Comment Cyber Crucible protège-t-il les entreprises de services financiers ?

Réponse courte : Il stoppe les infostealers et le vol de jetons de session au niveau du noyau, avant même que l'exfiltration ne commence, et il analyse tout localement afin que les clés et les jetons n'aient jamais à être téléchargés vers un cloud tiers.

La menace à laquelle les entreprises financières sont réellement confrontées

Des attaques hyper-automatisées de type « smash and grab » ciblent les jetons de session et les clés API. Elles passent de l'infiltration à l'auto-suppression en quelques secondes — plus vite qu'une alerte cloud ne peut quitter les locaux. Un jeton de session volé contourne souvent entièrement les mots de passe et la MFA, offrant à un attaquant un moyen d'accès apparemment légitime à tout moment.

Le cas documenté

Une importante entreprise de services financiers exploitait trois solutions EDR parmi les meilleures du secteur ainsi qu'un MSSP externalisé faisant partie du Top 50. Cyber Crucible a été déployé pour identifier l'angle mort. En 60 jours, il avait intercepté de manière autonome près de 10 000 processus malveillants — 98 % d'entre eux sur la ferme de serveurs Microsoft SQL hautement privilégiés de l'entreprise — sans aucune alerte de la part de la pile de sécurité existante.

La cause racine a été retracée jusqu'à un identifiant de surveillance à distance probablement compromis. Des mois plus tard, le secteur a signalé une vague mondiale de ransomware installant des portes dérobées sur des serveurs SQL à travers le monde. Le secteur financier a subi de graves violations. Ce client n'en a jamais été victime.

Revision #1
Created 2026-07-24 07:01:28 UTC by Dennis Underwood
Updated 2026-07-24 07:01:28 UTC by Dennis Underwood