¿En Qué Se Diferencia Esto del Monitoreo de Identidad Normal?

La capacidad de Cyber Crucible frente al robo de identidad digital es proactiva y preventiva. Impide el acceso a la información necesaria para llevar a cabo operaciones de chantaje, extorsión y robo de identidad moderno.

La protección tradicional contra el robo de identidad se ocupa de las contraseñas y otros datos en manos de los estafadores, y del monitoreo de asuntos como el uso fraudulento de tarjetas de crédito, la obtención de préstamos fraudulentos o el hallazgo eventual de contraseñas en filtraciones de datos. Esto es muy reactivo y resulta difícil de gestionar para los clientes en su vida diaria. Además, abre la posibilidad, que Cyber Crucible ha observado, de chantajear a personas, e incluso coaccionar a empleados y ejecutivos para que ayuden a los atacantes a atacar a sus propios empleadores.

Existe un esfuerzo concertado por parte de los atacantes para obtener cookies, credenciales de inicio de sesión, plataformas de mensajería y otras formas de autenticación y datos privados que faciliten sus ataques.

Los análisis de Cyber Crucible enfocados en el robo de identidad previenen esto, de una manera que proporciona una toma de decisiones conductual autorizada sin necesidad de intervención del usuario, frente a las tácticas modernas de extorsión y los ataques cibercriminales sin archivos (file-less).

Revision #1
Created 2026-07-24 01:42:42 UTC by Dennis Underwood
Updated 2026-07-24 01:42:42 UTC by Dennis Underwood