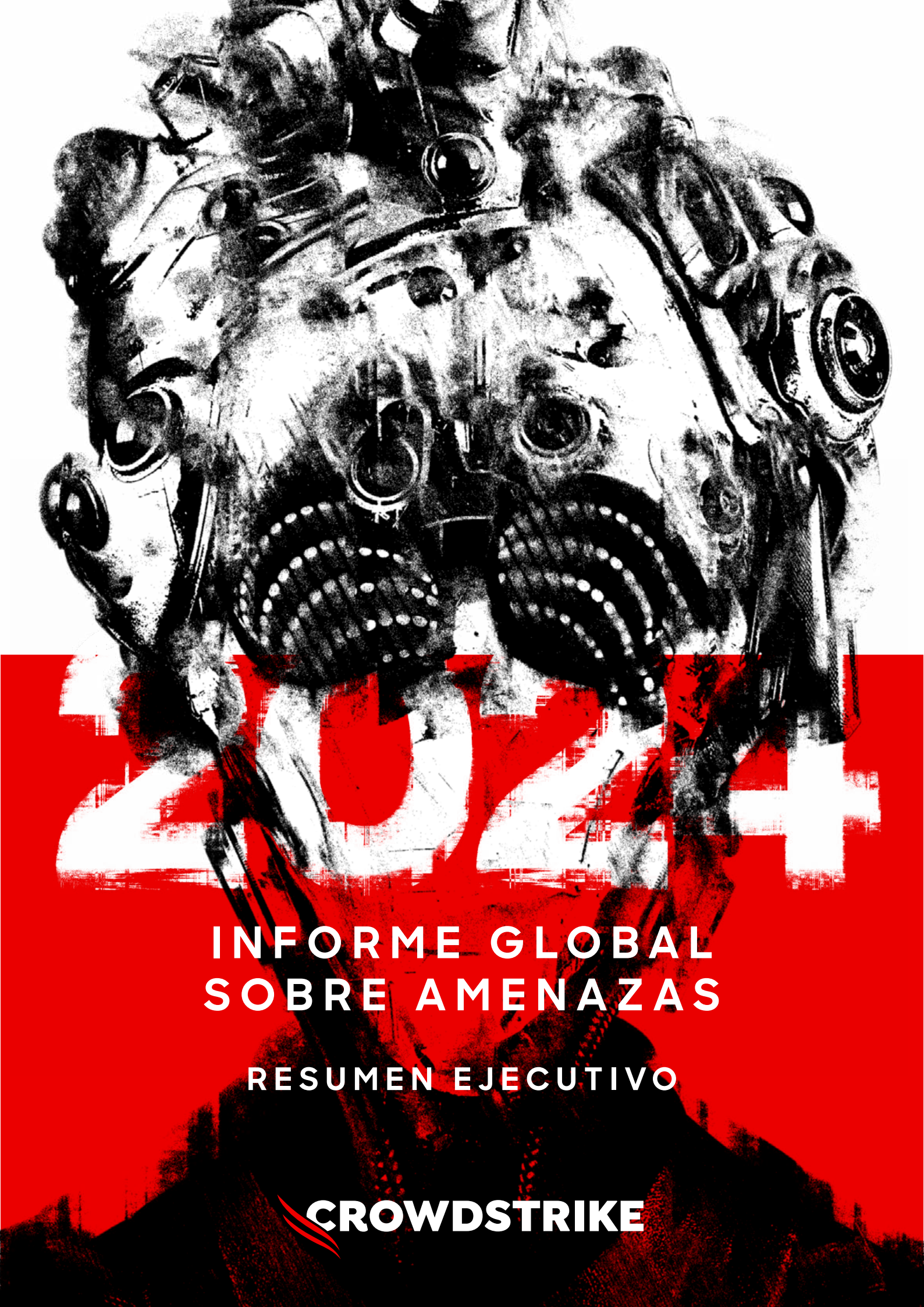
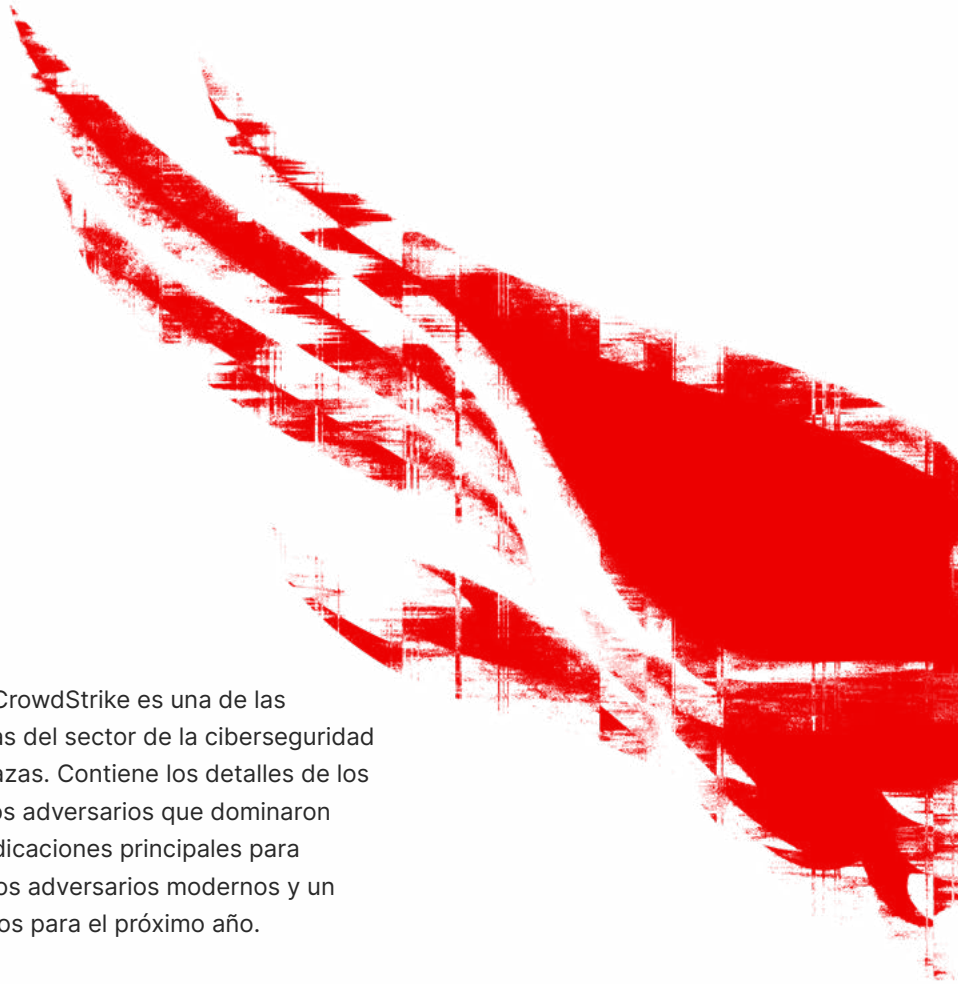


2024

INFORME GLOBAL SOBRE AMENAZAS

RESUMEN EJECUTIVO

CROWDSTRIKE



El Informe Global sobre Amenazas de CrowdStrike es una de las investigaciones más fiables y completas del sector de la ciberseguridad sobre el panorama actual de las amenazas. Contiene los detalles de los eventos y tendencias clave de 2023, los adversarios que dominaron la actividad durante todo el año, las indicaciones principales para las organizaciones que luchan contra los adversarios modernos y un resumen de los eventos que anticipamos para el próximo año.

Para derrotar a los adversarios de hoy en día, primero debes saber a qué te enfrentas. La ciberseguridad cambia constantemente a medida que las innovaciones tecnológicas afectan a los distintos sectores y los adversarios cambian sus técnicas para ser más rápidos, sofisticados y eficaces. El Informe Global sobre Amenazas 2024 de CrowdStrike repasa la actividad de 2023 para que las organizaciones puedan prepararse para el próximo año. Conocer los detalles de eventos pasados te permite comprender mejor lo que buscan los adversarios, quiénes son sus objetivos y cómo actúan.

En 2023, CrowdStrike Falcon® Intelligence y CrowdStrike® Falcon OverWatch® se fusionaron para convertirse en CrowdStrike Counter Adversary Operations (CAO), y combinaron el poder de la inteligencia sobre amenazas con la velocidad de los equipos de Threat Hunting especializados y billones de eventos de telemetría de la plataforma CrowdStrike Falcon® basada en IA nativa. El Informe Global sobre Amenazas de este año se desarrolló según las observaciones de primera mano de este equipo de élite.

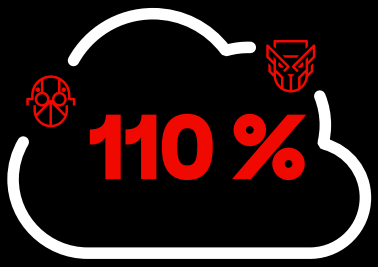
Este resumen contiene información general sobre los principales hallazgos del informe, que detallan información importante sobre lo que los equipos de seguridad deben saber (y hacer) en un panorama de amenazas cada vez más complejo.

CONVENCIONES DE DENOMINACIÓN

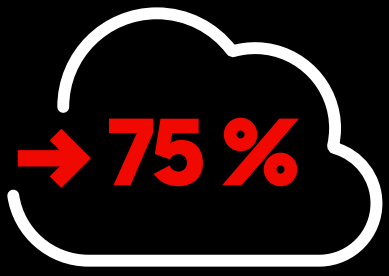
Atacante	Estado o categoría
BEAR	RUSIA
BUFFALO	VIETNAM
CHOLLIMA	COREA DEL NORTE
CRANE	REPÚBLICA DE COREA
HAWK	SIRIA
JACKAL	HACKTIVISTA
KITTEN	IRÁN
LEOPARD	PAKISTÁN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	REPÚBLICA POPULAR DE CHINA
SPHINX	EGIPTO
SPIDER	CIBERDELINCUENTE
TIGER	INDIA
WOLF	TURQUÍA

Información general sobre el panorama de amenazas

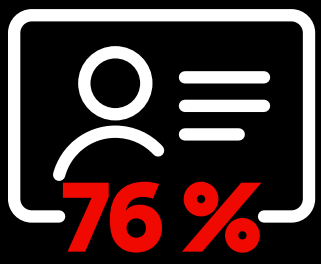
CrowdStrike ha rastreado **34** adversarios nuevos, por lo que el total asciende a **232**



Los ataques orientados a la nube han registrado un aumento interanual del **110 %**



Las intrusiones en entornos de nube han registrado un aumento interanual del **75 %**



Aumento interanual del 76 % en el número de víctimas mencionadas en sitios específicos de filtración de datos de ciberdelincuencia

El **84 %** de las intrusiones en la nube atribuidas a adversarios se centraron en la ciberdelincuencia

INFORMACIÓN GENERAL SOBRE EL PANORAMA DE AMENAZAS

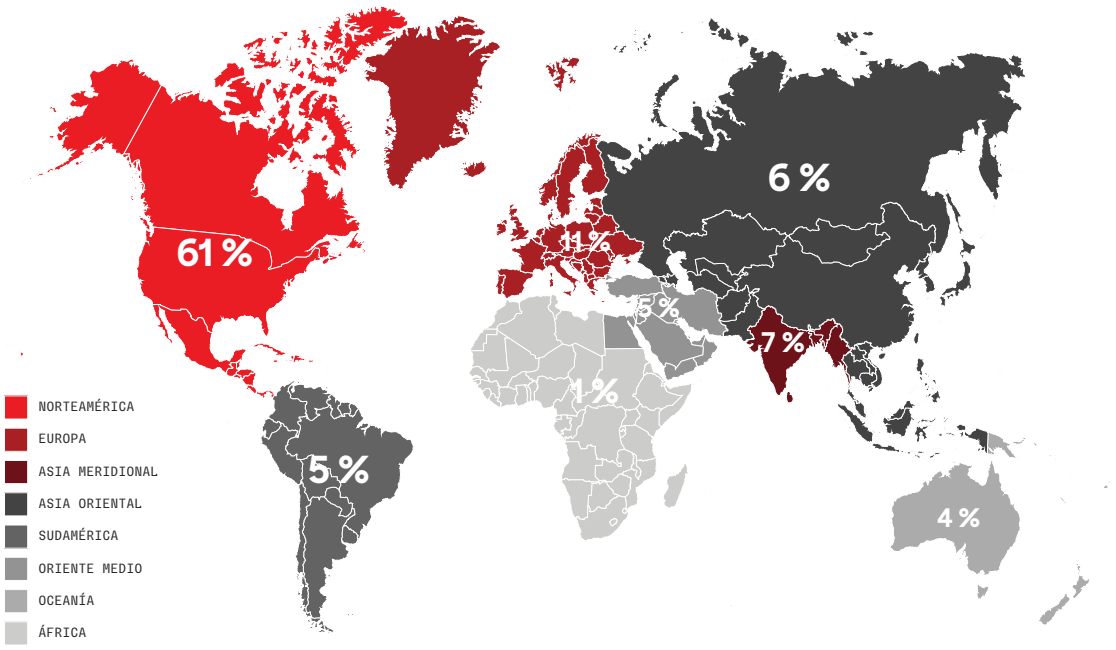
- **Los adversarios son cada vez más rápidos:** el tiempo medio de propagación de un ciberataque en 2023 fue de 62 minutos, y el más rápido registrado fue de 2 minutos y 7 segundos. En un ataque típico, CrowdStrike ha observado que más del 88 % del tiempo de ataque estaba dedicado a obtener acceso inicial, y los adversarios están haciendo todo lo posible para reducirlo. Una vez dentro, un atacante tardó solo 31 segundos en copiar una herramienta de descubrimiento inicial.

- **Las intrusiones interactivas se están acelerando:** la actividad "hands-on-keyboard" aumentó un 60 % en 2023 en comparación con 2022. En el segundo semestre de 2023, el aumento subió al 73 % en comparación con el mismo periodo de tiempo del año anterior. Tres cuartas partes de los ataques para obtener acceso inicial se llevaron a cabo sin malware, frente al 71 % en 2022, lo que pone de manifiesto el cambio de los adversarios hacia técnicas más rápidas y efectivas.

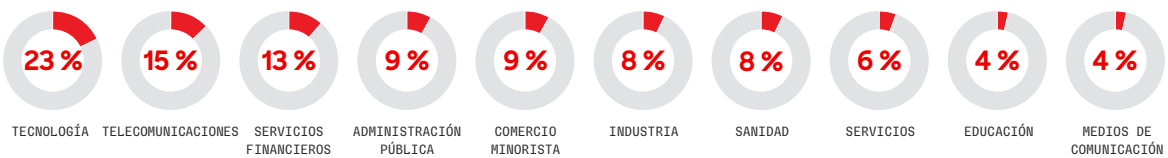
- **La nube es un campo de batalla en evolución:** a medida que las organizaciones trasladan sus operaciones a la nube, los adversarios continúan desarrollando su experiencia en la nube. Las intrusiones en la nube aumentaron en un 75 % en 2023 y los ataques orientados a la nube aumentaron en un 110 %.

- **La extorsión por robo de datos ayuda a la monetización:** CrowdStrike observó un aumento del 76 % en el número de víctimas mencionadas en los sitios específicos de filtración de datos BGH (caza mayor, del inglés "big game hunting"), lo que demuestra el estado de BGH como la amenaza de ciberdelincuencia más importante para las organizaciones que operan en distintos sectores y regiones.

Intrusiones interactivas por región



Intrusiones interactivas por sector



ANATOMÍA DE UN CIBERDELITO

INTRUSIÓN INTERACTIVA

En uno de los ataques (que se muestra en la figura anterior), el equipo de seguridad tenía desactivada la configuración de la directiva que establece que el archivo sospechoso se debe poner en cuarentena al detectar escritura, lo que permitió que se copiaran cuatro archivos en el disco. El adversario ejecutó una herramienta legítima con el fin de obtener la información del sistema para el reconocimiento y luego copió tres archivos más, incluido el ransomware, en el sistema. Intentaron ejecutar una herramienta de descubrimiento y reconocimiento de redes para utilizar opciones de movimiento lateral, que fue inmediatamente bloqueada y puesta en cuarentena por el sensor de Falcon. Esto provocó que el adversario abriera el panel de control para ver qué herramienta de seguridad estaba en uso. Cuando identificaron la plataforma Falcon, nunca intentaron ejecutar la segunda herramienta de descubrimiento ni el ransomware (que se habría bloqueado y puesto en cuarentena), y se dirigieron a otra víctima. En cuestión de minutos, los expertos en Threat Hunting de CrowdStrike CAO notificaron el ataque al cliente, desconectaron la máquina y restablecieron la contraseña del usuario.

Una vez que se produce un compromiso inicial, los adversarios solo tardan unos segundos en copiar herramientas o malware en el entorno de una víctima durante una intrusión interactiva. Sin embargo, el refrán "el tiempo es oro" se ajusta perfectamente a la actividad de los adversarios. Más del 88 % del tiempo del ataque se invirtió en forzar la entrada y obtener acceso inicial. Al reducir o eliminar este tiempo, los adversarios liberan recursos para llevar a cabo más ataques.

ACTIVIDAD SIN MALWARE

»

75 % 2023
71 % 2022
62 % 2021
51 % 2020
40 % 2019

Temas clave

Ataques basados en la identidad y de ingeniería social

Para llevar a cabo sus ataques, los adversarios que operan en varias regiones y con diversas motivaciones continúan utilizando técnicas de phishing que suplantan a usuarios legítimos para atacar cuentas válidas, además de robar otros datos de autenticación e identificación.

- Además de robar las credenciales de las cuentas, CrowdStrike CAO observó que los adversarios dirigían sus ataques a las claves de API y los secretos, las cookies de las sesiones y los tokens, las contraseñas de un solo uso y los tickets de Kerberos a lo largo de 2023.

- Estos ataques son comunes tanto entre los adversarios patrocinados por un Estado como entre los ciberdelincuentes por igual. En el caso de los ataques patrocinados por un Estado, FANCY BEAR llevó a cabo campañas periódicas de recopilación de credenciales a lo largo de 2023. En las campañas de phishing para recopilar credenciales, desarrollaron un kit de herramientas personalizado para capturar las credenciales de los usuarios de Yahoo! Mail y el correo web de ukr.net. COZY BEAR llevó a cabo campañas de phishing para recopilar credenciales a través de mensajes de Microsoft Teams en los que se solicitaban los tokens de autenticación multifactor (MFA) para cuentas de Microsoft 365.

- Las técnicas basadas en la identidad también son fundamentales para la actividad de SCATTERED SPIDER: a lo largo de 2023, este adversario llevó a cabo sofisticados ataques de ingeniería social para acceder a las cuentas de las víctimas.

Los adversarios continúan desarrollando sus ataques orientados a la nube

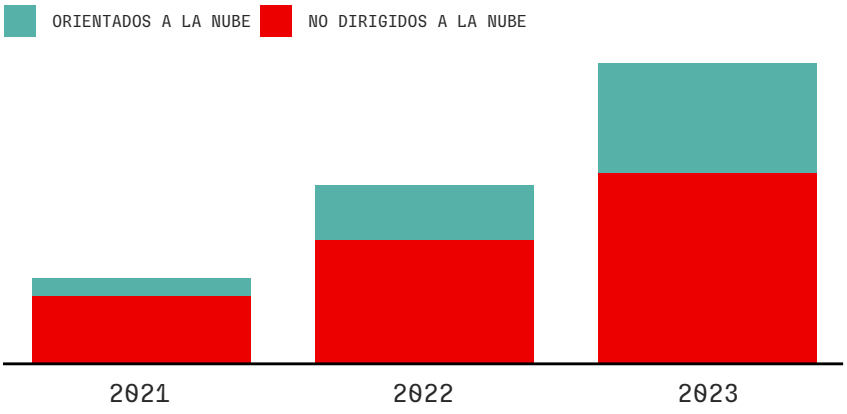
Como se predijo, la nube siguió siendo un campo de batalla en evolución para la actividad de los adversarios en 2023. CrowdStrike CAO observó un aumento del 110 % en los ataques orientados a la nube, en los que los adversarios sabían que habían vulnerado un entorno en la nube y habían utilizado este acceso para atacar el servicio en la nube. El equipo también observó un aumento del 60 % en los ataques que no estaban dirigidos a la nube. Los autores de los ataques que no estaban dirigidos a la nube no sabían que habían comprometido un entorno de nube o no aprovecharon las características específicas de la nube.

- SCATTERED SPIDER fue el ciberdelincuente que protagonizó principalmente el aumento en la actividad orientada a la nube a lo largo de 2023, y representa el 29 % del total de casos. El adversario demostró técnicas progresivas y sofisticadas dentro de entornos de nube específicos para mantener la persistencia, obtener credenciales, moverse lateralmente y exfiltrar datos.

- Los ciberdelincuentes fueron especialmente activos a la hora de atacar los entornos en la nube: el 84 % de las intrusiones en la nube atribuidas a los adversarios las llevaron a cabo posibles ciberdelincuentes.

- La preferencia de los adversarios por las técnicas basadas en la identidad es evidente en sus ataques centrados en la nube. A menudo utilizan credenciales válidas para conseguir el acceso inicial a los entornos en la nube, lograr la persistencia en el nivel de identidad y escalar privilegios al conseguir el acceso a identidades adicionales.

INCIDENTES EN LA NUBE



▲ 110 % ATAQUES ORIENTADOS A LA NUBE

LOS CIBERDELINCUENTES SON CONSCIENTES DE QUE HAN CONSEGUIDO ACCEDER A UN ENTORNO EN LA NUBE PROPIEDAD DE LA VÍCTIMA Y UTILIZAN SU ACCESO PARA REALIZAR UN USO INDEBIDO DEL SERVICIO EN LA NUBE QUE POSEE LA VÍCTIMA

▲ 60 % ATAQUES NO DIRIGIDOS A LA NUBE

LOS AUTORES NO SABÍAN QUE HABÍAN COMPROMETIDO UN ENTORNO EN LA NUBE O NO APROVECHARON LAS CARACTERÍSTICAS DE LA NUBE

↑75 %
EN INTRUSIONES EN LA NUBE

Exploits de relaciones con terceros

A lo largo de 2023, los autores de la intrusión selectiva intentaron aprovechar las relaciones de confianza para conseguir acceso inicial a las organizaciones. Este tipo de ataque aprovecha las relaciones entre proveedores y clientes para desplegar herramientas maliciosas mediante dos técnicas clave: una implica comprometer la cadena de suministro de software con software fiable para distribuir herramientas maliciosas; la otra consiste en aprovechar el acceso a los proveedores que prestan servicios de TI.

- Los adversarios que aprovechan las relaciones con terceros están motivados por el potencial de rentabilidad de la inversión: una organización comprometida puede dirigir a cientos o miles de objetivos secundarios.

- En 2023, los adversarios ligados a China aumentaron sus ataques a los terceros relacionados para desplegar implantaciones maliciosas y conseguir acceso inicial. JACKPOT PANDA y CASCADE PANDA aprovecharon las relaciones de confianza a través de vulneraciones en la cadena de suministro y ataques "actor-on-the-side" o "actor-in-the-middle".

- Corea del Norte también demostró un creciente interés en aprovechar las relaciones de confianza en 2023: en concreto, LABYRINTH CHOLLIMA abusó de una relación de confianza entre un proveedor de tecnología y un cliente en tres casos el año pasado.

Panorama de vulnerabilidades: Exploits desapercibidos

Los ciberdelincuentes se han adaptado a la visibilidad mejorada de los sensores tradicionales de detección y respuesta para endpoints (EDR) modificando sus tácticas de ataque para el acceso inicial y el movimiento lateral. Ahora, se dirigen a la periferia de la red, donde la visibilidad de los mecanismos de defensa se ve reducida por la posibilidad de que los endpoints carezcan de sensores EDR o no puedan admitir el despliegue de sensores.

- Se ha observado que los dispositivos de red no gestionados, en particular los dispositivos de gateway perimetral, siguieron siendo el vector de acceso inicial más habitual para los ataques en 2023.

- Los autores de amenazas están desarrollando exploits para productos que han alcanzado el final de su vida útil, que no admiten la aplicación de parches y que, a menudo, no permiten el despliegue de sensores modernos. Los servidores de sistemas operativos no compatibles y los dispositivos de gateway tradicionales ofrecen un acceso fácil, incluso a familias de malware más antiguas, lo que conduce a infecciones persistentes.

Conflicto entre Israel y Hamás en 2023: las ciberoperaciones se centran en la interrupción y la influencia

CrowdStrike CAO ha rastreado las ciberoperaciones en curso de intrusión selectiva y autores hacktivistas desde el comienzo del conflicto entre Israel y Hamás en 2023. La actividad y las afirmaciones de ambos tipos de autores de amenazas se centran principalmente en atacar la tecnología operativa u otros sistemas esenciales (probablemente para influir psicológicamente en las poblaciones objetivo), y en desplegar wipers destructivos contra Israel o entidades vinculadas a Israel.

- CrowdStrike CAO rastrea a muchos adversarios asociados con el grupo militante Hamás; sin embargo, hasta la fecha no se ha observado actividad atribuida a estos adversarios en relación con el conflicto entre Israel y Hamás. Es probable que esto se deba a la falta de recursos disponibles o a la degradación de la infraestructura de distribución de electricidad e Internet en la zona del conflicto.

- RENEGADE JACKAL fue el adversario más activo ligado a Hamás a lo largo de 2023. EXTREME JACKAL y RENEGADE JACKAL, los adversarios con posible sede en Gaza evaluados por CrowdStrike CAO, muestran su apoyo a los intereses estratégicos de Hamás.

- Es casi seguro que la actividad hacktivista continuará al ritmo de las fluctuaciones en los desarrollos geopolíticos relacionados. Esta evaluación se ha realizado con un nivel de confianza alto en función de los patrones de actividad demostrados hasta la fecha.

PERSPECTIVA PARA 2024

Mientras las organizaciones planifican sus medidas de protección antes las posibles amenazas que surjan en 2024, existen dos motores potenciales de la interrupción que son los más importantes: la IA generativa y las elecciones gubernamentales mundiales de 2024.

Uso de la IA generativa en el panorama de amenazas

La IA generativa ha democratizado enormemente la informática para mejorar las operaciones de los adversarios. También puede reducir potencialmente los obstáculos a los que se enfrentan los autores de amenazas menos sofisticados para entrar en el panorama de amenazas.

La IA generativa ofrece dos áreas principales de oportunidades dentro del panorama de amenazas:

- El desarrollo o ejecución de operaciones maliciosas de redes informáticas (CNO, del inglés "computer network operations"), incluido el desarrollo de herramientas y recursos, como scripts o código que podrían ser funcionalmente maliciosos si se utilizan correctamente.

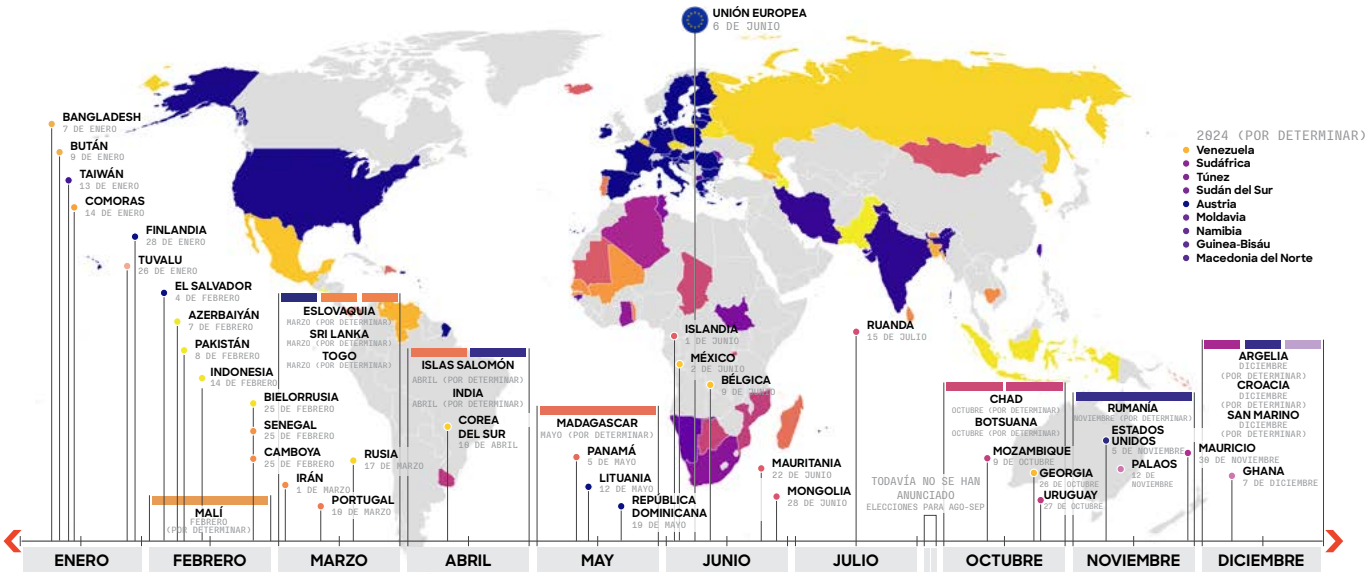
- El respaldo de la eficiencia y eficacia de las campañas de ingeniería social y operaciones de información (IO).

La evaluación de CrowdStrike CAO indica que es probable que la IA generativa se utilice para ciberactividades en 2024 a medida que continúe ganando popularidad. A lo largo de 2024, el equipo hará un seguimiento de cómo los autores de amenazas utilizan esta tecnología y cómo difiere este uso de las aplicaciones convencionales.

Elecciones de 2024

Los ciudadanos de 55 países que representan más del 42 % de la población mundial participarán en elecciones presidenciales, parlamentarias o generales. Esto incluye siete de los 10 países con mayor número de habitantes del mundo. Las elecciones a nivel nacional también se celebrarán en países o grupos implicados en conflictos geopolíticos importantes o próximos a ellos.

Históricamente, las actividades maliciosas más comunes dirigidas a las elecciones se han basado en IO, probablemente llevadas a cabo por entidades ligadas al estado contra ciudadanos de países que representan un interés geopolítico específico para el autor de las amenazas; estas actividades también se han basado en un hacktivismo simple y de corta duración, incluidos ataques de denegación de servicio distribuido (DDoS) y desfiguraciones de sitios web, contra entidades gubernamentales estatales y locales. Es muy probable que esta tendencia continúe en 2024. Es probable que los países de interés involucrados en los ciclos electorales corran el riesgo de sufrir campañas de IO significativas y prolongadas en el tiempo por parte de las principales potencias mundiales.

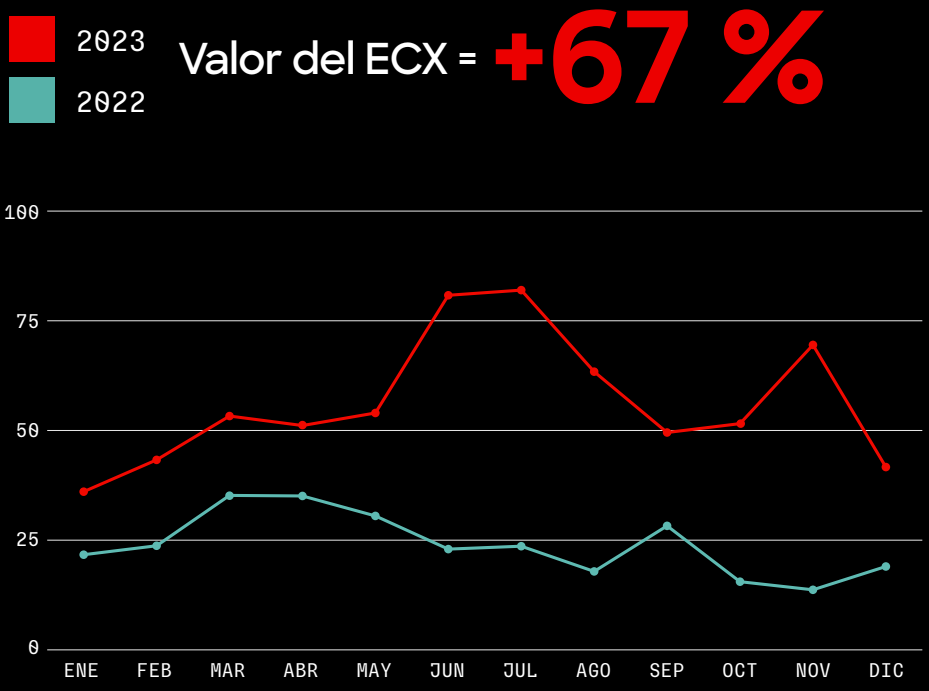


PANORAMA DE CIBERDELINCUENCIA

El índice de ciberdelincuencia CrowdStrike eCrime Index® (ECX) rastrea la actividad, incluido el número de correos electrónicos de spam observados y el coste promedio de la compra del acceso a una red corporativa, en varios segmentos del ecosistema de ciberdelincuencia, y calcula el número total de víctimas de ransomware observadas.

Hasta mayo de 2023, el ECX presentó tendencias similares a las que se observaron en 2022. Sin embargo, a partir de junio de 2023, el ECX creció significativamente, con repuntes importantes entre junio y agosto. Los factores que más contribuyeron a estos repuntes fueron la alta frecuencia de incidentes de BGH y un aumento repentino de los ataques DDoS observados.

El ECX volvió a repuntar en noviembre de 2023, lo que refleja el aumento del número de correos electrónicos spam y el incremento del precio medio de los cargadores y ladrones.



El ECX de 2023 registró la mayor actividad anual hasta la fecha, lo que representa el crecimiento interanual del índice. Es probable que los correos electrónicos spam disminuyeran en 2023 mientras los adversarios buscaban otros medios para conseguir el acceso inicial y después de que una operación multinacional bloqueara las infecciones por QakBot de MALLARD SPIDER.

Aunque la media de demandas de rescate fue menor en 2023 que en 2022, es muy probable que esto represente un valor atípico en el conjunto de datos y no una representación precisa del panorama de amenazas. Es probable que las demandas de rescate se hayan mantenido constantemente altas durante este periodo, pero la capacidad de rastrear estos valores es cada vez más difícil debido a que los autores de amenazas y las víctimas implementan medidas de privacidad más estrictas en torno a las demandas y los pagos de los precios de rescate.

Nuevas vulnerabilidades con una clasificación del CVSS3 de 9/10
+6 %

Incidentes de BGH que involucran filtraciones de datos
+76 %

Coste promedio del cargador
+169 %

Coste promedio del cifrador
+250 %

Coste promedio del ladrón
+286 %

Demanda media de rescate
-27 %

Correos electrónicos de spam identificados
-15 %

Caza mayor

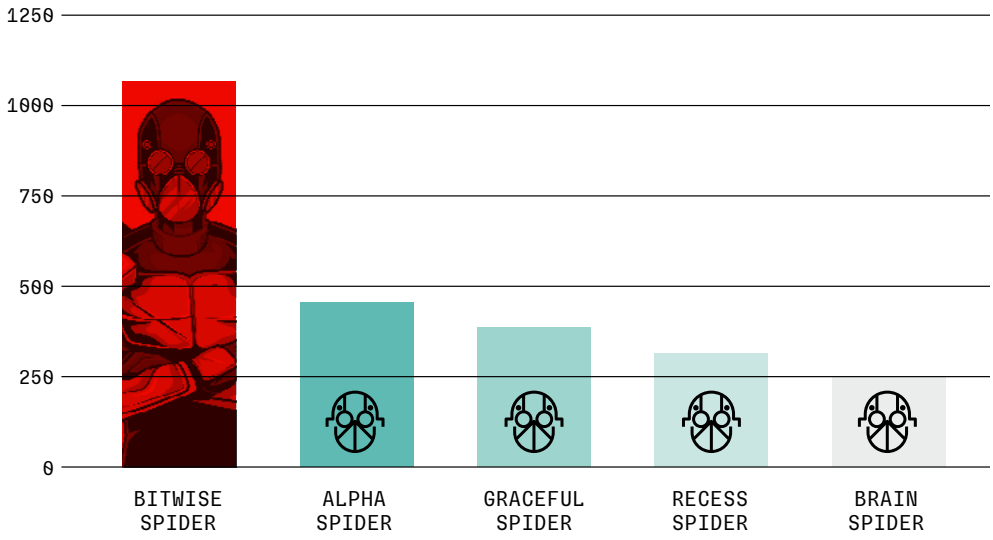
El número de víctimas mencionadas en los sitios específicos de filtración de datos de BGH aumentó significativamente el año pasado, con 4615 publicaciones sobre víctimas incluidas en sitios específicos para la filtración de datos (DLS, del inglés "dedicated leak sites") en 2023, lo que representa un aumento del 76 % con respecto a 2022. Varios factores contribuyeron a este crecimiento, incluidos los nuevos ciberdelincuentes de BGH, el crecimiento de las operaciones de los adversarios existentes y algunas campañas de gran volumen, como los numerosos exploits de día cero de GRACEFUL SPIDER.

En conjunto, ITWISE SPIDER, ALPHA SPIDER, GRACEFUL SPIDER, RECESS SPIDER y BRAIN SPIDER representan el 77 % de las publicaciones en todos los DLS de adversarios rastreados. BITWISE SPIDER y ALPHA SPIDER han publicado históricamente numerosas publicaciones nuevas de DLS y se han clasificado en primer y segundo lugar, respectivamente, por el mayor número de publicaciones de DLS en 2022 y 2023.

RECESS SPIDER y BRAIN SPIDER comenzaron sus propias operaciones de ransomware a mediados de 2022 y en enero de 2023, respectivamente. Desde entonces, han crecido en importancia hasta representar el cuarto número más alto (RECESS SPIDER) y el quinto número más alto (BRAIN SPIDER) de publicaciones de DLS en 2023.

GRACEFUL SPIDER, que lleva activo desde 2016 y generalmente ha llevado a cabo campañas de bajo volumen, aprovechó tres vulnerabilidades de día cero en 2023 para exfiltrar datos de cientos de víctimas en todo el mundo. Este adversario finalmente publicó el tercer mayor número de publicaciones de DLS ese año.

Principales adversarios por publicaciones de DLS



EL NÚMERO DE VÍCTIMAS MENCIONADAS EN LOS SITIOS ESPECÍFICOS DE FILTRACIÓN DE DATOS DE BGH AUMENTÓ SIGNIFICATIVAMENTE EN 2023, CON 4615 PUBLICACIONES SOBRE VÍCTIMAS INCLUIDAS EN DLS), LO QUE REPRESENTA UN AUMENTO DEL 76 % CON RESPECTO A 2022.

RECOMENDACIONES

CrowdStrike ofrece las siguientes recomendaciones para ayudar a las organizaciones a proteger sus recursos y defenderse de un ecosistema de ciberdelincuencia en constante evolución:

Haz que la protección de identidades sea imprescindible

Los ataques basados en la identidad y de ingeniería social conformaron el panorama de amenazas de 2023. Para contrarrestar estas amenazas, es esencial implementar la autenticación multifactor (MFA) y ampliarla a los sistemas y protocolos antiguos, formar a los equipos en materia de ingeniería social e implementar tecnología que pueda detectar y correlacionar amenazas en entornos de identidades, endpoints y la nube. La visibilidad y la aplicación en distintos dominios permiten a los equipos de seguridad detectar el movimiento lateral, obtener una visibilidad completa de la ruta de ataque y detectar el uso malicioso de herramientas legítimas. Abordar los métodos de acceso sofisticados, como el cambio de SIM, la omisión de la MFA y el robo de claves API, las cookies de sesión y los tickets de Kerberos, requiere una búsqueda continua de comportamientos maliciosos.

Prioriza las plataformas de protección de aplicaciones nativas de la nube (CNAPP)

Las empresas necesitan una visibilidad completa de la nube para eliminar errores de configuración, vulnerabilidades y otras amenazas. Las herramientas de seguridad en la nube no deben existir de forma aislada, y las CNAPP proporcionan una plataforma unificada que simplifica la supervisión, la detección y la actuación ante posibles amenazas y vulnerabilidades en la nube. Selecciona una CNAPP que incluya protección previa al tiempo de ejecución, protección en tiempo de ejecución y tecnología sin agente para ayudarte a descubrir y correlacionar tus aplicaciones y API que se ejecutan en producción, y que te muestre todas las superficies de ataque, amenazas y riesgos empresariales críticos.

Obtén visibilidad de las áreas más críticas del riesgo empresarial

A medida que los entornos empresariales se expanden, las organizaciones deben comprender las relaciones entre la identidad, la nube, los endpoints y la telemetría de protección de datos para identificar y bloquear los ataques modernos. Al consolidar los productos puntuales en una plataforma de seguridad unificada, las organizaciones pueden conseguir visibilidad completa en una sola vista y controlar fácilmente sus operaciones con el fin de mejorar su capacidad para descubrir, identificar y evitar las brechas.

Fomenta la eficiencia

Los atacantes son cada vez más rápidos. ¿Puedes seguir el ritmo? Las soluciones tradicionales de gestión de eventos e información de seguridad (SIEM, del inglés "security information and event management") suelen ser demasiado lentas, complejas y caras, y muchas se diseñaron para una época en la que los volúmenes de datos y la sofisticación de los adversarios eran solo una fracción de lo que son hoy. Las empresas modernas necesitan una solución SIEM moderna que sea más rápida, más fácil de desplegar y más rentable que las herramientas SIEM tradicionales. Investiga enfoques que unifiquen la detección, la investigación y la respuesta a las amenazas en una única plataforma de IA nativa en la nube.

Crea una cultura de la ciberseguridad

El usuario final sigue siendo un eslabón crítico de la cadena para detener las brechas de seguridad. Deberían llevarse a cabo programas de concienciación de usuarios para combatir la continua amenaza del phishing y las técnicas de ingeniería social relacionadas. Para los equipos de seguridad, la práctica hace al maestro. Es recomendable fomentar un entorno en el que se realicen rutinariamente ejercicios de simulación teórica y de equipo rojo/equipo azul con el fin de identificar las lagunas en la seguridad y eliminar cualquier fallo en tus procedimientos de ciberseguridad y de respuesta.

DESCARGA EL INFORME COMPLETO

El Informe Global sobre Amenazas 2024 de CrowdStrike incluye un profundo análisis que destaca los incidentes y las tendencias más relevantes en materia de ciberamenazas durante 2023. Descarga una copia gratuita en https://www.crowdstrike.com/global-threat-report/.

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa para la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, una protección y un rendimiento superiores, una menor complejidad y una rentabilidad inmediata.

CrowdStrike: We stop breaches.

Más información: www.crowdstrike.com

Síguenos: Blog | X | LinkedIn | Facebook | Instagram

Empieza una prueba gratuita hoy mismo: www.crowdstrike.com/free-trial-guide