CROWDSTRIKE

NOWHERE TO HIDE

No tienes un problema de malware, tienes un problema de adversarios.

Es fundamental que los equipos de seguridad sepan cómo operan los actores para estar mejor posicionados para detenerlos.

El Informe de Cacería de Amenazas 2023 de CrowdStrike, desarrollado por el equipo de Counter Adversary Operations de CrowdStrike, expone el tradecraft más reciente de los adversarios y proporciona conocimientos e insights para ayudar a detener los ataques.

Nuevos insights impactantes

LAS AMENAZAS A LA IDENTIDAD SE HAN VUELTO COMUNES

Los adversarios están intensificando sus ataques basados en la identidad, siendo el robo y abuso de identidades afectadas la estrategia más impactante.

62%
de las intrusiones interactivas involucraron identidades afectadas

583%
de aumento in Kerberoasting, una creciente técnica de ataque basada en identidades

EL CRIMEN ELECTRÓNICO AUMENTA A MEDIDA QUE LOS ADVERSARIOS SE VUELVEN MÁS RÁPIDOS

Los adversarios entran y salen de los entornos más rápido que nunca.

79 MINUTOS
es el tiempo promedio de comprometimiento por crimen electrónico

7 MINUTOS
fue el tiempo de comprometimiento más rápido registrado para un crimen electrónico

LOS ADVERSARIOS SE ESTÁN VOLVIENDO GRANDES CONOCEDORES DE LA NUBE

Los actores se están convirtiendo en expertos en la nube: explotan errores de configuración comunes y abusan de las herramientas de gestión integradas en la nube.

160%
de aumento en el robo de credenciales mediante APIs de metadatos de instancias en la nube

LA COMPETENCIA EN MÚLTIPLES PLATAFORMAS TOMA PROTAGONISMO

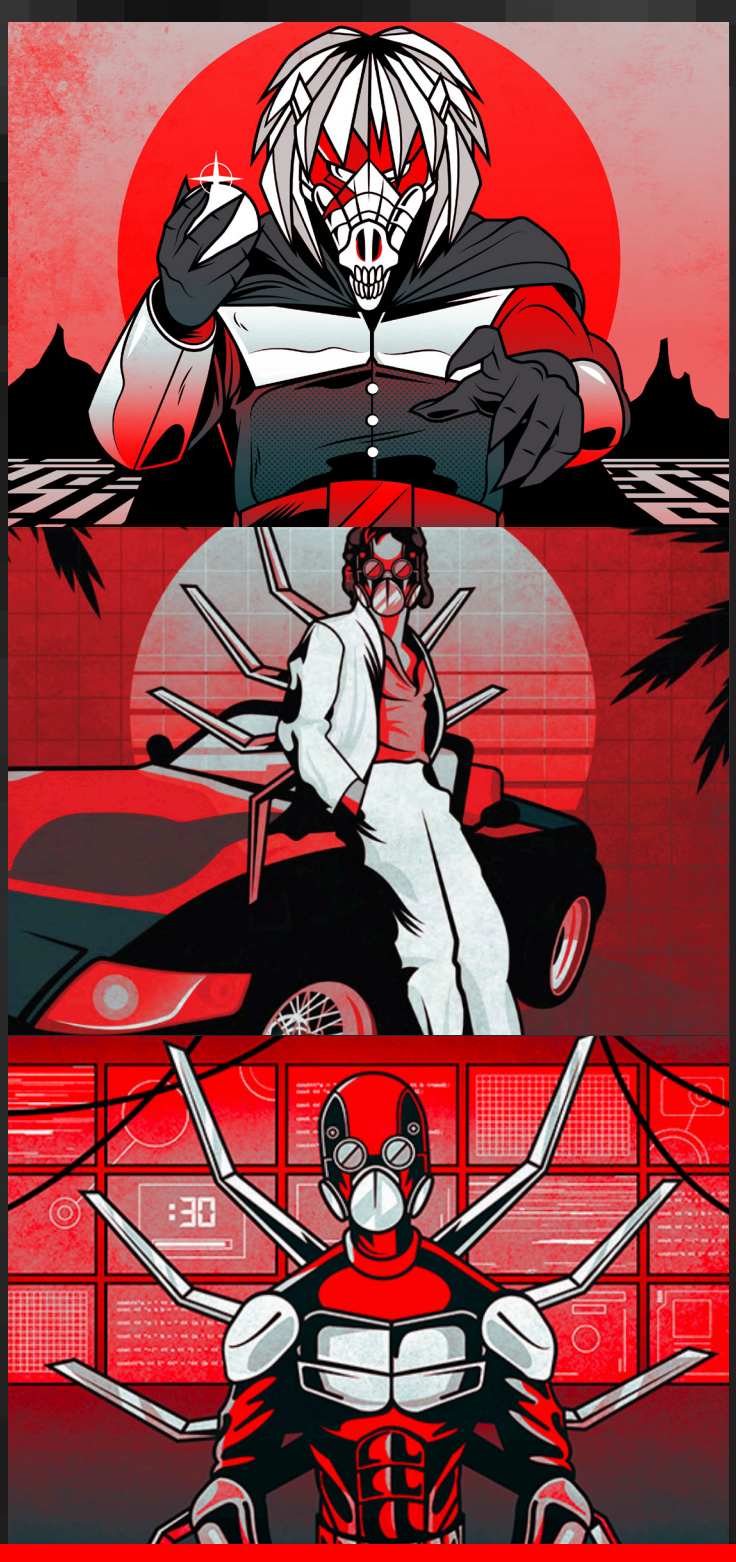
La competencia en todos los sistemas operativos es un rasgo distintivo de las intrusiones interactivas en 2023.

3X DE AUMENTO
en adversarios que reemplazan los módulos de autenticación enchufables (PAMs) por módulos maliciosos en Linux

FINANZAS, TECNOLOGÍA Y SERVICIOS
fueron las áreas más afectadas

Descubre qué adversarios te tienen por objetivo

CROWDSTRIKE ESTÁ SIGUIENDO ACTIVAMENTE A ESTOS ADVERSARIOS, JUNTO CON OTROS MÁS DE 200. OBTÉN MÁS INFORMACIÓN SOBRE ELLOS EN EL REPORTE THREAT HUNTING 2023.



LABYRINTH CHOLLIMA

Encabezó múltiples ataques en sistemas operativos

VICE SPIDER

Responsable del 27% de los ataques de Kerberoasting

INDRIK SPIDER

Pasó de crímenes electrónicos oportunistas a ataques personalizados

Quiénes son. **Dónde** están. **Cómo** detenerlos.

- Obtener insights incomparables de nuestros expertos del equipo de threat hunters mientras discuten las intrusiones y técnicas más destacadas.
- Equípate con experiencias del mundo real para fortalecer tu estrategia de seguridad y superar las amenazas que se mueven rápidamente.
- Mantenerte adelante de los adversarios entendiendo tanto las tendencias globales como regionales.

OBTENER INFORME

CROWDSTRIKE

© 2023 CrowdStrike, Inc. Todos los derechos reservados.