2025

elastic security labs

REPORTE DE INVESTIGACIÓN SOBRE AMENAZAS GLOBALES

RESUMEN EJECUTIVO

La era de los ataques pacientes y sigilosos está dando paso a una nueva era de amenazas de alta velocidad.

Nuestro análisis año tras año revela un claro cambio estratégico: los adversarios se están reorganizando para la velocidad, utilizando la IA como arma para generar nuevas amenazas a gran escala y priorizando la ejecución inmediata sobre el sigilo prolongado. Esta aceleración obliga a los defensores a adaptarse a un ciclo de vida de ataque medido en minutos, no meses, donde las decisiones rápidas y ricas en contexto extraídas de datos en tiempo real y datos históricos se han convertido en la clave para una defensa efectiva.

El 2025 Elastic Global Threat reporte de Elastic Security Labs desglosa este nuevo panorama.

Basándonos en nuestro análisis de la telemetría de amenazas globales, hemos identificado los comportamientos de los adversarios y las innovaciones defensivas más relevantes. Aquí tienes un adelanto de lo que aprenderás:

#01

Las prioridades de los adversarios en Windows cambiaron

La categoría táctica de **Ejecución** ahora representa el **32,1 %** del comportamiento malicioso, duplicando su participación anterior de ~16 %, y superando a **Evasión de Defensa** como la táctica principal. Esto interrumpe una tendencia de tres años e indica un cambio estratégico hacia el despliegue inmediato de la carga útil sobre el sigilo inicial.

2025 **32,1%**

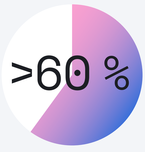
2024 ~16 %

QUÉ SIGNIFICA ESTO PARA TI

→ Los atacantes ya no esperan para esconderse; se enfocan en ejecutar código malicioso inmediatamente al entrar. Esto hace que la protección de la memoria en tiempo de ejecución y la prevención de acceso inicial sean más críticas que nunca.

#02

La superficie de ataque del cloud está altamente concentrada



Más del 60 % de todos los eventos de seguridad en cloud se reducen a solo tres objetivos del adversario:

objetivos del adversario

/Acceso inicial
/Persistencia
/Acceso a credenciales

QUÉ SIGNIFICA ESTO PARA TI

→ En todas las plataformas de cloud principales, este enfoque preciso en **los ataques basados en la identidad** es una señal clara de que el fortalecimiento de los flujos de autenticación y la supervisión del acceso privilegiado anómalo son las formas más efectivas de defender tus cargas de trabajo en el cloud.

#03

La militarización de la IA está en aumento

+15,5 %

Observamos un **aumento del 15,5 % en las amenazas "genéricas"**, una tendencia probablemente impulsada por adversarios que emplean LLMs para generar rápidamente cargadores y herramientas maliciosos simples pero efectivos.

QUÉ SIGNIFICA ESTO PARA TI

→ El aumento de las amenazas generadas por IA aumenta significativamente el volumen y la variedad de malware al que te enfrentas. Esto significa depender menos de firmas estáticas y más en **análisis de comportamiento y detección impulsada por IA** para identificar y detener automáticamente la avalancha de amenazas novedosas a gran escala.

#04

El robo de credenciales del navegador es un gran negocio

>1 de cada 8
diseñado para robar datos del navegador

Nuestro análisis de más de **150 000** muestras de **malware** reveló que **más de 1 de cada 8 está diseñado para robar datos del navegador**. Esto no es para uso aislado; estas credenciales son la materia prima que alimenta la **economía de broker de acceso**, proporcionando un suministro constante de claves para que otros atacantes comprometan las cuentas corporativas en el cloud.

QUÉ SIGNIFICA ESTO PARA TI

→ El navegador es un campo de batalla principal para los datos más confidenciales de tu organización. Los ladrones de información se han adaptado a las protecciones integradas del navegador, lo que significa que los controles de identidad tradicionales ya no son suficientes.

Estas tendencias están profundamente interconectadas.

Un adversario puede usar malware generado por IA para robar credenciales del navegador, que luego se usan para obtener acceso inicial a una cuenta en el cloud. Una vez dentro, se centran inmediatamente en la ejecución para desplegar ransomware o robar datos. Este reporte conecta los puntos, mostrando cómo estos TTP forman la cadena de ataque moderna y, lo que es más importante, cómo romperla en múltiples puntos.

El panorama de amenazas es complejo, pero al comprender los comportamientos de malware y amenazas y aprovechar las defensas avanzadas, las organizaciones pueden mejorar significativamente su resiliencia.

Paso n.° 1
céntrate en la ejecución

Paso n.° 2
consigue acceso inicial a una cuenta en el cloud

Paso n.° 3
usar malware generado por IA

Paso n.° 4
robar las credenciales del navegador

Elastic Security ofrece la inteligencia compartida, las capacidades avanzadas y la información que necesitas para atravesar las amenazas actuales y construir un futuro más seguro.