

Pourquoi la protection des données d'identité nécessite-t-elle un accès au niveau du noyau ?

Réponse courte : Parce que le vol se produit dans l'espace entre le moment où un programme demande des données d'identification et celui où le système d'exploitation les délivre. Seule une défense opérant au niveau du noyau — en dessous des applications et des bibliothèques qu'un attaquant peut manipuler — peut voir cette requête, en juger l'intention et l'arrêter à temps.

Les trois exigences

1. Voir l'accès au moment où il se produit. Le vol d'identité ne se traduit pas par l'apparition d'un fichier sur le disque ; c'est une lecture. Les outils qui recherchent des fichiers malveillants ne voient rien, car dans un infostealer moderne, rien n'est écrit. L'événement à détecter est la tentative d'accès elle-même.

2. Décider assez rapidement. Les outils automatisés peuvent s'infiltrer, collecter des données et s'autodétruire en quelques secondes. Toute architecture qui envoie des télémétries à un service cloud et attend un verdict a déjà perdu la course. La décision doit se prendre localement, en quelques millisecondes.

3. Ne pas dépendre de ce que l'attaquant contrôle. Les outils de sécurité qui s'appuient sur les bibliothèques du système d'exploitation peuvent être aveuglés lorsqu'un attaquant compromet ces bibliothèques en mémoire — l'agent continue de s'exécuter mais ne signale plus rien. Cyber Crucible a été délibérément découplé des bibliothèques Windows afin qu'un système d'exploitation compromis ne puisse pas le réduire au silence.

La conséquence

Le fonctionnement au niveau du noyau permet de réunir ces trois exigences à la fois : la visibilité sur la tentative d'accès, une décision locale en moins de 200 millisecondes, et l'indépendance vis-à-vis d'un système d'exploitation potentiellement compromis.

C'est également ce qui permet à la protection de fonctionner sans aucune connectivité — en environnement isolé (air-gapped), hors ligne, ou en mer — puisqu'aucune donnée n'a besoin de quitter l'appareil pour qu'une décision soit prise.

Revision #1

Created 2026-07-24 06:53:23 UTC by Dennis Underwood

Updated 2026-07-24 06:53:23 UTC by Dennis Underwood