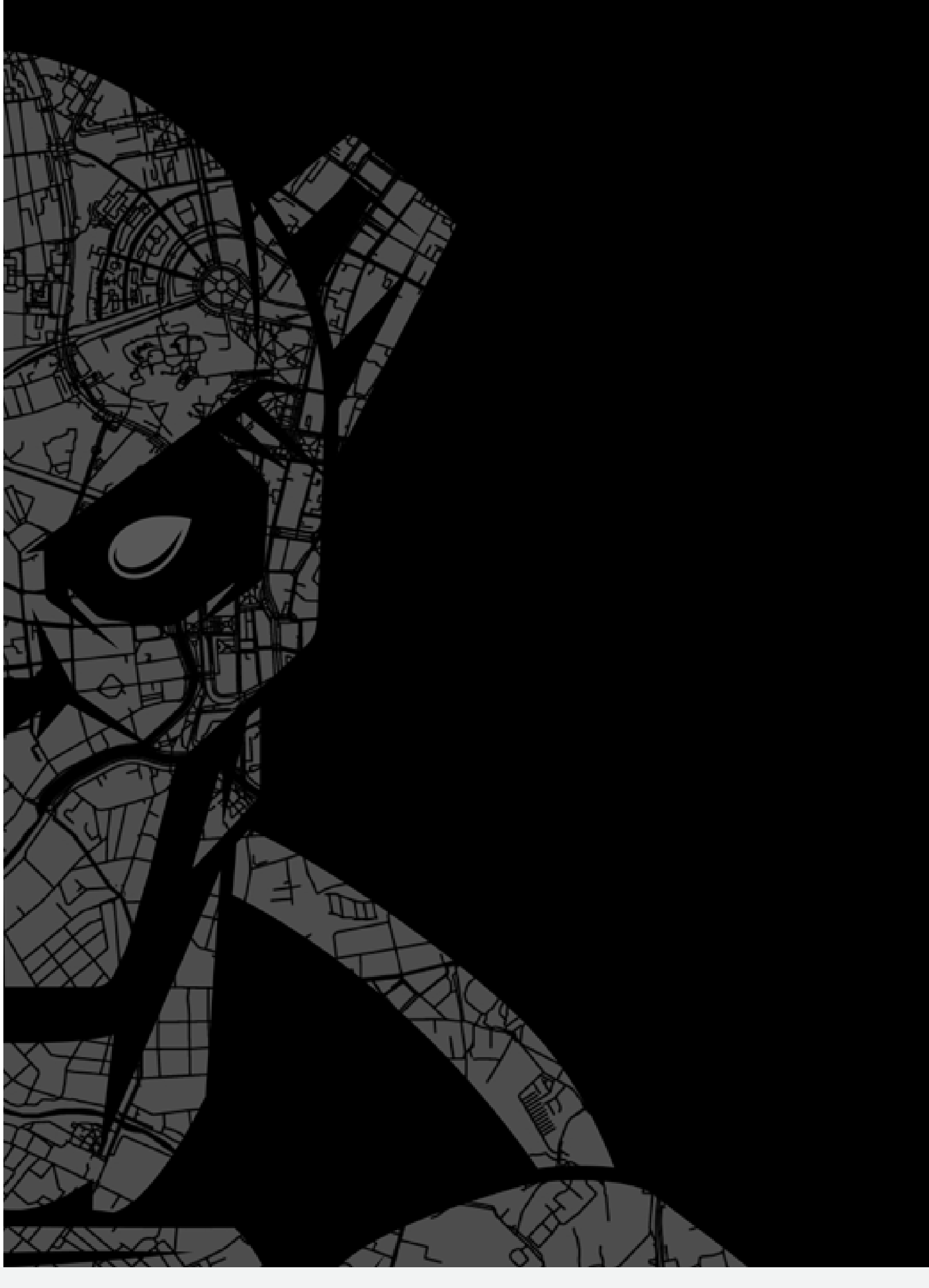
CROWDSTRIKE



2023 INFORME GLOBAL DE AMENAZAS

Adversarios implacables aumentan su velocidad y sofisticación en el 2022: **qué necesitas saber**

El Informe Global de Amenazas 2023,
uno de los análisis más fiables y completos de la industria
sobre el entorno de amenazas actuales y sobre las estrategias adversarias
en constante evolución, explora las tendencias más relevantes de 2022
y estudia a los adversarios por detrás de ellas.

CONOCE A TUS ADVERSARIOS

eCRÍMES | PATROCINADOS POR ESTADOS | HACKTIVISTAS

33 nombres de nuevos adversarios se presentaron en 2022

+ DE **200** adversarios rastreados

DÓNDE ESTÁN ACTIVOS

- Tecnología
- Servicios
- Servicios
- Telecomunicaciones
- Industria
- Universidades
- Gobierno

CÓMO OPERAN

El panorama de amenazas siguió evolucionando en 2022, con lo que las operaciones adversarias dificultaron cada vez más la protección de las organizaciones.

98'

84'

EL TIEMPO DE COMPROMETIMIENTO SIGUE ESTANDO POR DEBAJO DE DOS HORAS

Los adversarios de crimen electrónico necesitan un promedio de 1 hora y 24 minutos para moverse lateralmente, lo que constituye una disminución de 14 minutos comparado con 2021.

1'24"

71%

DE LOS ATAQUES FUERON SIN MALWARE

Los adversarios continúan avanzando más allá del malware y emplean técnicas de ataque interactivo, una tendencia relacionada, en parte, a su exitoso abuso de credenciales válidas para permitir el acceso y la persistencia, asi como su capacidad de accionar los exploits de vulnerabilidad con rapidez.

50%

DE AUMENTO EN LAS CAMPAÑAS DE INTRUSIÓN INTERACTIVA

CrowdStrike observó un aumento significativo de intrusiones interactivas, con un gran crecimiento de las actividades en el tercer trimestre de 2022.

LOS ANUNCIOS DE BROKERS DE ACCESO TUVIERON UN INCREMENTO DE 112%

La popularidad de los servicios de brokers de acceso aumentó en 2022: se identificaron más de 2500 anuncios de acceso, lo que constituye una pronunciada subida en comparación con 2021, recalcando la creciente demanda de estos servicios.

QUÉ ESTÁN BUSCANDO

Los adversarios fueron implacables al atacar la infraestructura y los datos de las víctimas en el 2022.

LOS INCIDENTES DE EXPLOTACIÓN DE LA NUBE CRECIERON 95%

En el trascurso del 2022, los casos en los que participaron agentes de amenazas conscientes de la nube casi se triplicaron en comparación con el 2021, lo que significa una tendencia más amplia de crímenes electrónicos y agentes de Estado-nación que adoptan conocimientos y técnicas para atacar entornos de nube.

LAS CAMPAÑAS DE ROBO DE DATOS Y EXTORSIÓN CONTINUARON —SIN EL RANSOMWARE

El equipo de inteligencia de CrowdStrike observó un incremento de 20% en el número de adversarios que realizaron robo de datos y extorsión sin desplegar ransomware. Este modelo de "extorsión doble" es la táctica más común entre los adversarios de caza mayor (BGH, big game hunting).

LA REUTILIZACIÓN DE VULNERABILIDADES PONE EN RIESGO LOS COMPONENTES EXPUESTOS

Las vulnerabilidades de Día Cero y Día N observadas en el 2022 demostraron la capacidad que tienen los adversarios de utilizar sus conocimientos especializados para eludir las mitigaciones de parches anteriores y atacar repetidas veces a los mismos componentes vulnerables.

LOS ADVERSARIOS VINCULADOS A CHINA FUERON LOS GRUPOS MÁS ACTIVOS DE INTRUSIÓN DIRIGIDA.

Se observó en el 2022 que los adversarios vinculados a China –y los agentes que utilizaban tácticas, técnicas y procedimientos (TTPs) consistentes con ellos– apuntaban a casi todos los 39 sectores globales de la industria y a las 20 regiones geográficas rastreadas por el equipo de inteligencia de CrowdStrike.

LOS ADVERSARIOS VINCULADOS A RUSIA CONTINUARON LOS ATAQUES MILITARES, PSICOLÓGICOS Y HACKTIVISTAS CONTRA UCRANIA

A lo largo de 2022, se observó el uso sin precedentes de capacidades cibernéticas con el objetivo de reunir inteligencia, destruir la infraestructura o sembrar la división, e influir en el sentimiento público que se difunde en Europa.

¿QUÉ VIENE A CONTINUACIÓN?

Todo. Para estar preparado, necesitas:

- Conocer a tus adversarios
- Priorizar la protección de la nube y de las identidades
- Parchear los componentes vulnerables
- Practicar tu lucha: **estar listo cuando cada segundo cuenta**

Descarga el informe

Comprender cómo juegan es la única manera de derrotarlos.

Acerca de CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder global en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa de la nube más avanzada del mundo para proteger áreas críticas de riesgo corporativo —endpoints y workloads de nube, identidades y datos. Impulsada por CrowdStrike Security Cloud y por inteligencia artificial de punta, la Plataforma CrowdStrike Falcon® potencia los indicadores de ataque en tiempo real, inteligencia contra amenazas, tareas adversarias en evolución, y telemetría optimizada de toda la empresa para ofrecer detecciones extremadamente precisas, protección y reparación automatizadas, cacería de amenazas superior y visibilidad prioritaria de vulnerabilidades. Construida para ese fin en la nube con una arquitectura única y liviana de agente, la plataforma Falcon entrega una implantación rápida y escalable, protección y desempeño superiores, complejidad reducida y un tiempo de amortización inmediato.

CrowdStrike: **Detenemos brechas**.

Más información: **https://www.crowdstrike.com/**

Síguenos:

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

CROWDSTRIKE
Protection that powers you