elastic security labs

2024

## Reporte de amenazas globales de Elastic

# Tendencias de amenazas que los líderes de SOC deberían saber

Diseñado para proporcionar información procesable tanto para los equipos de seguridad como para los CISO, el Reporte de amenazas globales de Elastic 2024 presenta los principales resultados de meses de análisis en más de mil millones de puntos de datos, cortesía de la telemetría pública y específica de Elastic. Estas conclusiones se han organizado en información de los datos y acciones sugeridas para tu organización.

## Principales perspectivas

### 01 Las empresas están configurando incorrectamente los entornos del cloud

Nuestra nueva sección sobre administración de postura de seguridad en cloud (CSPM) comparó los entornos con los puntos de referencia del Center for Internet Security (CIS) y encontró que, en promedio, en ~ 50 % de los entornos fallaron en las comprobaciones, independientemente del proveedor de servicios de cloud (CSP).

### 02 La evasión de la defensa sigue siendo la táctica más frecuente en los endpoints

La evasión de la defensa representó el 38 % de los comportamientos de los endpoints, lo que sugiere que los adversarios se sienten cómodos al navegar por los sistemas de seguridad. En particular, este número disminuyó un 6 % con respecto al año pasado, lo que pone de manifiesto que las herramientas de defensa están funcionando de manera efectiva.

### 03 Las alertas de acceso a credenciales siguen aumentando, en especial, dentro del cloud

Dentro de los entornos del cloud, el acceso a credenciales representó el 23 % de la actividad. Además, los entornos de endpoints revelaron un aumento del 3 % en estas técnicas de un año a otro. Esto se puede atribuir a la creciente prevalencia de ladrones de información y brokers de credenciales, así como al hecho de que las herramientas de seguridad tienen cada vez más visibilidad.

### 04 Los adversarios se abusan de las herramientas de defensa para entrar en los sistemas de manera eficiente

El 53 % de los archivos maliciosos observados se identificaron como herramientas de seguridad ofensivas, que las empresas aprovechan para descubrir debilidades y de los cuales se abusan los adversarios que los explotan. Estos OST tienen grandes equipos de investigación y desarrollo para crear nuevas capacidades, como la inyección de procesos, una forma de evasión de defensa que representó el 53 % de los eventos de alerta de Windows este año.

### 05 La IA generativa no aumentó la cantidad ni el impacto de los ataques que observamos

Los equipos de seguridad se preocuparon por una inminente avalancha de ataques de GenAI. Si bien observamos un pequeño aumento en el volumen de amenazas, GenAI reforzó en gran medida las tecnologías de defensa con capacidades tales como resumen de alertas y automatización de tareas.

# Sugerencias clave

## 01 Audita tu entorno con frecuencia

Los adversarios confían en los controles de seguridad permisivos o mal configurados para infiltrarse en los entornos, y, una vez dentro, se enfocan en manipular con sensores y datos. La evaluación comparativa y las evaluaciones de riesgos pueden ayudarte a identificar si estás usando las mejores prácticas y los estándares de la industria para controlar de manera efectiva el acceso dentro de tu empresa.

## 02 Prepárate para la IA generativa ajustando tus controles de seguridad

El aumento de la GenAI se traducirá en un repunte de los intentos de ingeniería social. Si bien siempre es una buena idea capacitar a tu base de usuarios para identificar estos intentos y más, los equipos de seguridad también deben verificar sus controles y permisos para asegurarse de que un intento de phishing exitoso no cause daños a largo plazo.

## 03 Implementa agentes de endpoints interactivos para neutralizar los ataques de evasión de defensa

Los ataques de evasión de defensa fueron la táctica principal durante algunos años. Aunque están disminuyendo, los adversarios siguen usando estos métodos para infiltrarse y navegar por los entornos. Las tecnologías de endpoint como Elastic Agent brindan visibilidad y capacidad, a la vez que reducen la cantidad de herramientas que necesitas.

## 04 Crea un plan de respuesta sólido para las credenciales expuestas

Observamos que periódicamente se usan técnicas como la fuerza bruta y el acceso a las credenciales del navegador desde la memoria sospechosa. Rotar las credenciales expuestas y organizar flujos de trabajo rápidos para responder a las violaciones marcará una gran diferencia. Los equipos de seguridad deben exigir la autenticación multifactor si aún no lo han hecho.

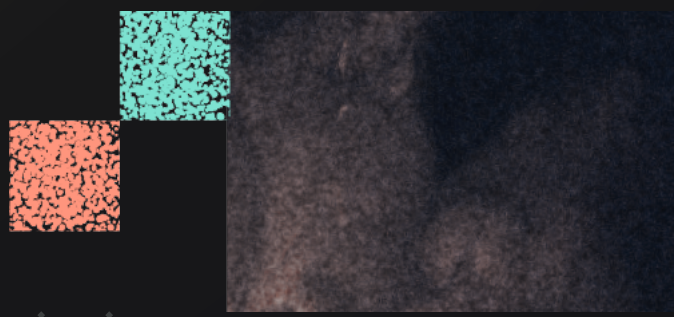
## 05 Compara tu entorno del cloud con los puntos de referencia de CIS

Los puntos de referencia de CIS son un estándar de la industria y te ayudarán a identificar rápidamente qué áreas necesitan atención. Tu equipo debe desarrollar un plan para monitorear y aumentar tu puntaje, lo que mejorará la detección de amenazas y reducirá el riesgo a largo plazo.

# Domina el panorama de las amenazas

Prepárate para la evolución de estas amenazas y más. Obtén todas nuestras sugerencias y observa el panorama completo de amenazas actuales en el Reporte de amenazas globales de Elastic 2024. También puedes seguir a nuestros expertos en @ElasticSecLabs.

Descubre cómo Elastic Security puede modernizar tus operaciones de seguridad.





elastic security labs