¿Qué es un ataque sin archivos (en memoria)?

Respuesta breve: Un ataque sin archivos es aquel que nunca escribe un programa en el disco. El atacante inyecta código malicioso directamente en la memoria de un proceso legítimo y de confianza, y construye allí su carga útil (payload). Como nunca se crea ningún archivo, las herramientas de seguridad que analizan archivos —incluida la mayoría de EDR— no tienen nada que encontrar.

Por qué derrota a las herramientas basadas en archivos

La protección tradicional de endpoints se construye sobre una suposición simple: el malware es un archivo, así que hay que inspeccionar archivos. Las técnicas sin archivos eliminan por completo el archivo.

En una implementación real, una empresa de servicios financieros utilizaba tres productos EDR líderes en la industria (Microsoft, CrowdStrike y Sophos) junto con un SOC gestionado del Top 50. Los atacantes comprometieron una herramienta de monitoreo remoto de confianza, inyectaron código en los procesos de administración de Microsoft SQL Server y compilaron su ransomware y malware de robo de datos directamente en la memoria del servidor. Como nada tocó el disco duro, los tres EDR, el MDR y el SOC quedaron completamente ciegos. Cyber Crucible interceptó de forma autónoma casi 10,000 procesos maliciosos —el 98% de ellos en la granja de servidores SQL— sin una sola alerta de la pila de herramientas heredada.

Cómo lo ve Cyber Crucible

Cyber Crucible observa el comportamiento y la intención a nivel del kernel en lugar de analizar archivos. Un proceso que actúa de manera maliciosa se detiene en menos de 200 milisegundos, se haya escrito un archivo o no.

Revision #1
Created 2026-07-24 01:41:34 UTC by Dennis Underwood
Updated 2026-07-24 01:41:34 UTC by Dennis Underwood