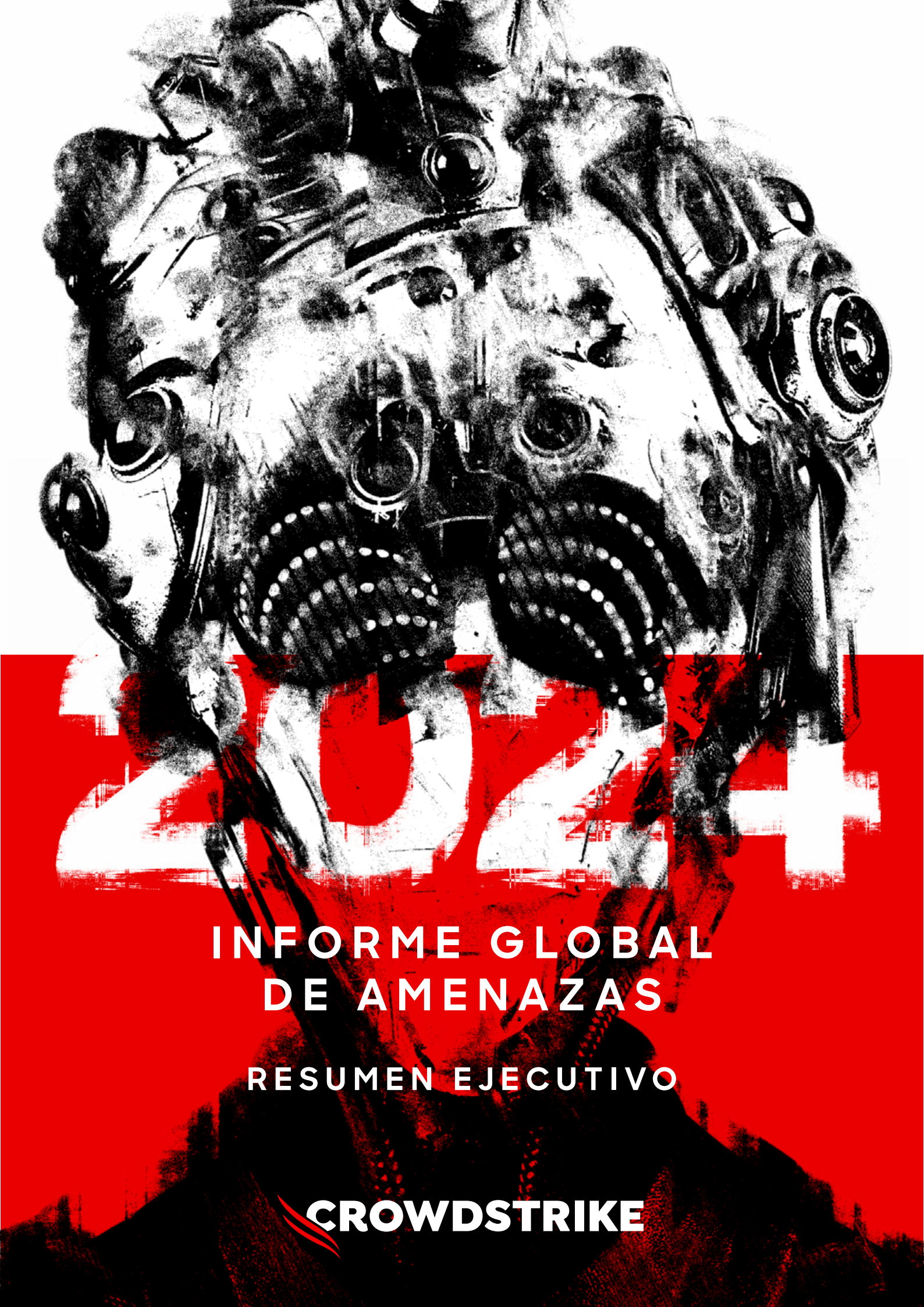


2024

INFORME GLOBAL DE AMENAZAS

RESUMEN EJECUTIVO

CROWDSTRIKE

El Informe Global de Amenazas de CrowdStrike es conocido en toda la industria de la ciberseguridad por su investigación confiable y completa sobre el panorama moderno de amenazas. Contiene los detalles de los eventos y tendencias clave que dieron forma al 2023, los adversarios que impulsan la actividad del año, orientación clave a las organizaciones que luchan contra los adversarios modernos y un vistazo a los eventos que anticipamos para el próximo año.

Para derrotar a los adversarios de hoy, primero debes saber a qué te enfrentas. La ciberseguridad cambia constantemente a medida que las innovaciones tecnológicas alteran las industrias y los adversarios cambian sus técnicas para ser más rápidos, furtivos y efectivos. El Informe Global de Amenazas de CrowdStrike 2024 repasa el año 2023 para que las organizaciones puedan prepararse para lo que viene. Conocer los detalles de eventos pasados puede fundamentar una mejor comprensión de lo que buscan los adversarios, a quién tienen por objetivo y cómo funcionan.

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

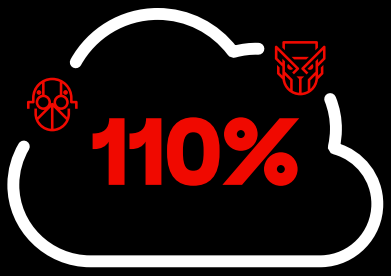
Este resumen es una descripción general de los hallazgos clave del informe, detalla información importante sobre lo que los equipos de seguridad deben saber (y hacer) en un panorama de amenazas cada vez más complejo.

CONVENCIÓN DE NOMBRES

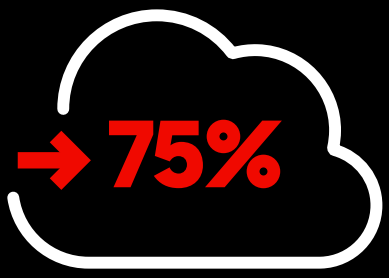
Adversario	Estado-nación o categoría
BEAR	RUSIA
BUFFALO	VIETNAM
CHOLLIMA	RPDC (COREA DEL NORTE)
CRANE	REPÚBLICA DE COREA
HAWK	SIRIA
JACKAL	HACKTIVISTA
KITTEN	IRÁN
LEOPARD	PAKISTÁN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	REPÚBLICA POPULAR CHINA
SPHINX	EGYPT
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURQUÍA

Descripción general del panorama de amenazas

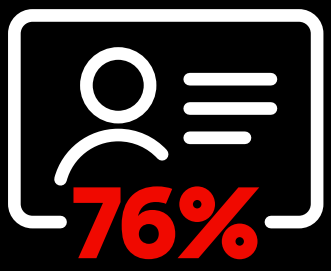
34 nuevos adversarios rastreados por CrowdStrike, elevando el total a **232**



Los casos conscientes de la nube aumentaron en un **110 % interanual**



Las intrusiones en el entorno de la nube aumentaron en un **75 % interanual**



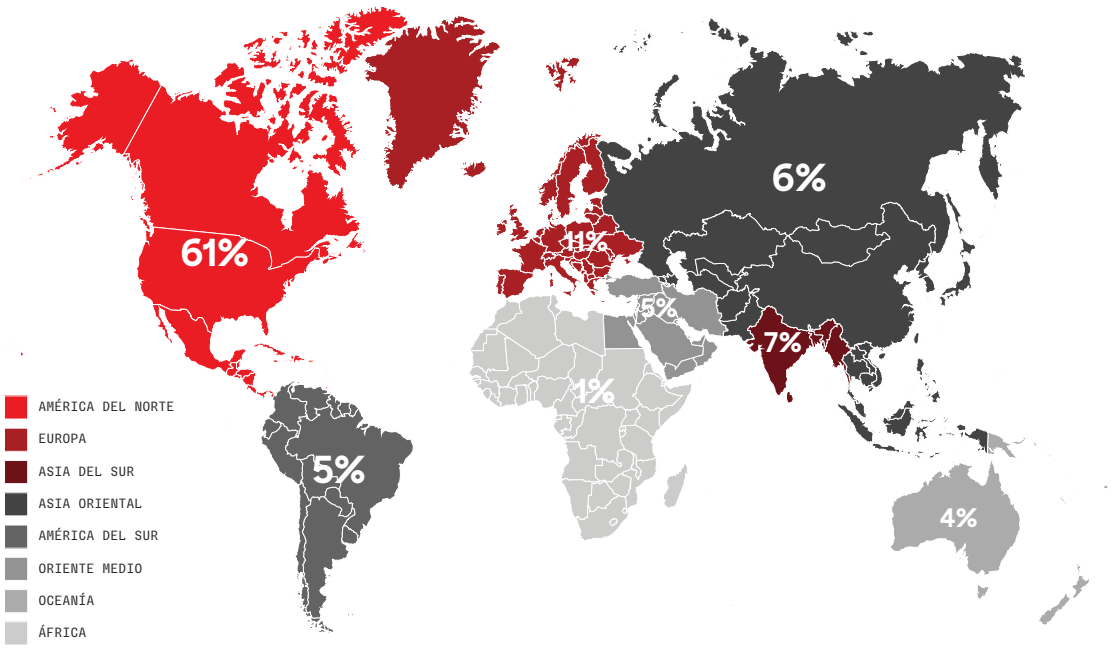
Aumento interanual del 76 % en las víctimas nombradas en los sitios específicos de filtración de datos de crimen electrónico

El 84 % de las intrusiones conscientes de la nube atribuidas a los adversarios se centraron en el crimen electrónico

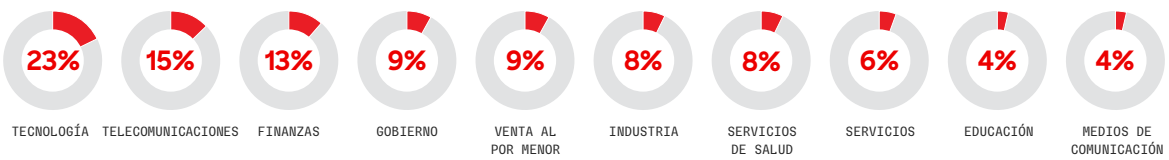
DESCRIPCIÓN GENERAL DEL PANORAMA DE AMENAZAS

- **Los adversarios son cada vez más rápidos:** el tiempo de comprometimiento promedio del crimen electrónico en el 2023 fue de 62 minutos, y el tiempo de comprometimiento más rápido registrado fue de 2 minutos y 7 segundos. En un ataque típico observado por CrowdStrike, más del 88% del tiempo de ataque se dedicó a obtener acceso inicial, y los adversarios están trabajando para reducirlo. Una vez dentro, un actor de ciberamenazas tardó solo 31 segundos en dejar una herramienta de descubrimiento inicial.
- **Las intrusiones interactivas se están acelerando:** la actividad de accesos interactivos para ejecutar comandos aumentó un 60% en el 2023 en comparación con el 2022. En la segunda mitad del 2023, el aumento se elevó al 73% en comparación con el mismo período del año anterior. Tres cuartas partes de los ataques con el objetivo de obtener acceso inicial estuvieron libres de malware, frente al 71% en el 2022, lo que subraya 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 experiencia en la nube. Las intrusiones en la nube aumentaron un 75% en el 2023 y los casos conscientes de la nube aumentaron un 110%.
- **La extorsión por robo de datos ayuda a la monetización:** CrowdStrike observó un aumento del 76% en el número de víctimas nombradas en los sitios específicos de filtración de datos de caza mayor (BGH), lo que demuestra el estado de caza mayor como la amenaza de crimen electrónico más importante para las organizaciones que abarcan regiones e industrias.

Intrusiones interactivas por Región

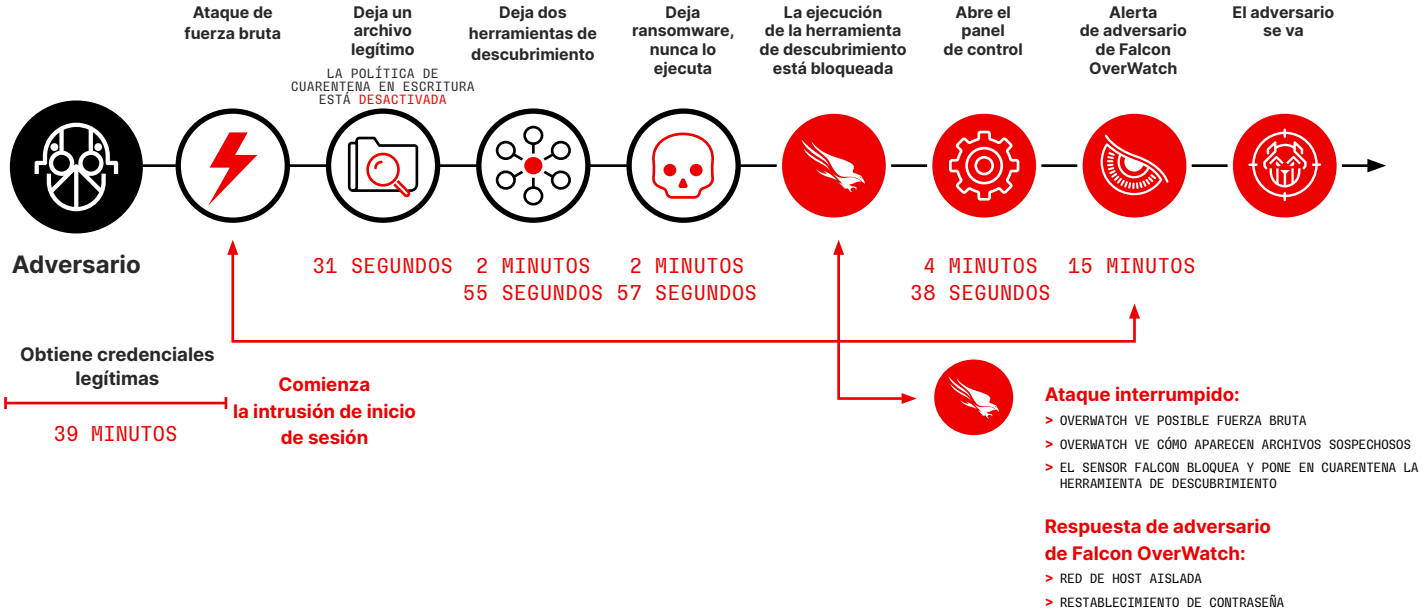


Intrusiones interactivas por Industria



ANATOMÍA DE UN CRIMEN ELECTRÓNICO

INTRUSIÓN INTERACTIVA



En un ataque, que se muestra en la figura anterior, el equipo de seguridad tenía deshabilitada la configuración de política “cuarentena en escritura”, lo que permitió que cuatro archivos se escribieran en el disco. El adversario ejecutó una herramienta legítima para obtener información del sistema con fines de reconocimiento y, a continuación, dejó tres archivos más, entre ellos ransomware, en el sistema. Intentaron ejecutar una herramienta de descubrimiento y reconocimiento de redes para mapear las opciones de movimiento lateral, que fue inmediatamente bloqueada y puesta en cuarentena por el Sensor Falcon. Esto provocó que el adversario abriera el panel de control para comprender qué herramienta de seguridad estaba en uso. Cuando identificaron la plataforma Falcon, nunca intentaron ejecutar la segunda herramienta de descubrimiento o el ransomware (que se habría evitado y puesto en cuarentena) y se trasladaron a otra víctima. En cuestión de minutos, el equipo de threat hunters de CrowdStrike CAO notificó al cliente, desconectó la máquina y restableció la contraseña del usuario.

Una vez que se produce una afectación inicial, los adversarios solo tardan unos segundos en dejar herramientas o malware en el entorno de la víctima durante una intrusión interactiva. Sin embargo, el dicho “el tiempo es oro” es válido para los adversarios. Más del 88 % del tiempo de ataque se dedicó a irrumpir y obtener acceso inicial. Al reducir o eliminar este tiempo, los adversarios liberan recursos para llevar a cabo más ataques.

ACTIVIDAD LIBRE DE MALWARE

»

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

Temas Clave

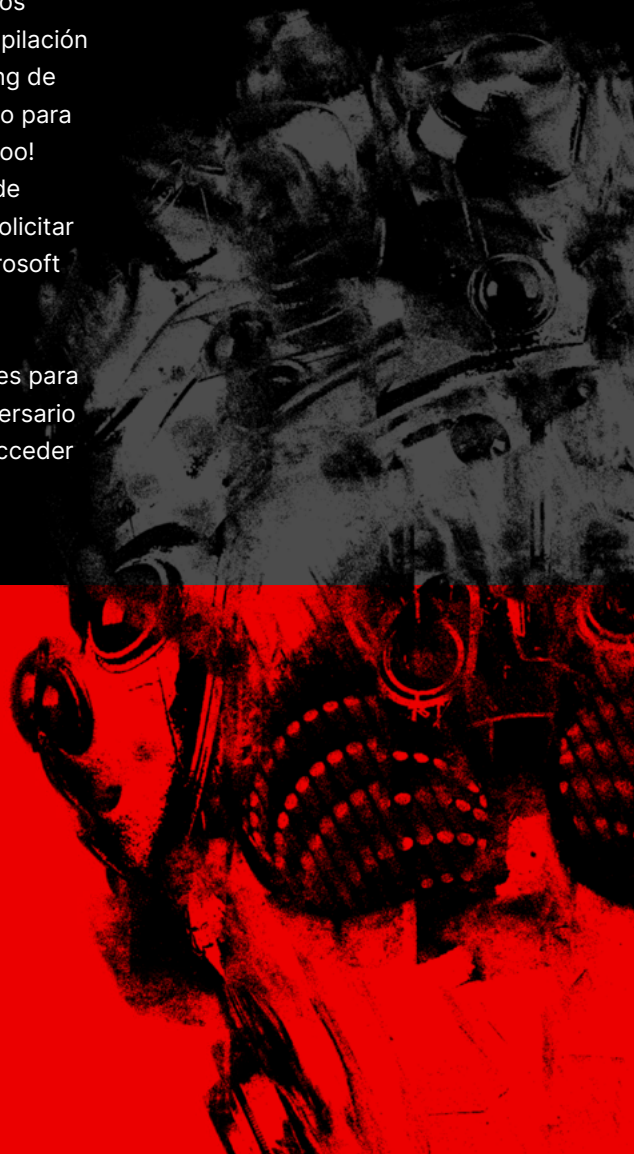
Ataques basados en la identidad y de ingeniería social

Los adversarios que abarcan múltiples regiones y motivaciones continúan utilizando técnicas de phishing suplantando la identidad de usuarios legítimos para enfocarse en cuentas válidas, junto con otros datos de autenticación e identificación,a fin de llevar a cabo sus ataques.

- Además de robar las credenciales de la cuenta, CrowdStrike CAO observó que los adversarios tenían por objetivo las claves de API y secretos, las cookies y tokens de sesión, las contraseñas de un solo uso y los tickets de Kerberos a lo largo del 2023.

- Estos ataques son comunes tanto entre los adversarios de los Estados nación como entre los cibercriminales. En el frente de los Estados nación, FANCY BEAR llevó a cabo campañas periódicas de recopilación de credenciales a lo largo del 2023. En las campañas de phishing de credenciales, desarrollaron un kit de herramientas personalizado para capturar las credenciales de los usuarios de correo web de Yahoo! Mail y ukr.net. COZY BEAR llevó a cabo campañas de phishing de credenciales utilizando mensajes de Microsoft Teams a fin de solicitar tokens de autenticación multifactor (MFA) para cuentas de Microsoft 365.

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

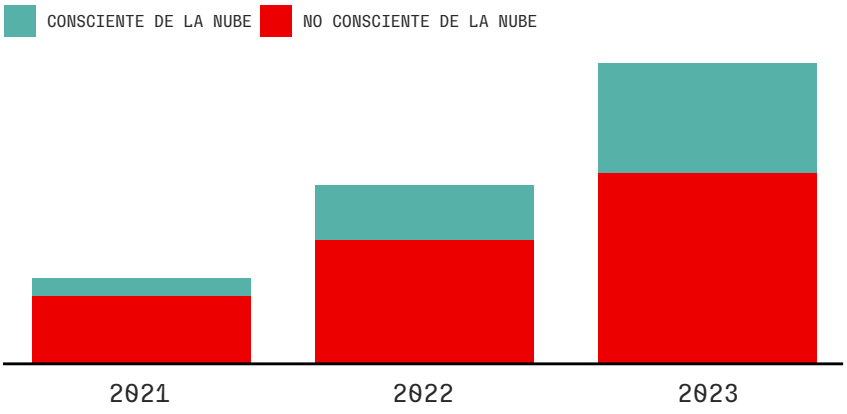


Los adversarios continúan desarrollando la conciencia a la nube

Como se predijo, la nube continuó demostrando ser un campo de batalla en evolución para la actividad de los adversarios en el 2023. CrowdStrike CAO observó un aumento del 110% en los casos conscientes de la nube, en los que los adversarios eran conscientes de que habían accedido a un entorno en la nube y utilizaban este acceso para abusar del servicio en la nube, y un aumento del 60% en los casos no conscientes de la nube. Los actores de ciberamenazas involucrados en casos no conscientes de la nube no sabían que afectaban un entorno de la nube o no aprovecharon las características específicas de la nube.

- SCATTERED SPIDER impulsó predominantemente los aumentos en la actividad consciente de la nube durante el 2023, lo que representó el 29% del total de casos. El adversario demostró una estrategia progresiva y sofisticada en los entornos de la nube específicos para mantener la persistencia, obtener credenciales, moverse lateralmente y exfiltrar datos.
- Los adversarios del crimen electrónico fueron especialmente activos a la hora de enfocarse en los entornos en la nube: el 84% de las intrusiones conscientes de la nube atribuidas a los adversarios fueron realizadas por probables cibercriminales.
- La preferencia de los adversarios por las técnicas basadas en la identidad es evidente en sus ataques centrados en la nube. A menudo usan credenciales válidas para lograr el acceso inicial a los entornos en la nube, lograr la persistencia en el nivel de identidad y escalar privilegios mediante la obtención de acceso a identidades adicionales.

INCIDENTES EN LA NUBE



▲ 110% CASOS CONSCIENTES DE LA NUBE

LOS ACTORES SON CONSCIENTES DE QUE OBTUVIERON ACCESO A UN ENTORNO EN LA NUBE PROPIEDAD DE LA VÍCTIMA Y UTILIZAN SU ACCESO PARA ABUSAR DEL SERVICIO EN LA NUBE PROPIEDAD DE LA VÍCTIMA

▲ 60% CASOS NO CONSCIENTES DE LA NUBE

LOS ACTORES NO ERAN CONSCIENTES DE QUE HABÍAN AFECTADO UN ENTORNO EN LA NUBE O NO APROVECHARON LAS FUNCIONES DE LA NUBE

↑75%
INTRUSIONES EN LA NUBE

Explotación de relaciones con terceros

A lo largo del 2023, los actores de intrusión selectiva intentaron explotar constantemente las relaciones de confianza para obtener acceso inicial a las organizaciones. Este tipo de ataque aprovecha las relaciones proveedor-cliente a fin de desplegar herramientas maliciosas utilizando dos técnicas clave: una implica afectar la cadena de suministro de software utilizando software confiable para distribuir herramientas maliciosas; el otro consiste en aprovechar el acceso a los proveedores que suministran servicios de TI.

- Los adversarios que apuntan a las relaciones con terceros están motivados por el retorno potencial de la inversión: una organización afectada puede conducir a cientos o miles de objetivos de seguimiento.

- En el 2023, los adversarios vinculados con China se enfocaron cada vez más en las relaciones con terceros para desplegar implantes maliciosos y obtener acceso inicial. JACKPOT PANDA y CASCADE PANDA explotaron constantemente las relaciones de confianza a través de afectaciones de la cadena de suministro y ataques de actores en el lado o actores en el medio.

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

Panorama de vulnerabilidades: explotación desapercibida

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

- Los dispositivos de red no gestionados, en particular los dispositivos de puerta de entrada periférica, siguieron siendo el vector de acceso inicial para la explotación más observado de forma rutinaria en el 2023.

- Los actores de ciberamenazas están desarrollando exploits para productos al final de su vida útil que no se pueden parchear y, a menudo, no permiten el despliegue de sensores modernos. Los servidores de sistemas operativos no compatibles y los dispositivos de puerta de entrada tradicionales ofrecen un fácil acceso, incluso a familias de malware más antiguas, lo que conduce a infecciones persistentes.

Conflicto entre Israel y Hamás 2023: las operaciones cibernéticas se centran en la disrupción y la influencia

CrowdStrike CAO ha rastreado las operaciones cibernéticas en curso de actores de intrusión selectiva y hacktivistas desde el inicio del conflicto entre Israel y Hamás en el 2023. La actividad y las afirmaciones de ambos tipos de actores de ciberamenazas se centran principalmente en atacar la tecnología operativa u otros sistemas esenciales, que es probable que influyan de manera psicológica en las poblaciones objetivo, y en desplegar wipers destructivos contra Israel o entidades vinculadas a Israel.

- CrowdStrike CAO rastrea a múltiples 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 de conflicto.
- RENEGADE JACKAL fue el adversario más activo vinculado con Hamás durante el 2023. Los probables adversarios con sede en Gaza evaluados por CrowdStrike CAO EXTREME JACKAL y RENEGADE JACKAL 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 realiza con un alto grado de confianza en función de los patrones de actividad exhibidos hasta la fecha.

PERSPECTIVA PARA EL 2024

A medida que las organizaciones planifican las posibles amenazas que surgirán en el 2024, dos posibles impulsores de la interrupción son los más destacados: la IA generativa y las elecciones gubernamentales globales del 2024

El uso de la IA generativa en el panorama de amenazas

La IA generativa ha democratizado enormemente la computación para mejorar las operaciones de los adversarios. También puede reducir potencialmente la barrera de entrada al panorama de amenazas para los actores de ciberamenazas menos sofisticados.

Entre las principales áreas de oportunidad de la IA generativa en el panorama de amenazas se encuentran dos:

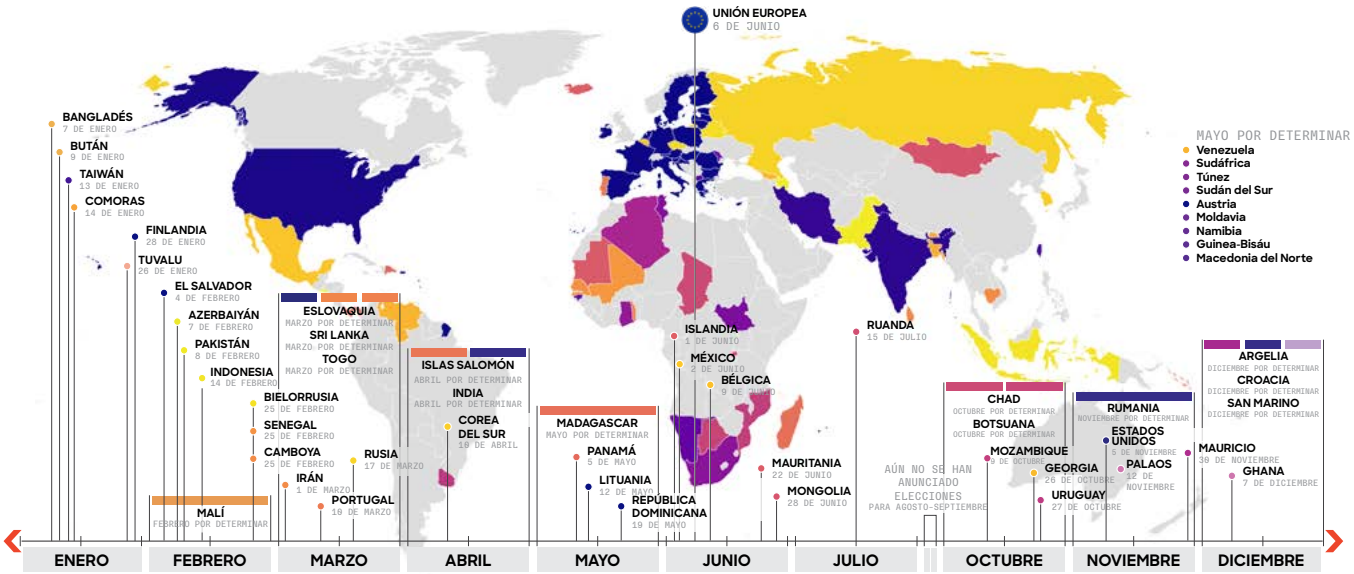
- Desarrollar o ejecutar operaciones maliciosas de redes informáticas (CNO), incluido el desarrollo de herramientas y recursos, como scripts o código, que podrían ser funcionalmente maliciosos si se utilizan de manera correcta.
- Apoyar la eficiencia y eficacia de las campañas de ingeniería social y operaciones de información (IO)

CrowdStrike CAO evalúa que es probable que la IA generativa se utilice para actividades cibernéticas en el 2024 a medida que continúe ganando popularidad. Durante el 2024, el equipo hará un seguimiento de cómo los actores de ciberamenazas utilizan esta tecnología y cómo difiere de las aplicaciones convencionales.

Elecciones del 2024

Personas de 55 países que representan más del 42% de la población mundial participarán en elecciones presidenciales, parlamentarias o generales. Esto incluye a 7 de los 10 países más poblados del mundo. También se celebrarán elecciones nacionales en países o grupos implicados en conflictos geopolíticos importantes o cercanos a ellos.

Históricamente, las actividades maliciosas más comunes que tienen por objetivo a las elecciones han involucrado IO, que es probable que realizadas por entidades vinculadas con el Estado contra ciudadanos de países que tienen un interés geopolítico específico para el actor de ciberamenazas y hacktivismo simple y de corta duración, incluidos ataques de denegación de servicio distribuidos (DDoS) y desfiguraciones de sitios web, contra entidades gubernamentales estatales y locales. Es muy probable que esta tendencia continúe en el 2024. Es probable que los países de interés involucrados en ciclos electorales corran el riesgo de sufrir campañas de IO significativas y prolongadas por parte de las principales potencias mundiales.

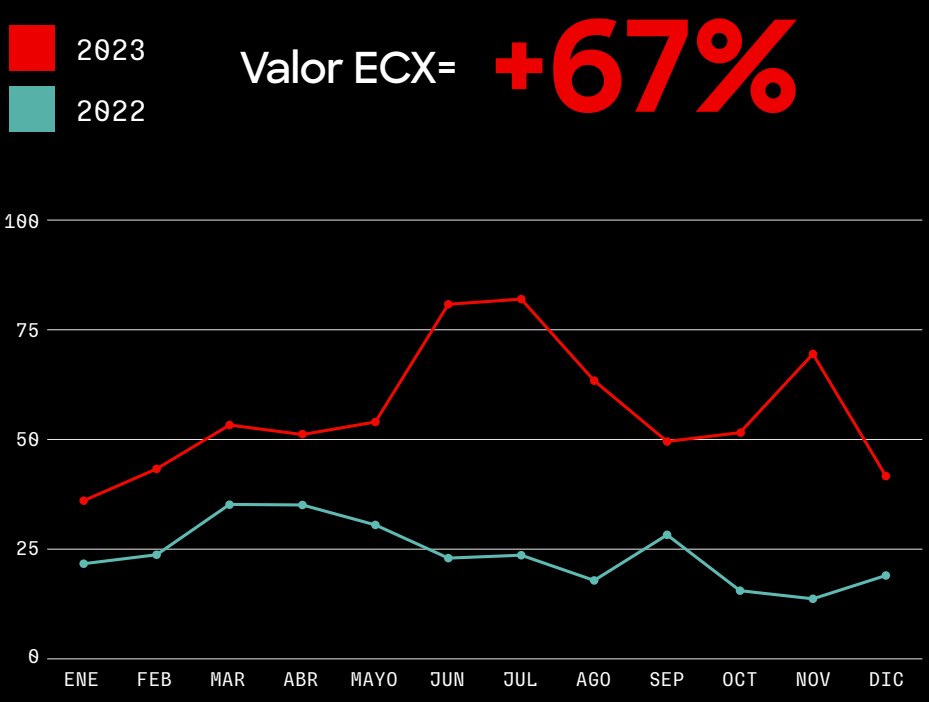


PANORAMA DEL CRIMEN ELECTRÓNICO

El Crimen electrónico Index® de CrowdStrike (ECX) rastrea la actividad, incluido el número de correos electrónicos no deseados observados y el costo promedio de comprar acceso a una red corporativa, en múltiples segmentos del ecosistema de crimen electrónico y calcula el número total de víctimas de ransomware observadas.

Hasta mayo del 2023, el ECX exhibió tendencias similares a las observadas en el 2022. Sin embargo, a partir de junio del 2023, el ECX creció significativamente, con aumentos importantes entre junio y agosto. Los factores que más contribuyeron a estos aumentos fueron la alta frecuencia de incidentes de caza mayor y un aumento repentino de los ataques de denegación de servicio distribuido (DDoS) observados.

El ECX volvió a dispararse en noviembre del 2023, lo que refleja el aumento del número de correos electrónicos no deseados y el aumento del precio promedio de los cargadores y ladrones.



El ECX del 2023 registró la mayor actividad anual hasta la fecha, lo que representa el crecimiento interanual del índice. Es probable que los correos electrónicos no deseados disminuyeran en el 2023 a medida que los adversarios buscaban otros medios de acceso inicial y después de que una operación multinacional cerrara el QakBot de MALLARD SPIDER.

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

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

Incidentes de caza mayor que involucran filtraciones de datos
+76%

Costo promedio del cargador
+169%

Costo promedio del crypter
+250%

Costo promedio del ladrón
+286%

Demanda promedio de rescate
-27%

Correos electrónicos no deseados identificados
-15%

Caza mayor

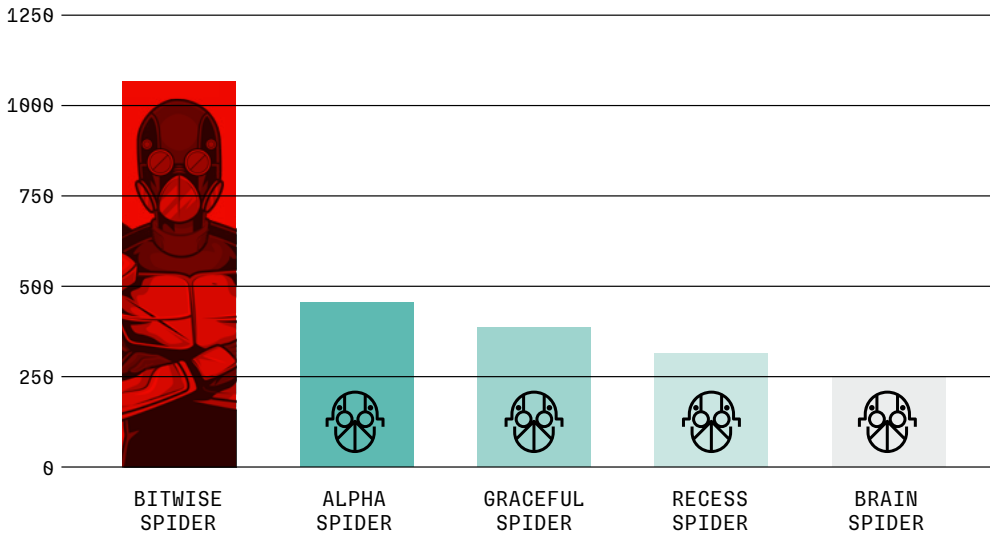
El número de víctimas nombradas en los sitios específicos de filtración de datos de caza mayor aumentó significativamente en el año pasado, con 4615 publicaciones de víctimas realizadas en un sitio específico de filtración de datos, un aumento del 76% con respecto al 2022. Varios factores contribuyeron a este crecimiento, incluidos los nuevos adversarios de caza mayor, el crecimiento de las operaciones de los adversarios existentes y algunas campañas de gran volumen, como las múltiples explotaciones de día cero de GRACEFUL SPIDER.

En conjunto, BITWISE 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 el 2022 y el 2023.

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

GRACEFUL SPIDER, que ha operado desde el 2016 y generalmente ha realizado campañas de bajo volumen, explotó tres vulnerabilidades de día cero en el 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 publicación de DLS



EL NÚMERO DE VÍCTIMAS NOMBRADAS EN LOS SITIOS ESPECÍFICOS DE FILTRACIÓN DE DATOS DE CAZA MAYOR AUMENTÓ SIGNIFICATIVAMENTE EN EL 2023, CON 4615 PUBLICACIONES DE VÍCTIMAS REALIZADAS EN UN SITIO ESPECÍFICO DE FILTRACIÓN DE DATOS, UN AUMENTO DEL 76% CON RESPECTO AL 2022.

RECOMENDACIONES

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

Hacer de la protección de la identidad algo imprescindible

Los ataques basados en la identidad y la ingeniería social dieron forma al panorama de amenazas en el 2023. Para contrarrestar estas amenazas, es esencial implementar la autenticación multifactor (MFA) y extenderla a los sistemas y protocolos tradicionales, educar a los equipos en ingeniería social e implementar tecnología que pueda detectar y correlacionar amenazas en entornos de identidad, endpoint y nube. La visibilidad y la aplicación entre dominios permiten a los equipos de seguridad detectar el movimiento lateral, obtener una visibilidad completa de la ruta de ataque y cazar el uso malicioso de herramientas legítimas. Abordar los métodos de acceso sofisticados, como el intercambio de SIM, la omisión de MFA y el robo de claves de API, cookies de sesión y tickets de Kerberos, requiere una cacería continua de comportamientos maliciosos.

Priorizar las plataformas de protección de aplicaciones nativas para la nube (CNAPP)

Las empresas necesitan una visibilidad completa de la nube para eliminar configuraciones erróneas, 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 mapear tus aplicaciones y API que se ejecutan en producción, lo que te muestra todas las superficies de ataque, amenazas y riesgos comerciales graves.

Obtener visibilidad de las áreas más esenciales 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 obtener una visibilidad completa en una sola vista y controlar fácilmente sus operaciones, mejorando su capacidad para descubrir, identificar y detener los ataques.

Impulsar la eficiencia

Los adversarios son cada vez más rápidos. ¿Puedes seguirles el ritmo? Las soluciones tradicionales de Información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés) suelen ser demasiado lentas, complejas y costosas, y muchas se diseñaron para una época en la que los volúmenes de datos y la sofisticación de los adversarios eran 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 nativa de IA ofrecida por la nube.

Construir una cultura de ciberseguridad

El usuario final sigue siendo un eslabón crucial en la cadena para detener los ataques. Se deben realizar programas de sensibilización de los usuarios para combatir la amenaza continua del phishing y otras técnicas de ingeniería social relacionadas. Para los equipos de seguridad, la práctica hace al maestro. Fomenta un entorno que realice rutinariamente ejercicios de simulación y de equipos rojo/azul para identificar brechas y eliminar las debilidades en sus prácticas y respuestas de ciberseguridad.

DESCARGAR EL INFORME COMPLETO

El Informe Global de Amenazas de CrowdStrike del 2024 presenta un análisis profundo que destaca los eventos y tendencias más significativos en las actividades de amenazas cibernéticas en el 2022. Descarga una copia gratuita del informe en https://www.crowdstrike.com/global-threat-report/.

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), es un líder global en ciberseguridad que ha redefinido la seguridad moderna con una de las plataformas nativas para la nube más avanzadas del mundo para proteger áreas críticas de riesgo corporativo — endpoints y workloads de nube, identidad y datos.

Impulsado por CrowdStrike Security Cloud™ y una Inteligencia Artificial de clase mundial, la plataforma CrowdStrike Falcon® aprovecha indicadores de ataque en tiempo real, inteligencia sobre amenazas, el tradecraft cambiante de los adversarios y telemetría enriquecida de toda la empresa para ofrecer detecciones hiper precisas, protección y remediación automatizadas, cacería de amenazas de élite y observabilidad priorizada de vulnerabilidades.

Construida para ese fin en la nube con una arquitectura única y liviana de agente, la plataforma Falcon entrega implantación rápida y escalable, protección y desempeño superiores, complejidad reducida y un tiempo de valor inmediato.

CrowdStrike: Detenemos los ataques.

Obtén más información en: www.crowdstrike.com

Síguenos: Blog | X | LinkedIn | Facebook | Instagram

Me gustaría comenzar una prueba gratuita: www.crowdstrike.com/free-trial-guide