

# ¿Por qué el ransomware ataca los archivos compartidos antes de llegar a mi escritorio?

**Respuesta breve:** Cuando el ransomware infecta una estación de trabajo individual, esa máquina rara vez es el objetivo real. Los atacantes utilizan la infección inicial como punto de partida para alcanzar recursos de red compartidos, y solo cifran o dañan el escritorio local después de haber atacado ya datos de mayor valor en otros lugares.

## Por qué el escritorio es la última parada, no la primera

Un error común es pensar que, si el ransomware se instala en el equipo de un empleado en particular, los archivos de ese empleado son lo que persiguen los atacantes. En realidad, el malware está programado para ir más allá de la máquina local casi de inmediato. Una vez que obtiene acceso, comienza a escanear la red en busca de recursos accesibles de mayor valor, como servidores de archivos, wikis internas o bases de datos que contienen información de clientes. Cifrar o exfiltrar estos datos centralizados es el verdadero objetivo, ya que afecta a una parte mucho mayor de la organización que la carpeta de un solo usuario.

## La nota de rescate llega al final, no al principio

Debido a que los atacantes priorizan los datos de toda la red antes de tocar el dispositivo de origen, el empleado infectado suele ser la última persona en notar que algo anda mal. Para cuando aparece una nota de rescate en la pantalla de esa persona, los atacantes ya suelen haber terminado de cifrar o robar datos en gran parte de la infraestructura de la empresa. Esta secuencia es intencional. Permite a los atacantes infligir el máximo daño operativo antes de que alguien en la organización tenga la oportunidad de detectar la intrusión o responder a ella. La nota de rescate visible es, en esencia, una señal de que el daño más grave ya ha ocurrido entre bastidores.

## Qué significa esto para la defensa

Las fotos o documentos personales almacenados localmente en un escritorio suelen ser el objetivo menos importante en un ataque de ransomware, aunque puedan ser la señal más visible de uno. Una defensa eficaz debe tener en cuenta este patrón centrándose en detectar y detener la actividad maliciosa lo antes posible, antes de que pueda alcanzar los sistemas compartidos. FortressAI de Cyber Crucible está diseñado teniendo en cuenta esta secuencia de ataque, con el objetivo de intervenir en las primeras etapas de una intrusión en lugar de reaccionar únicamente cuando el cifrado se hace visible en máquinas individuales.

<https://player.vimeo.com/video/1043466243?texttrack=es>

[Ver en Vimeo](#) · Subtítulos: English, Français, Español, العربية

---

Revision #2

Created 2026-07-24 02:14:00 UTC by Dennis Underwood

Updated 2026-08-06 18:34:44 UTC by Dennis Underwood