

¿Por qué la protección de los datos de identidad requiere acceso a nivel de kernel?

Respuesta breve: Porque el robo ocurre en el espacio entre el momento en que un programa solicita datos de credenciales y el momento en que el sistema operativo los entrega. Solo una defensa que opera en el kernel —por debajo de las aplicaciones y bibliotecas que un atacante puede manipular— puede ver esa solicitud, evaluar su intención y detenerla a tiempo.

Los tres requisitos

1. Ver el acceso en el momento en que ocurre. El robo de identidad no es un archivo que aparece en el disco; es una lectura. Las herramientas que buscan archivos maliciosos no ven nada, porque en un infostealer moderno no se escribe nada. El evento que hay que detectar es el intento de acceso en sí.

2. Decidir con la suficiente rapidez. Las herramientas automatizadas pueden infiltrarse, recopilar datos y autoeliminarse en cuestión de segundos. Cualquier arquitectura que envíe telemetría a un servicio en la nube y espere un veredicto ya ha perdido la carrera. La decisión debe tomarse localmente, en milisegundos.

3. No depender de lo que el atacante controla. Las herramientas de seguridad que dependen de bibliotecas del sistema operativo pueden quedar ciegas cuando un atacante compromete esas bibliotecas en memoria: el agente sigue ejecutándose y no informa nada. Cyber Crucible fue deliberadamente desacoplado de las bibliotecas de Windows para que un sistema operativo comprometido no pueda silenciarlo.

La consecuencia

El funcionamiento a nivel de kernel es lo que permite las tres cosas a la vez: visibilidad sobre el intento de acceso, una decisión local en menos de 200 milisegundos, e independencia de un sistema operativo potencialmente comprometido.

Esto también explica por qué la protección funciona sin conectividad —en entornos con air gap, sin conexión, o en el mar— ya que no es necesario que nada salga del dispositivo para que se tome una decisión.

Revision #1

Created 2026-07-24 01:44:51 UTC by Dennis Underwood

Updated 2026-07-24 01:44:51 UTC by Dennis Underwood