



# 2023 GLOBAL THREAT REPORT

Adversarios implacables cada vez más rápidos y sofisticados en 2022: **lo que debes saber**

El informe CrowdStrike 2023 Global Threat Report, uno de los análisis más completos y fiables del sector sobre el panorama de las amenazas y las nuevas tácticas de los atacantes en la actualidad, analiza las tendencias más significativas de 2022 y describe a los ciberdelincuentes responsables.

## CONOCE A TU ENEMIGO

CIBERDELINCUENTES | FINANCIADOS POR ESTADOS | HACKTIVISTAS



**33** nuevos adversarios identificados en 2022

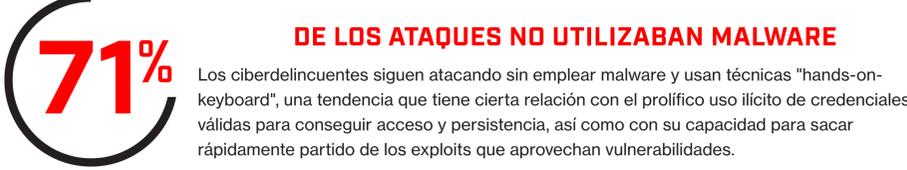
**200+** adversarios bajo vigilancia

## DÓNDE ACTÚAN



## CÓMO FUNCIONAN

El panorama de las amenazas siguió evolucionando en 2022 y para las organizaciones es cada vez más difícil defenderse de las acciones de los ciberdelincuentes.



**PROLIFERAN LOS ANUNCIOS DE INTERMEDIARIOS DE ACCESO, CON UN AUMENTO DEL 112 %**

La popularidad de los servicios de intermediarios de acceso aumentó en 2022. Se identificaron más de 2500, lo que representa un incremento respecto a 2021. Esto pone de manifiesto la creciente demanda de este tipo de servicios.



## CUÁL ES SU OBJETIVO

Los ciberdelincuentes atacaron sin tregua para conseguir acceso a los datos y la infraestructura de las víctimas en 2022.



**CONTINUÓ LA TENDENCIA DE LAS CAMPAÑAS DE EXTORSIÓN Y ROBO DE DATOS; SIN RANSOMWARE**

CrowdStrike Intelligence observó un incremento del 20 % en el número de campañas de extorsión y robo de datos, sin el empleo de ransomware. Este modelo de "doble extorsión" es la táctica más habitual entre los adversarios calificados como "big game hunters (BGH)", o de caza mayor.

**EL APROVECHAMIENTO REPETIDO DE VULNERABILIDADES PONE EN RIESGO LOS COMPONENTES EXPUESTOS**

Las vulnerabilidades desconocidas (de día cero/zero-day) y conocidas (de día N/N-day) observadas en 2022 han demostrado la capacidad del adversario para utilizar conocimientos especializados que le permiten sortear las medidas de mitigación de parches anteriores y atacar varias veces los mismos componentes vulnerables.

**LOS ADVERSARIOS LIGADOS A CHINA, ENTRE LOS GRUPOS RESPONSABLES DE INTRUSIONES SELECTIVAS MÁS ACTIVOS**

En 2022 se observó cómo ciberdelincuentes ligados a China, así como los adversarios (TTP) que empleaban tácticas, técnicas y procedimientos (TTP) que conueneban con las usadas generalmente por este grupo, dirigían ataques contra casi la totalidad de los 39 sectores a nivel mundial y las 20 zonas geográficas que sigue CrowdStrike Intelligence.

**PERSISTEN LOS ATAQUES MILITARES, PSICOLÓGICOS Y DE HACKTIVISMO DE ADVERSARIOS LIGADOS A RUSIA CONTRA UCRANIA**

A lo largo de 2022, se ha observado un uso sin precedentes de ciberestrategias destinadas a recopilar inteligencia, destruir infraestructuras o fomentar la división, así como influir en la opinión pública, en toda Europa.



En 2022 se observó cómo ciberdelincuentes ligados a China, así como los adversarios (TTP) que empleaban tácticas, técnicas y procedimientos (TTP) que conueneban con las usadas generalmente por este grupo, dirigían ataques contra casi la totalidad de los 39 sectores a nivel mundial y las 20 zonas geográficas que sigue CrowdStrike Intelligence.

## ¿Y AHORA QUÉ?

Todo es posible. Para prepararte, necesitas:

- > Conocer a tu enemigo
- > Priorizar la protección de identidades
- > Aplicar parches en los componentes vulnerables
- > Practicar el ataque:

**Estar preparado para cuando cada segundo cuenta**



**Solo hay una forma de derrotarlos: conocer sus tácticas.**

### Acerca de CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), un líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo. Para proteger a los aspectos fundamentales del riesgo y a una excelente inteligencia de trabajo en endpoints y la nube, la identidad y los datos. Gracias a la agilidad de CrowdStrike Falcon y a una excelente inteligencia de trabajo en endpoints, la plataforma CrowdStrike Falcon® se nutre de indicadores de ataque en tiempo real, inteligencia sobre amenazas, distintas tácticas usadas por los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y corrección 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, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: **We stop breaches.**

Más información: <https://www.crowdstrike.es/>  
Síguenos:

Empieza una prueba gratuita hoy mismo: <https://www.crowdstrike.com/free-trial-guide/>  
© 2023 CrowdStrike, Inc. Todos los derechos reservados.