??? ????? ??? ?? ????????? ????????? ????????

تتميز قدرة Cyber Crucible في مكافحة سرقة الهوية الرقمية بأنها استباقية ووقائية. فهي تمنع الوصول إلى المعلومات اللازمة لتنفيذ عمليات الابتزاز، والتهديد، وسرقة الهوية الحديثة.

تتعامل الحماية التقليدية من سرقة الهوية مع كلمات المرور والبيانات الأخرى التي تقع في أيدي المحتالين، وتراقب أموراً مثل الاستخدام الاحتيالي لبطاقات الائتمان، أو الحصول على قروض احتيالية، أو اكتشاف كلمات المرور لاحقاً في خروقات البيانات. وهذا أسلوب تفاعلي بدرجة كبيرة، ويصعب على العملاء إدارته في حياتهم اليومية. كما أنه يفتح المجال، وهو ما لاحظته Cyber Crucible، لابتزاز الأفراد، بل وحتى إجبار الموظفين والمدراء التنفيذيين على مساعدة المهاجمين في مهاجمة أصحاب عملهم.

هناك جهد منسق من قبل المهاجمين لاستهداف ملفات تعريف الارتباط (cookies)، وبيانات تسجيل الدخول، ومنصات المراسلة، وغيرها من أشكال المصادقة والبيانات الخاصة لتمكين هجماتهم.

تمنع تحليلات Cyber Crucible المتخصصة في سرقة الهوية ذلك، بطريقة توفر اتخاذ قرارات سلوكية موثوقة دون الحاجة إلى تدخل المستخدم، في مواجهة أساليب الابتزاز الحديثة وهجمات مجرمي الإنترنت التي لا تعتمد على الملفات (fileless).

Revision #1
Created 2026-07-24 02:59:10 UTC by Dennis Underwood
Updated 2026-07-24 02:59:10 UTC by Dennis Underwood