¿Cómo protege Cyber Crucible a las empresas de servicios financieros?

Respuesta breve: Detiene el robo de información (infostealers) y el robo de tokens de sesión a nivel de kernel, antes de que comience la exfiltración, y analiza todo de forma local para que las claves y los tokens nunca tengan que subirse a una nube de terceros.

La amenaza que realmente enfrentan las empresas financieras

Los ataques hiperautomatizados de "entrar y arrasar" (smash and grab) se dirigen a tokens de sesión y claves de API. Estos pasan de la infiltración a la autoeliminación en segundos, más rápido de lo que tarda una alerta en la nube en salir del edificio. Un token de sesión robado a menudo elude por completo las contraseñas y la MFA, dándole al atacante una forma aparentemente legítima de volver a entrar en cualquier momento.

El caso documentado

Una importante empresa de servicios financieros utilizaba tres EDR líderes de la industria y un MSSP subcontratado entre los 50 principales. Se implementó Cyber Crucible para encontrar el punto ciego. En un plazo de 60 días, había interceptado de forma autónoma casi 10,000 procesos maliciosos, el 98% de ellos en el conjunto de servidores Microsoft SQL altamente privilegiados de la empresa, sin ninguna alerta por parte de la infraestructura heredada.

La causa raíz se remontó a una credencial de monitoreo remoto probablemente comprometida. Meses después, la industria reportó una ola global de ransomware que instalaba puertas traseras en servidores SQL en todo el mundo. El sector financiero sufrió graves brechas de seguridad. Este cliente nunca fue una víctima.

Revision #1
Created 2026-07-24 01:52:18 UTC by Dennis Underwood
Updated 2026-07-24 01:52:18 UTC by Dennis Underwood