CROWDSTRIKE

2023 GLOBAL THREAT REPORT

DE ADVERSARIOS IMPLACABLES A NEGOCIOS RESILIENTES

RESUMEN EJECUTIVO

RESUMEN EJECUTIVO

El Informe Global de Amenazas de CrowdStrike está entre las investigaciones más fiables y amplias de la industria de ciberseguridad sobre el panorama actual de amenazas y sobre las estrategias adversarias en constante evolución. En sus páginas, exploramos los eventos de seguridad y las tendencias más relevantes del año anterior, además de estudiar a los adversarios por detrás de ellos.

El Informe Global de Amenazas de CrowdStrike 2023 investiga el pasado reciente de la actividad de los adversarios para que puedas prepararte mejor para futuros ataques. Al estudiar los detalles de estos eventos, obtienes visibilidad de la dinámica cambiante de las tácticas adversarias: qué se proponen, a quién apuntan y cómo operan.

El informe de este año se desarrolló en base a las observaciones de primera mano de nuestros equipos de élite de CrowdStrike® Intelligence y CrowdStrike® Falcon OverWatch™, combinados con información de la vasta telemetría de CrowdStrike Security Cloud. Proporciona información esencial sobre lo que los equipos de seguridad necesitan saber (y hacer) en un panorama de amenazas cada vez más preocupante.

DESCRIPCIÓN GENERAL DEL PANORAMA DE AMENAZAS

TÁCTICAS DE LOS ADVERSARIOS

71%	**2022**
62%	2021
51%	2020
40%	2019
39%	2018

Libre de Malware

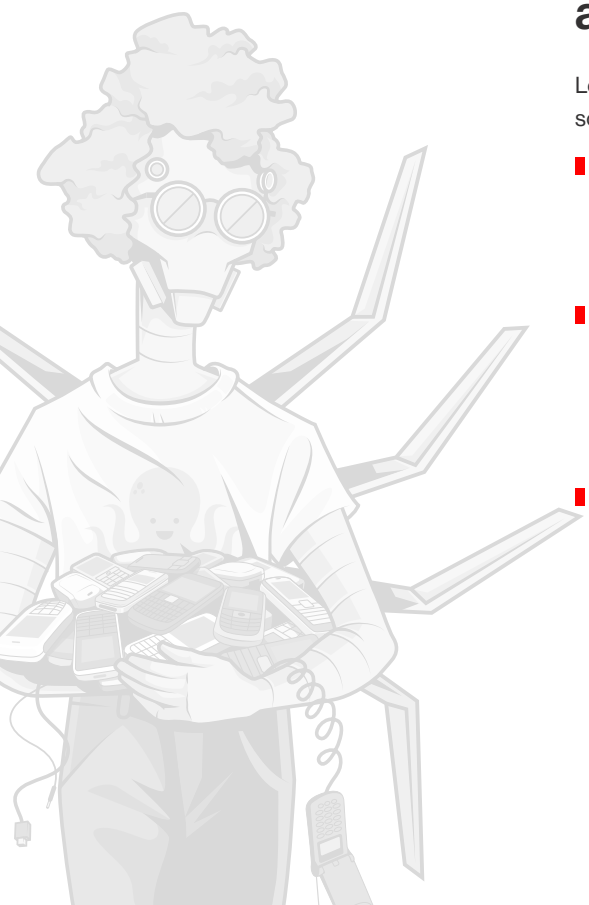
- **Disminuyó el tiempo de ruptura:** el equipo Falcon OverWatch calcula que el tiempo promedio de ruptura — el período que tarda un adversario en moverse lateralmente de un host comprometido a otro dentro del entorno de la víctima— fue de 84 minutos para la actividad de intrusión de crimen electrónico en el 2022.
- **Los servicios de bróker de acceso se hicieron más populares:** en 2022 se identificaron más de 2500 anuncios de servicios de bróker de acceso, que brindan o venden acceso ilícitamente adquirido a organizaciones. Esto marca un aumento del 112% con respecto a 2021. Una táctica muy utilizada involucró el abuso de credenciales comprometidas adquiridas a través de robo de información o compradas clandestinamente.
- **Los ataques libres de malware aumentaron:** las actividades libres de malware constituyeron 71% de todas las detecciones en el 2022, comparado a 62% en el 2021. Esto destaca un continuo alejamiento del uso de malware y una mayor dependencia del abuso de credenciales y de la explotación de vulnerabilidades entre los adversarios.
- **Las actividades hands-on-keyboard aumentaron:** el número de intrusiones interactivas aumentó 50% en 2022 con una actividad acelerada en el cuarto trimestre.

PRINCIPALES HALLAZGOS:

Los agentes de crimen electrónico ganaron notoriedad por ataques de alto perfil

Los adversarios están operando con una determinación incansable, lanzando ataques más sofisticados y frecuentes en una amplia gama de objetivos.

- A lo largo del año 2022, el equipo de inteligencia de CrowdStrike observó a dos adversarios con nuevos nombres, SLIPPY SPIDER y SCATTERED SPIDER, forzando los límites operativos al apuntar a víctimas de alto perfil e impactando a empleados asociados, clientes y socios.
- En su actividad durante el 2022, SLIPPY SPIDER atrajo gran atención debido a incidentes de robo y extorsión de datos de alto perfil dirigidos a empresas de tecnología. SCATTERED SPIDER aprovechó la ingeniería social para superar la autenticación multifactor (MFA). Ambos adversarios han utilizado con éxito una gama de técnicas que incluyen fatiga de MFA, vishing e intercambio de SIM.
- El equipo de inteligencia de CrowdStrike observó un incremento de 20% en el número de adversarios que realizaron campañas de robo de datos y extorsión, sin desplegar ransomware, en 2022.



El equipo de inteligencia de CrowdStrike observó que los adversarios se alejaron de la desactivación de tecnologías antivirus y firewall, así como de los esfuerzos de adulteración de registros. En cambio, se los observó buscando formas de modificar los procesos de autenticación y hacer ataques a identidades.

Aumento en la explotación de la nube

Los adversarios están cada vez más concentrando sus ataques en la nube y utilizan operaciones más avanzadas para el acceso inicial, el movimiento lateral posterior a la brecha, la escalada de privilegios, la evasión de defensa y la recopilación de datos.

- Los adversarios incrementaron la actividad centrada en la nube durante el 2022. Los casos observados de explotación de la nube crecieron un 95%, y los casos que involucraban a agentes de amenazas conscientes de la nube casi se triplicaron a partir del 2021. Este patrón significa una tendencia mayor de adversarios que adoptan el conocimiento y las herramientas que necesitan para apuntar a los entornos de nube.
- El equipo de inteligencia de CrowdStrike vio que los adversarios se alejaron de la desactivación de tecnologías antivirus y firewall, así como de los esfuerzos de manipulación de registro. En cambio, se les observó buscando formas de modificar los procesos de autenticación y las identidades de destino.
- Si bien los objetivos de las operaciones adversarias siguen siendo similares a sus ambiciones de intrusión fuera de la nube, la naturaleza efímera de algunos entornos de nube significa que pueden necesitar un enfoque más tenaz para tener éxito. Se espera que ese enfoque consciente de la nube continúe en el 2023.

Descubrimiento, redescubrimiento y evasión: se vuelven a usar las vulnerabilidades como armas

Los adversarios volvieron a explotar cada vez más las vulnerabilidades y se enfocaron en vectores y componentes de ataques establecidos. Hay dos maneras en que esto se puede desdoblar. Los agentes pueden modificar o volver a aplicar la misma explotación para atacar otros productos igualmente vulnerables; como alternativa, pueden identificar un objetivo potencial y enfocarse en estos componentes vulnerables conocidos, bien como eludir el parcheo explorando otros vectores de exploit.

- Las debilidades arquitectónicas en las tecnologías de Microsoft crean un riesgo sistémico para los clientes. La liberación de parches y mitigaciones no significa necesariamente que las organizaciones estén a salvo de los exploits de vulnerabilidad. La naturaleza notoria y prolongada de la explotación de Log4Shell fue el ejemplo más destacado de descubrimiento de vulnerabilidades en varios productos en 2022.
- Las vulnerabilidades de Día Cero y Día N observadas en el 2022 demostraron la capacidad de los adversarios de utilizar conocimientos especializados para eludir las mitigaciones de parches anteriores y apuntar a los mismos componentes vulnerables.
- A pesar de los parches iniciales y de los nuevos, la plataforma CrowdStrike Falcon® Intelligence Recon acompañó discusiones continuas sobre el Log4Shell en la clandestinidad criminal a lo largo del 2022, reflejando un interés constante en la explotación de Log4Shell.

Los adversarios vinculados a China aumentaron la escala operativa y dominaron el entorno de espionaje

Se observó que los adversarios vinculados a China 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.

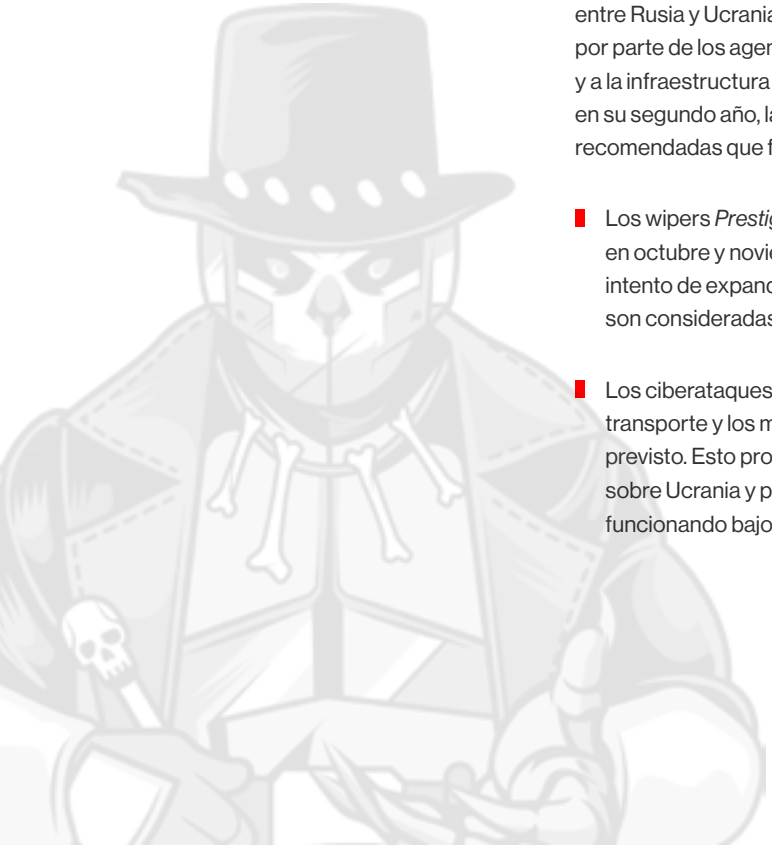
Si bien se asocien a menudo los agentes de amenazas vinculados a China con actividades dirigidas a los intereses regionales de naciones de Asia, Pacífico y Japón, y/o a los sectores industriales occidentales avanzados, su actividad se expandió enormemente en el 2022. Se observó que los adversarios vinculados a China 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.

- El equipo de inteligencia de CrowdStrike observó a agentes vinculados a China que apuntaban principalmente a organizaciones de tecnología con sede en Taiwán en el 2022. Esto tiene sentido considerando la probable misión de espionaje económico asociada con los agentes vinculados a China apoyando a los objetivos del PCCh de independencia y dominio tecnológico.

- En el 2022, se observaron exploits de Día Cero con más frecuencia en intrusiones que se dirigían a organizaciones con sede en Norteamérica. Los adversarios vinculados a China usaron esos exploits para afectar a instituciones en los sectores aeroespacial, jurídico y académico.

Operaciones cibernéticas rusas en Ucrania: impacto limitado, pero las amenazas continúan

La guerra en el territorio ha eclipsado hasta ahora los ciberataques previstos en el conflicto entre Rusia y Ucrania. Pese a los titulares osados y las narrativas políticas, aún no ha surgido por parte de los agentes vinculados a Rusia un ataque directo de ciberseguridad a los sistemas y a la infraestructura de los aliados. Sin embargo, en este momento en que la guerra entra en su segundo año, las organizaciones deben tomar precauciones y seguir las prácticas recomendadas que fueron discutidas en la iniciativa Shields Up de CISA.



- Los wipers *Prestige* y *RansomBoggs* , disfrazados de ransomware, fueron desplegados en octubre y noviembre del 2022. El cambio de Russia hacia ransomware falso sugiere un intento de expandir sus objetivos a sectores y regiones en que las operaciones destructivas son consideradas riesgosas políticamente.

- Los ciberataques contra sectores esenciales, como energía, telecomunicaciones, transporte y los medios de comunicación, no han sido tan difundidos como se había previsto. Esto probablemente indica que Rusia esperaba una victoria rápida y decisiva sobre Ucrania y planeaba utilizar estos activos funcionales para mantener a la nación funcionando bajo un nuevo régimen.

RECOMENDACIONES

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

01

Ten buena visibilidad de tus brechas de seguridad

Una organización solo es segura si todos los activos están protegidos. Mientras los adversarios continúan enfocando vulnerabilidades y utilizándolas como armas, los equipos de seguridad deben priorizar la visibilidad y el cumplimiento de la higiene de TI en todo el inventario de activos de la empresa.

02

Prioriza la protección de identidades

El aumento de los ataques libres de malware, ingeniería social e intentos parecidos para obtener acceso o credenciales lo ha dejado bastante claro: una solución tradicional apenas de endpoints no es suficiente. Encuentra soluciones que no solamente ayuden a extender la MFA a sistemas heredados y no administrados, sino que también brinden detección inmediata y prevención en tiempo real contra movimientos laterales, comportamientos sospechosos, uso indebido de cuentas de servicio y mucho más.

03

Prioriza la protección de la nube

Los adversarios están apuntando agresivamente a la infraestructura de la nube y utilizando una amplia gama de tácticas, técnicas y procedimientos —como configuraciones erróneas, robo de credenciales, etc.— para comprometer aplicaciones y datos corporativos críticos en la nube. Detener las brechas en la nube requiere capacidades sin agente para protegerse contra errores de configuración y ataques basados en el plano de control e identidades, bien como seguridad en tiempo de ejecución para proteger workloads en la nube.

04

Conozca a sus adversarios

Invierte en inteligencia de amenazas que va más allá de suministrar indicadores de compromiso (IOC). Asegúrate de que esa inteligencia también exponga a las personas por detrás del ataque, así como su motivación, sus capacidades y herramientas. Los equipos de seguridad pueden utilizar este conocimiento para hacer con que las defensas se dediquen a la acción.

05

La práctica hace la perfección

Si bien la tecnología es crítica en la lucha para detectar y detener las intrusiones, los equipos de seguridad son un eslabón esencial en la cadena para detener las brechas. Fomente 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.

DESCARGUE EL INFORME COMPLETO.

El Informe Global de Amenazas de CrowdStrike 2023 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/.