacerlo. El *malware* seguirá siendo la amenaza favorita y los ataques de *ransomware* continuarán su escalada. El modelo *Zero trust* y la IA van a ser cada vez más necesarios para hacer frente a este crecimiento y reducir el tiempo de reacción".

IA



CHAT GPT
(Preguntado por Revista SIC a 10 de enero de 2023)

"Es difícil predecir con certeza qué ciberamenazas específicas serán las más comunes en 2023, ya que el panorama de la ciberseguridad evoluciona y cambia constantemente. Sin embargo, algunos tipos de amenazas que probablemente seguirán siendo una preocupación importante en el futuro incluyen:

- **Amenazas persistentes avanzadas (APT):** estos son ataques altamente sofisticados y dirigidos que a menudo son lanzados por estados-nación u otros actores bien financiados y altamente motivados. Las APT generalmente implican un ataque de varias etapas que comienza con el reconocimiento inicial y avanza hasta la instalación de malware en los sistemas del objetivo.
- **Ataques de IoT:** a medida que la cantidad de dispositivos conectados continúa creciendo, es probable que los ataques dirigidos a estos dispositivos se vuelvan más frecuentes. Los dispositivos IoT suelen ser menos seguros que los dispositivos informáticos tradicionales, lo que los convierte en un objetivo atractivo para los ciberdelincuentes.
- **Seguridad en la nube:** a medida que más y más empresas migran a la nube, la infraestructura y los servicios basados en la nube se convertirán en un objetivo más atractivo para los atacantes. Esto incluye violaciones a los servicios en la nube, servidores en la nube mal configurados y violaciones de datos causadas por la falta de visibilidad y la mala gestión del acceso.
- **Ataques a la cadena de suministro:** los ataques a la cadena de suministro se dirigen a los diversos terceros y proveedores de los que depende una empresa, y pueden proporcionar a los atacantes un punto de apoyo en las redes y los datos de una organización.
- **Ataques basados en IA:** a medida que las tecnologías de IA y aprendizaje automático se vuelven más avanzadas y más ampliamente adoptadas, es probable que veamos un aumento correspondiente en los ataques que explotan estas tecnologías.

También es importante tener en cuenta que las amenazas cibernéticas suelen ser muy adaptables y pueden cambiar rápidamente sus métodos para aprovechar las nuevas vulnerabilidades y tendencias, por lo que es importante mantenerse alerta y mantenerse informado sobre las últimas amenazas de seguridad cibernética y las mejores prácticas para protegerse contra ellas".

CONGRESOS

8.8 CONFERENCE

Gabriel Bergel
Fundador

"Considerando la situación actual post pandemia común en todas las empresas y países, donde el trabajo remoto ha persistido y probablemente en la mayoría se mantenga para siempre, donde sin querer se mezcla el trabajo doméstico con el laboral, sumado a la propagación del Internet de las cosas (IoT) en todos los ámbitos de negocios y la sociedad, indican que los ciber ataques seguirán orientados a las personas (engaños) y los nuevos dispositivos inteligentes carentes de ciberseguridad. Como Forbes lo indica, habrá más ataques patrocinados por Estados, los que representan la cima de la asimetría entre el mundo que se dedica a proteger las organizaciones y los cibercriminales, ya que luchamos contra cibercriminales de elite, con presupuestos incalculables y con todo el tiempo del mundo".

BITUP ALICANTE

Josep Moreno (aka Jomoza)
Coorganizador

"Vivimos en la época del Cloud, del 'as a service', del teletrabajo y la retaría terminológica que nos acompaña desde hace años que ocultan que, en el fondo, se ha estandarizado la delegación de tecnologías e información. Este contexto dificulta no caer en los clásicos futuribles a la hora de hacer estimaciones de riesgos. Nuevos APT's que usan exploits 0day-0click con LPE's indetectables. Una ingeniería social se vale más que nunca de las inteligencias artificiales para generar deepfakes de cara, voz o comportamiento. Una explosión del uso IoT que está por llegar, en la que tanto las casas de los particulares e infraestructuras abrirán los vectores de ataque a absolutamente todo lo que nos rodea. Y, sin duda, llegarán riesgos, que desconocemos, para ponernos a prueba…".

C1B3RWALL

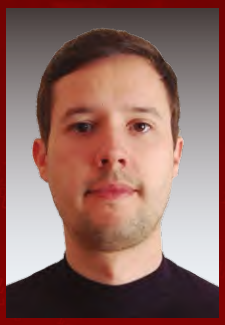
Casimiro Nevado
Inspector Jefe. Policía Nacional
Coordinador Proyecto @C1b3rWall

"2023 no será una excepción en la evolución ascendente de la estadística de cibercriminalidad en nuestro país ni en la tendencia a la mayor especialización e impacto de la actividad de los grupos criminales. Seguiremos sufriendo las ya conocidas modalidades delictivas como el *ransomware* en su modelo de doble extorsión y el nutrido grupo de ciberestafas, pero con nuevos modus operandi. Lo sencillo triunfa y las técnicas de ingeniería social seguirán siendo un filón muy rentable. Los grupos de cibercrimen presentarán estructuras y esquemas de funcionamiento más complejos y grises, con lo que se dificultará aún más la labor de investigación policial y será más necesario aún el reforzamiento de las estrategias de colaboración pública privada y el intercambio de inteligencia. Es evidente que el criminal buscará la vía de acceso más fácil y menos costosa por lo que los ataques a la cadena de suministro serán la mejor opción de explotación de las vulnerabilidades de las defensas más débiles que presenten los actores menos concienciados. Desgraciadamente, creo que, a la seguridad, fuera del ámbito profesional de la misma, se la sigue viendo como un inconveniente o una traba con la que convivir y no como una parte fundamental de la actividad. Mientras el cibercrimen siga siendo una actividad tan rentable, los delincuentes siempre estarán un paso por delante de los defensores. En mi opinión, la clave estará en conseguir romper las vías de financiación".

CRIPTORED CYBERSECURITY CONFERENCE

Alfonso Muñoz
Fundador

"La tendencia cibercriminal y de espionaje industrial será continuista aprovechándose de las tecnologías cada vez más complejas (y poco auditadas), la IA usada en ataques ofensivos y las carencias, no siempre confesables, de las organizaciones en los *basics* de la seguridad, incluida la inadecuada gestión de la manida cadena de suministro. 2023 puede ser una buena oportunidad para volver a los orígenes, robustecer las organizaciones con mecanismos de autorización y autenticación basados en confianza cero y apostar, de verdad, por la cripto-agilidad, protegiendo comunicaciones extremo a extremo y secretos en sentido amplio".



EUSKALHACK

Miguel Ángel Hernández
Fundador y Presidente

"El tormentoso panorama geopolítico internacional intensificará los ataques patrocinados por estados ante infraestructuras críticas, organizaciones estratégicas, y sector público. La IA y ML jugará un papel fundamental en la predicción de amenazas mediante grandes volúmenes de datos, y la automatización de la gestión del riesgo tendrá un mayor peso.

Los atacantes también utilizarán estas capacidades a fin de identificar sistemas vulnerables a gran escala, desarrollo de *malware*, y sofisticación en las técnicas de ingeniería social. La evidente tendencia a la nube entre las organizaciones las empujará a madurar su nivel de ciberseguridad ante vulnerabilidades y fuga de información. Finalmente, continuaremos viendo multitud de compromisos en la cadena de suministro".

H-0CON

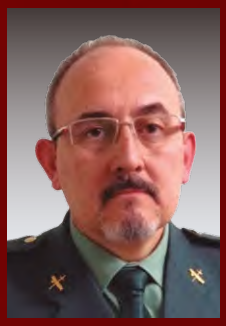
Vicente Motos
Fundador

"La ciberdelincuencia seguirá evolucionando y expandiéndose a la vez que lo hacen las tecnologías. La Web3, la constante proliferación de dispositivos inteligentes (IoT), una IA cada vez más práctica y alcanzable para todos, son sólo ejemplos de la creciente sofisticación de nuestra realidad digital que los ciberdelincuentes readaptan y aprovechan. Y para mí una de las mayores amenazas de 2023 está precisamente en esa expansión de ataques y la falta de especialistas para contenerlos. Tenemos que incentivar e incorporar más gente al sector, ofrecer a los estudiantes formación de calidad, asistencia a conferencias, que aprendan, contribuyan y colaboren en comunidad. En definitiva, que conviertan este trabajo en su pasión para protegerse y protegernos de lo que está por llegar...".

NAVAJA NEGRA

Rubén Ródenas
Cofundador

"A medida que la tecnología avanza y más empresas y organizaciones adoptan sistemas y dispositivos conectados a internet, se vuelven cada vez más vulnerables a los ataques cibernéticos. En 2023, se esperan amenazas y ataques cibernéticos de gran impacto y complejidad. Entre ellos estarán los de *ransomware*, con ataques dirigidos a empresas y organizaciones críticas, como hospitales y servicios públicos; de *phishing* y *spear phishing* cada vez más sofisticados y contra objetivos específicos, como empleados de alto nivel en empresas y organizaciones. También a dispositivos IoT que pueden utilizarlos para lanzar ataques contra redes y sistemas. No faltará el ciberespionaje, cada vez más sofisticado y dirigido contra empresas que manejan datos sensibles o secretos de estado. Por último, continuarán los ataques automatizados, cada vez más populares por la disponibilidad de herramientas y software fácil de usar, resultando difíciles de detectar y mitigar".



NATIONAL CYBERLEAGUE GC

Luis Fernando Hernández
Coronel de la Guardia Civil
Director Técnico

"Por su potencial alto impacto, hay que destacar aquellos ciberincidentes que persigan, a través de una disrupción activa, socavando los pilares sociales, económicos y políticos de las democracias occidentales; enmarcados en la peligrosa deriva de los conflictos geopolíticos entre bloques antagónicos. La privacidad seguirá quebrada mientras no se erradique la actividad, no reglada cuando no abiertamente ilegal, de los "corredores de datos" y el creciente mercadeo en la *Darknet*. Las estafas seguirán su crecimiento exponencial, castigando al sistema financiero, tejido productivo y a la ciudadanía. Tecnologías disruptivas como son la IA, el IoT, el Big Data, el Cloud Data, la hiperconectividad 5G/ 6G o la Computación Cuántica continuarán catalizando prosperidad, pero a la vez favoreciendo la cibercriminalidad. Sólo los esfuerzos en ciberseguridad rebajarán la probabilidad de que se materialicen tales amenazas".

SECADMIN SECURITY CONFERENCE

Adrián Ramírez
Organizador y CEO de Dolbuck

"Los ataques de *ransomware* junto con la estafa del CEO, en sus distintas modalidades, seguirán liderando los tipos de cibercrimen más utilizados en 2023. Si a eso le añadimos el uso de la Inteligencia Artificial como, por ejemplo, en la identificación de víctimas en redes sociales, y el procesamiento automatizado de datos robados y filtrados como usuarios y sus contraseñas, observaremos cómo aumentan exponencialmente los ciberataques. Además, estos ataques están siendo cada vez más difíciles de detectar y de mayor impacto para la resiliencia de las empresas. Por lo tanto, la peor amenaza que puede tener una organización es un CEO que no invierta en ciberseguridad".

ROOTEDCON

Omar Benbouazza
Co-organizador

"La candente situación geopolítica actual jugará un papel fundamental, ya que los estados continuarán promocionando ataques orientados principalmente a infraestructuras críticas de los que consideran enemigos directos o indirectos. Tampoco debemos olvidar que en estos momentos estamos sumidos de forma indirecta en una guerra híbrida, y eso nos convertirá a los profesionales de la seguridad y a las empresas, en parte importante de sus objetivos".

HACKERS

Pedro Candel
Aka @NN2ed_s4ur0n

"Encendiendo mi bola de adivino, me atrevería a afirmar que la IA y lo fácil que se han puesto las cosas incluso para gente sin conocimientos específicos de desarrollo de *exploits* o explotación de sistemas, sacan cosas y en algunos casos de uso reales. Con la (in)seguridad de IoT y las infraestructuras críticas, vamos a ver alguna fuga masiva de datos en algún dispositivo de uso personal que revelará cosas que no queremos que se sepan, incluso creo que algún hardware muy conocido, no del todo seguro y empleado por millones de clientes, va a permitir una ejecución remota de código que permitirá obtener los datos necesarios para hacer cosas 'malas'...

En cuanto a infraestructuras críticas en Europa, veremos un incremento en el número de ataques a importantes centros por la guerra de Ucrania, pero como vamos a derivar en una mayor provisión de recursos económicos e intelectuales, haremos el esfuerzo y es uno de los sitios por donde 'nos van a dar fuerte'...

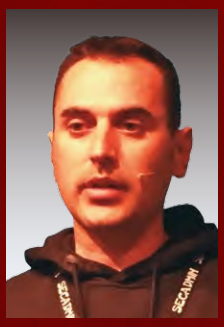
Por supuesto, volveremos a ver comprometidos sitios gubernamentales y en la cadena de suministro, ya que por más esfuerzo que hacen, sus medidas de seguridad son bastante mejorables por más controles que los CISO's quieran imponer faltando los recursos humanos y económicos para poder hacerlo... pero que los CEO's descansen en paz y se marchen a bucear al Pacífico...

Anonymous y el *hacktivismo* volverán o harán alguna de las suyas; es seguro que se intentará una desestabilización de los mercados económicos y que las criptomonedas y el *blockchain* sean la salvación del Capitán del Titanic y sus siervos...

Por último, los EDR's con IA/ML seguirán por detrás de las nuevas amenazas sin protegernos de nada pero vendiendo mucho humo y sacando mucho dinero a quien no esté informado realmente de lo que pasa en el 'cibermundo'…".

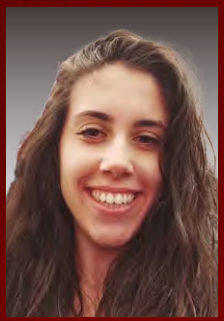
Nuria Prieto
Aka @sí, soy esa

"La verdad es que en nuestra institución es lo mismo de siempre, DDoS, escaneos, intentos de intrusión, etc. Si es cierto que hemos notado un aumento de dispositivos móviles infectados, por eso he hablado más de ellos. Actualmente los teléfonos son nuestro elemento de comunicación y trabajo, ya sea con instituciones públicas, sanitarias, privadas (bancos). Es una herramienta de trabajo muy importante y si te das cuenta, es el elemento que menos protegemos. Con ellos nos conectamos a unas cuantas RRSS, al correo, abrimos enlaces que nos mandan nuestros amigos, etc. Tenemos sesiones abiertas en todas las aplicaciones nombradas y eso supone que en cualquier momento estamos expuestos a un robo de sesión".



Luis Vacas
Aka @CyberVaca

"La evolución del *ransomware* ha sido constante y acelerada en los últimos años. Lo que comenzó como una forma simple de extorsión se ha vuelto cada vez más sofisticada y peligrosa. En el futuro, es probable que veamos un aumento en la utilización de *ransomware* en ataques a grandes corporaciones y gobiernos, ya que estos objetivos suelen tener más recursos para pagar el rescate y son más propensos a ceder ante la presión. También es posible que veamos un aumento en la utilización de técnicas de ciberseguridad más avanzadas por parte de los ciberdelincuentes, como el uso de IA para mejorar la efectividad de los ataques de *ransomware*. Por otro lado, es probable que también veamos un aumento en la utilización de medidas de las empresas y los gobiernos, como la copia de seguridad de datos y la formación de personal para detectar y prevenir ataques de *ransomware*. En resumen, es importante seguir estando alerta y protegiéndose contra el *ransomware*, ya que representa una amenaza que continuará evolucionando y creciendo".



Lucía Cachinero
Aka @QwertyStack

"2023 va a ser muy diferente a los años vividos un tiempo atrás en relación con ciberataques y amenazas. Nos encontramos en una realidad dependiente de la tecnología, los malos lo saben y se aprovechan de ello.

Apostaría como claro ganador a todo aquello que llegue a tener relación con el robo, la venta o el uso de datos (un bien valioso), por ello como joya de la corona pondría el *phishing* en todas y cada una de sus tipologías (*spear, whale, smishing, ...);* tanto es así que me atrevería a decir que no lo trataremos en su versión tradicional como hasta ahora, los cibercriminales cada vez son más creativos en sus proyectos y es por ello que creo fielmente que veremos el desarrollo de nuevas IAs dedicadas al mal como se pudo apreciar en 2022 con el *deepfake*, entre otros".

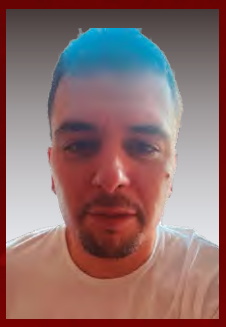
BUG BOUNTY

DragonJAR

Jaime Andrés Restrepo
Hunter y Socio de Epic Bounties
y fundador de DragonJAR Conference

"La suplantación de voz con inteligencia artificial es una amenaza creciente en el panorama de la seguridad informática. Y 2023 podría ser el año en que veamos un aumento significativo en el uso de esta tecnología para fines fraudulentos. Una de las herramientas más recientes en esta área es VALL-E, una IA capaz de generar códigos basados en fonemas y en grabaciones de audio para clonar voces con solo una pequeña cantidad de datos de referencia. Los resultados son sorprendentes y permiten crear audios muy similares a los originales con solo unos pocos segundos de audio de referencia.

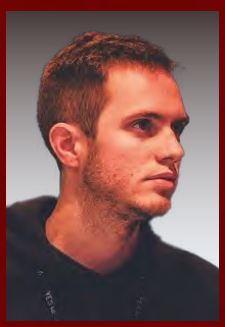
Pero ¿qué significa esto en términos de seguridad y posibles fraudes? Imaginemos recibir una nota de voz de un ser querido o de tu jefe por WhatsApp que, en realidad, ha sido generada por VALL-E con solo una pequeña cantidad de audio de referencia de tu contacto. Los fraudes podrían ser muy creíbles y realizarse con poco esfuerzo. Por eso es importante estar alerta y verificar la autenticidad de las voces y comunicaciones que recibimos. Confirmar por un medio distinto la información recibida y estar pendientes de las últimas tendencias en fraudes con estas tecnologías es clave para protegernos de estas amenazas".



HACKER ONE

José Domingo Carrillo
Hunter. Aka 0xd0m7

"Tras la última publicación del RCE (ejecución remota de código) en Microsoft Exchange (ProxyShell) el 2023 será un año en el que veremos muchas vulnerabilidades asociadas a servicios de correo profesional. Sin duda los atacantes tendrán muy en cuenta este tipo de servicios y podríamos ver un amplio abanico de vulnerabilidades asociadas a estos servicios. El análisis del tráfico UDP/TCP por parte de las empresas será un factor determinante a la hora de paliar este tipo de ataques ya que como se comprobó en el 2022 muchos de estos ataques son de día cero (0day) y los parches para paliar estos atacantes a veces llegan demasiado tarde".



YESWEHACK

Adrien Jeanneau
Hunter. Aka Hisxo's

"A medida que las tecnologías de inteligencia artificial (IA) y aprendizaje automático (ML) se vuelven cada vez más omnipresentes, los actores malintencionados pueden explotarlas con fines nefastos. Por ejemplo, un ciberdelincuente podría usar modelos de aprendizaje automático para hacerse pasar por un usuario legítimo o crear correos electrónicos de *phishing* convincentes.

Los ataques a la cadena de suministro también podrían ver un mayor aumento en el próximo año. Es probable que la proliferación de dispositivos conectados y el Internet de las cosas (IoT) creen nuevas vulnerabilidades y oportunidades para los atacantes. A medida que se conectan más dispositivos a Internet, existe un mayor riesgo de que puedan ser utilizados para lanzar ataques u obtener acceso a otros sistemas.

Finalmente, el uso de los programas *Bug Bounty* podría desempeñar un papel fundamental en la mitigación de los riesgos de este tipo de ataques. Al identificar y revelar las vulnerabilidades antes de que los ciberdelincuentes puedan explotarlas, los cazadores de errores pueden ayudar a las organizaciones a parchear y proteger sus sistemas".