Explication de l'identité numérique

Ce que sont réellement les jetons de session, les jetons de rafraîchissement, les cookies, les clés API et les clés de portefeuille, pourquoi les attaquants les ciblent, et comment le moteur comportemental noyau de Cyber Crucible les protège sans jamais les lire.

Collectez-vous des données d'identité ?

La réponse courte est non, nous ne le faisons pas.

La réponse plus longue est, non, nous ne le faisons pas, mais de deux manières différentes :

Premièrement, nous ne transmettons jamais de mots de passe, de cookies, de jetons oauth, ou quoi que ce soit d'autre qui serait considéré comme des données d'identité vers nos serveurs Cyber Crucible. Cela est vrai que le serveur soit hébergé par le client ou par Cyber Crucible.

Deuxièmement, nous avons appris à réaliser une analyse comportementale des informations d'identité, sans réellement traiter les informations d'identité. Cela signifie que nos analyses ne traitent ni n'exposent réellement de données sensibles telles que les mots de passe réels, les jetons de session, etc.

En quoi cela diffère-t-il de la surveillance d’identité classique ?

La fonctionnalité de protection contre le vol d’identité numérique de Cyber Crucible est proactive et préventive. Elle empêche l’accès aux informations nécessaires pour mener des opérations de chantage, d’extorsion et de vol d’identité moderne.

La protection traditionnelle contre le vol d’identité traite des mots de passe et autres données entre les mains de fraudeurs, et surveille des éléments tels que l’utilisation frauduleuse de cartes de crédit, la souscription de prêts frauduleux, ou la découverte éventuelle de mots de passe lors de violations de données. Cette approche est très réactive et difficile à gérer au quotidien pour les clients. Elle ouvre également la voie, comme Cyber Crucible l’a observé, au chantage envers des particuliers, voire à la coercition d’employés et de dirigeants pour qu’ils aident les attaquants à s’en prendre à leurs employeurs.

Les attaquants déploient des efforts concertés pour cibler les cookies, les identifiants de connexion, les plateformes de messagerie et d’autres formes d’authentification et de données privées afin de faciliter leurs attaques.

Les analyses de Cyber Crucible axées sur le vol d’identité empêchent cela, grâce à une prise de décision comportementale faisant autorité, sans intervention de l’utilisateur, face aux tactiques d’extorsion modernes et aux attaques sans fichier menées par des cybercriminels.

Quelles données d'identité sont protégées ?

Système d'exploitation Windows principal

- NTDS (Active Directory)
- Fonctionnalité en phase d'incubation qui continuera à être améliorée

Identifiants de client VPN

- noms d'utilisateur
- mots de passe
- authentification par clé

Navigateurs Web

- cookies
- jetons de rafraîchissement (jetons d'authentification « se souvenir de moi »)
- jetons oAuth (jetons de session, jetons d'accès)
- mots de passe
- noms d'utilisateur
- historique de navigation

Applications de collaboration et de messagerie

- contacts
- noms d'utilisateur
- historiques de discussion
- contenus de discussion enregistrés
- pièces jointes de discussion enregistrées
- clés de chiffrement de messagerie privée
- mots de passe
- jetons oauth (jetons de session, jetons d'accès, jetons de rafraîchissement)

Portefeuilles crypto

- contenu du portefeuille
- enregistrements de transactions
- mots de passe
- clés de chiffrement

Jeux :

- En phase d'incubation - actuellement uniquement Steam
- mots de passe
- achats
- identifiants
- noms d'utilisateur
- jetons oAuth (jetons de session, jetons d'accès, jetons de rafraîchissement)

Partage de fichiers :

- En phase d'incubation - actuellement uniquement FileZilla
- mots de passe
- achats
- identifiants
- noms d'utilisateur
- authentification par clé
- serveurs et paramètres de serveur

Comment les données d'identité sont-elles protégées ?

Réponse courte : Cyber Crucible identifie les emplacements où sont stockées les données d'identité et protège ces emplacements au niveau du noyau (kernel). Lorsqu'un programme tente d'y accéder, son accès est tracé et analysé — **sans que les mots de passe, jetons ou clés de chiffrement eux-mêmes ne soient jamais consultés ou collectés**. Sur la base de cette analyse, le programme est autorisé, reçoit des données fictives, est refusé, ou est suspendu.

Protéger l'accès, pas le secret

La plupart des solutions de protection de l'identité travaillent sur le secret : le chiffrer, le mettre en coffre-fort, ou surveiller son apparition dans une fuite de données. Cyber Crucible agit sur **l'acte de vouloir y accéder**.

Les attaques automatisées sont prévisibles d'une manière bien précise — elles doivent se rendre à des emplacements connus pour trouver des identifiants. Les magasins de cookies des navigateurs, les chemins d'identifiants VPN, le magasin d'identifiants Windows, les fichiers de portefeuilles (wallets) et les données Active Directory se trouvent tous à des endroits que les attaquants savent déjà où chercher. Cette prévisibilité constitue l'opportunité défensive.

Cyber Crucible identifie ces magasins de données d'identité, puis les protège. Tout programme touchant l'un d'entre eux est évalué, ainsi que ses processus parents et enfants et les bibliothèques qu'il a chargées.

Les secrets ne sont jamais lus

Il s'agit d'une contrainte de conception délibérée, et non d'un effet secondaire : **l'accès est tracé et analysé sans que l'identifiant lui-même soit consulté.** Cyber Crucible ne lit, ne traite, ne collecte ni ne transmet les mots de passe, jetons de session, cookies ou clés de chiffrement — vers aucun serveur, qu'il soit hébergé par Cyber Crucible ou par le client.

Il s'avère que l'analyse comportementale de l'accès à l'identité ne nécessite pas les données d'identité elles-mêmes. Ce qui compte, c'est *quel programme accède où, dans quel contexte, après avoir fait quoi au préalable* — rien de tout cela ne nécessite d'ouvrir le secret.

La conséquence est que la protection ne peut pas elle-même devenir la brèche, et il n'existe aucun magasin central de vos identifiants pouvant être assigné en justice, divulgué ou perdu.

Ce qu'évalue le moteur comportemental

La décision n'est pas « ce programme figure-t-il sur une liste ? » — c'est « que fait réellement ce code en ce moment ? ». Les signaux incluent :

- **État et comportement de la mémoire** — suivis sur l'ensemble du cycle de vie du programme, y compris les modifications en mémoire qui ne touchent jamais le disque. Il s'agit de la couche de capteurs fondamentale de la plateforme, partagée avec la protection des données et FortressAI, plutôt que spécifique à l'identité.
- **Lignage des processus** — ce qui a lancé ce programme, et ce que ce programme a lancé à son tour.
- **Modèle d'accès** — s'agit-il d'une application normale lisant son propre identifiant, ou d'un balayage à travers de nombreux emplacements d'identité à la fois ?
- **Activité des bibliothèques et injections** — ce processus de confiance a-t-il fait l'objet d'une injection ou d'une altération en mémoire ?

La réponse est graduée, pas binaire

Tout programme cherchant à accéder à des données d'identité n'est pas un attaquant, donc la réponse dépend de la nature du programme et de son comportement :

Situation	Réponse
Une application connue, non compromise, accédant à ce dont elle a légitimement besoin	Autorisée
Une application connue, non compromise, mais **dépassant** son accès approprié	**Reçoit des données fictives, ou l'accès est refusé** — régi par les règles comportementales de confidentialité
Une application **inconnue**	**Rejetée ou suspendue**, selon le moteur comportemental et vos paramètres
Une application **compromise** — processus ou bibliothèques exploités	**Rejetée ou suspendue**, selon le moteur comportemental et vos paramètres

Le cas intermédiaire importe plus qu'il n'y paraît de prime abord. De nombreux logiciels légitimes accèdent plus profondément aux magasins d'identité que nécessaire. Les suspendre perturberait la journée de l'utilisateur sans aucun gain de sécurité — mais leur transmettre de véritables identifiants représente une exposition inutile. Le renvoi de données fictives satisfait le programme tandis que le véritable secret reste en place.

La distinction que trace le moteur se situe entre un programme de confiance qui *dépasse ses prérogatives* et un programme inconnu ou *pris en otage*. Seul ce dernier cas est traité comme une attaque.

Pourquoi cela se produit sur le poste de travail (endpoint)

Un infostealer automatisé peut s'infiltrer, collecter des données et supprimer ses propres outils en mémoire en quelques secondes. Envoyer une télémétrie à un service cloud et attendre un verdict ne peut rivaliser avec cette rapidité. La boucle complète de détection-décision-réponse (detect-decide-respond) s'exécute donc localement dans le noyau, ce qui explique également pourquoi elle fonctionne sans aucune connectivité.

> Voir aussi : *« Collectez-vous des données d'identité ? »*, *« Quelles données d'identité sont protégées ? »*, et *« Que se passe-t-il lorsqu'un programme tente d'accéder à des données d'identité auxquelles il ne devrait pas avoir accès ? »*

Quels portefeuilles de cryptomonnaies sont protégés ?

- Coinomi
- Armory (« Bitcoin Armory »)
- Electrum
- Exodus
- Guarda

Que se passe-t-il lorsqu'un programme tente d'accéder à des données d'identité auxquelles il ne devrait pas avoir accès ?

Réponse courte : cela dépend du fait que le programme soit fiable et qu'il ait été compromis ou non. Une application légitime qui outrepasse simplement ses droits reçoit des données fictives ou se voit discrètement refuser l'accès. Une application inconnue ou compromise est rejetée ou suspendue. L'identifiant réel n'est jamais transmis dans aucun de ces cas.

Pourquoi une réponse unique serait erronée

La conception évidente consiste à « bloquer tout ce qui touche à un magasin d'identifiants ». Elle échoue immédiatement en pratique, car les logiciels légitimes touchent constamment ces magasins — navigateurs, gestionnaires de mots de passe, clients VPN, outils de synchronisation et agents de sauvegarde ont tous de bonnes raisons d'y accéder.

Tout bloquer casse la machine. Tout autoriser pour les éléments fiables signifie qu'un navigateur exploité obtiendra tout ce qu'il demande. La question pertinente est plus précise : **ce programme se comporte-t-il comme il le devrait ?**

Les quatre résultats possibles

1. Autorisé. Une application connue, non exploitée, accédant à ce dont elle a légitimement besoin. Rien ne change.

2. Données fictives renvoyées. Une application connue, non exploitée, dépassant son accès approprié. Les règles comportementales de confidentialité s'appliquent : le programme reçoit des données plausibles mais fausses. Il continue de fonctionner normalement, et l'identifiant réel ne quitte jamais le stockage. Du point de vue du programme, rien n'a échoué — ce qui explique

précisément pourquoi cela fonctionne sans perturber les flux de travail.

3. Accès refusé. La même situation, où le renvoi de données fictives n'est pas approprié. La demande est refusée ; l'application continue de fonctionner.

4. Rejeté ou suspendu. Le programme est inconnu, ou un programme connu dont le processus ou les bibliothèques présentent des signes d'exploitation. Ici, la préoccupation n'est pas le dépassement de droits, mais le fait que le programme n'agit plus comme lui-même. Le fait qu'il soit rejeté ou suspendu dépend de l'évaluation du moteur comportemental et de vos paramètres configurés.

Pourquoi la tromperie plutôt que le blocage

Renvoyer des données fictives est un choix délibéré. Une demande bloquée indique à un attaquant qu'il a été détecté et l'incite à essayer une autre voie. Des données fictives d'apparence réelle ne le font pas — les outils poursuivent avec des identifiants qui ne débloquent rien, et l'opérateur peut ne pas se rendre compte du problème avant un certain temps.

C'est le même principe que celui des fichiers canari dans la défense contre les rançongiciels : donner à l'attaquant quelque chose de convaincant à saisir, sans aucun coût pour vous.

Configurabilité

La frontière entre rejet et suspension est ajustable. Les environnements ayant une faible tolérance aux interruptions — systèmes cliniques, chaînes de production — peuvent privilégier le refus et les données fictives plutôt que la suspension, tandis que les environnements à haute sécurité peuvent adopter une approche plus agressive.

Qu'est-ce qu'un jeton de session, et pourquoi le vol de celui-ci est-il pire que le vol d'un mot de passe ?

Réponse courte : Un jeton de session est l'identifiant que votre navigateur ou votre application conserve *après* votre connexion, prouvant que vous êtes déjà authentifié. Voler un tel jeton est souvent pire que voler un mot de passe, car cela contourne généralement à la fois le mot de passe et l'authentification multifacteur — l'attaquant reprend simplement votre session existante.

Pourquoi cela existe

Ressaisir un mot de passe à chaque requête serait inutilisable ; c'est pourquoi, après une connexion réussie, le service émet un jeton. Chaque requête ultérieure transporte ce jeton au lieu de vos identifiants. Le service lui fait confiance comme preuve que vous vous êtes déjà authentifié.

Pourquoi les attaquants le préfèrent

- **Cela contourne l'authentification multifacteur (MFA).** La MFA est vérifiée lors de la connexion. Un jeton émis *après* cette vérification représente une authentification déjà validée, de sorte que le rejouer ne déclenche généralement pas à nouveau le deuxième facteur.
- **Cela paraît légitime.** Pour le service, un jeton valide équivaut à un utilisateur valide. Il n'y a aucun signal d'échec de connexion et rien d'anormal à signaler.
- **C'est portable.** De nombreux jetons fonctionnent depuis une machine, un réseau ou un pays différent.

Pourquoi cela a changé le comportement des attaquants

Les attaquants évitent de plus en plus de s'attarder dans un réseau. Rester présent augmente les risques de détection. Ils préfèrent au contraire s'emparer des éléments d'identité et repartir — puis revenir à volonté en tant qu'utilisateur authentifié. Le jeton est une porte dérobée à l'apparence légitime, émise par le système d'authentification lui-même.

Comment Cyber Crucible y remédie

Le vol de jeton est stoppé au moment même de l'accès. Lorsqu'un programme tente d'accéder au stockage du navigateur ou de l'application où résident les jetons, son accès est évalué en moins de 200 millisecondes. Un programme légitime mais excessif se voit fournir de fausses données ou se voit refuser l'accès ; un programme inconnu ou compromis est rejeté ou suspendu. Dans tous les cas, le jeton réel n'est jamais transmis.

Qu'est-ce qu'un jeton d'actualisation, et pourquoi sa perte est-elle particulièrement dommageable ?

Réponse courte : un jeton d'actualisation (refresh token) est un identifiant de longue durée utilisé pour obtenir silencieusement de nouveaux jetons d'accès sans que l'utilisateur ait à se reconnecter. C'est ce sur quoi repose la fonction « se souvenir de moi ». Comme il peut permettre de générer indéfiniment de nouveaux accès, un jeton d'actualisation dérobé peut offrir à un attaquant un accès durable bien après la fin de votre session.

Jeton d'accès vs. jeton d'actualisation

- **Jeton d'accès (jeton de session) :** de courte durée, utilisé à chaque requête, expire en quelques minutes ou quelques heures.
- **Jeton d'actualisation :** de longue durée, utilisé uniquement pour demander de nouveaux jetons d'accès. Parfois valable pendant des semaines ou des mois.

Un jeton d'accès dérobé finit par expirer. Un jeton d'actualisation dérobé peut être utilisé pour générer de nouveaux jetons d'accès de manière répétée — ce qui transforme un vol ponctuel en un accès persistant.

Pourquoi « se souvenir de moi » implique un compromis

Rester connecté nécessite de stocker un élément durable sur l'appareil. Cette commodité est précisément ce qui rend le jeton stocké précieux pour un attaquant. Les magasins d'identifiants des navigateurs et des applications constituent des emplacements standards et prévisibles, de sorte que les outils automatisés s'y attaquent directement.

Réduire les dommages

Révoquer un jeton d'actualisation invalide l'accès qu'il peut générer — c'est pourquoi la fonction « se déconnecter de tous les appareils » et la révocation des jetons sont importantes après toute compromission suspectée. Mais la révocation est une réponse mise en œuvre *après* le vol.

L'approche de Cyber Crucible consiste à empêcher la lecture. Le magasin d'identifiants est un emplacement protégé : un programme légitime qui outrepasse ses droits à cet endroit reçoit des données factices ou se voit refuser l'accès, tandis qu'un programme inconnu ou compromis est rejeté ou suspendu. Le jeton d'actualisation lui-même n'est jamais divulgué.

Que sont les cookies de navigateur, et comment les attaquants en abusent-ils ?

Réponse courte : Les cookies sont de petites données qu'un site web stocke dans votre navigateur, et certains d'entre eux sont des cookies d'authentification qui vous maintiennent connecté. Les voler équivaut fonctionnellement à voler une session active — l'attaquant peut les charger dans son propre navigateur et paraître être vous.

Tous les cookies n'ont pas la même importance

- **Cookies de préférence** — langue, thème, mise en page. Faible valeur.
- **Cookies d'analyse** — mesure d'utilisation. Faible valeur.
- **Cookies d'authentification / de session** — prouvent que vous êtes connecté. **Valeur élevée.**

Les attaquants s'intéressent presque exclusivement à cette troisième catégorie.

Pourquoi le vol de cookies est efficace

Un cookie d'authentification volé ne déclenche généralement ni un événement de connexion, ni une invite de mot de passe, ni un défi MFA. La session existe déjà ; l'attaquant ne fait que présenter la preuve de celle-ci. Du point de vue de l'application, cela ressemble à une activité normale et continue.

Les navigateurs stockent les cookies dans des emplacements de fichiers connus et prévisibles sur chaque système d'exploitation, ce qui permet aux outils automatisés de les localiser sans avoir besoin de connaître quoi que ce soit de spécifique sur la machine.

Pourquoi le navigateur est un point central

Le navigateur regroupe en un seul endroit les cookies, les mots de passe enregistrés, les jetons OAuth et l'historique, ce qui en fait la cible d'identité la plus riche sur la plupart des postes de travail. Cyber Crucible l'a constaté directement : à partir du quatrième trimestre 2023, les réponses automatisées contre l'activité de Chrome, Edge et Chromium sont passées de zéro à plusieurs milliers, avec des CVE associés publiés ultérieurement par Google et Microsoft.

Protection

Le stockage des identifiants du navigateur est l'un des emplacements d'identité protégés. Un processus tentant d'y accéder en lecture est évalué en contexte — un navigateur exploité est traité très différemment d'un navigateur sain, et dans aucun des deux cas une requête excessive ne reçoit le véritable cookie.

Qu'est-ce qu'une clé API, et que se passe-t-il si elle est volée ?

Réponse courte : Une clé API est une chaîne secrète qui identifie et autorise un programme — plutôt qu'une personne — lorsqu'il fait appel à un service. Une clé volée permet à un attaquant d'effectuer des requêtes en se faisant passer pour votre application, souvent sans aucune interaction humaine, sans MFA, et sans signe évident que quelque chose ne va pas.

Pourquoi elles constituent des cibles attrayantes

- **Aucun humain dans la boucle.** Les clés sont conçues pour un usage automatisé et non surveillé, il n'y a donc pas d'invite MFA pour interférer.
- **Souvent largement étendues.** Les clés sont fréquemment émises avec plus de permissions que ce que la tâche exige.
- **Longue durée de vie.** Beaucoup ne sont jamais renouvelées, si bien qu'une clé volée aujourd'hui peut encore fonctionner des mois plus tard.
- **Stockées dans des emplacements prévisibles.** Fichiers de configuration, variables d'environnement et magasins d'identifiants — tous des emplacements que l'automatisation peut énumérer.

Conséquences typiques

Selon ce que la clé autorise : lecture ou exportation de données clients, envoi de messages au nom de votre organisation, dépenses sur un compte cloud, ou rebond vers d'autres systèmes connectés.

Comme les requêtes sont correctement authentifiées, elles apparaissent généralement dans les journaux comme du trafic applicatif normal. La détection intervient généralement bien après les faits, via une facture ou un audit.

Réduire l'exposition

Limitez la portée des clés, renouvelez-les régulièrement, et gardez-les hors du contrôle de version. Ce sont de bonnes pratiques, mais elles limitent le rayon d'impact plutôt que d'empêcher le vol.

Cyber Crucible cible le vol lui-même. Les emplacements des identifiants et des configurations sont protégés, et un programme qui les lit est évalué en contexte : données factices ou refus en cas de dépassement légitime, rejet ou suspension pour un processus inconnu ou compromis. La clé n'est remise dans aucun des deux cas.

Où Windows stocke-t-il les mots de passe et les identifiants ?

Réponse courte : À plusieurs endroits prévisibles — le Gestionnaire d'identification Windows, les magasins de mots de passe des navigateurs, la configuration du client VPN et, sur les contrôleurs de domaine, la base de données Active Directory (NTDS). « Prévisible » est le mot clé : les attaques automatisées reposent sur le fait que ces emplacements sont identiques sur chaque machine.

Les principaux emplacements de stockage

- **Gestionnaire d'identification Windows** — identifiants enregistrés pour les ressources réseau et les applications.
- **Magasins de mots de passe des navigateurs** — Chrome, Edge et Firefox conservent chacun les identifiants enregistrés dans des chemins de profil connus.
- **Identifiants du client VPN** — noms d'utilisateur, mots de passe et éléments d'authentification par clé.
- **NTDS (Active Directory)** — sur un contrôleur de domaine, les données d'identification de l'ensemble du domaine. La cible la plus précieuse du réseau.
- **Magasins propres aux applications** — les outils de messagerie et de collaboration, les clients de transfert de fichiers et les plateformes de jeu gèrent chacun les leurs.

Pourquoi la prévisibilité est l'essentiel du problème

Les attaquants ne connaissent rien de votre environnement spécifique. Leur automatisation est conçue pour des chemins qui existent partout — `C:\Users\[Username]`, les dossiers de données d'application standard, les lettres de lecteur standard. Un script n'a pas besoin de comprendre votre réseau ; il se contente de parcourir des chemins connus.

C'est une faiblesse dans leur méthode. Si ces emplacements précis sont ceux qui sont surveillés, l'exigence de fiabilité propre à l'attaquant devient elle-même le déclencheur qui permet de le repérer.

Ce que Cyber Crucible en fait

Ces magasins constituent les points d'entrée surveillés du vol d'identité. L'intention d'un programme qui les lit est évaluée en moins de 200 millisecondes — et il est suspendu si cette intention est malveillante, avant que le moindre identifiant ne soit dérobé.

Que sont les clés de portefeuille de cryptomonnaie, et pourquoi leur vol est-il irréversible ?

Réponse courte : Une clé de portefeuille est la clé cryptographique privée qui autorise les dépenses depuis une adresse de cryptomonnaie. Quiconque la détient contrôle les fonds. Le vol est effectivement irréversible car les transactions sur la blockchain ne peuvent pas être annulées, et il n'existe aucune institution auprès de laquelle faire appel.

En quoi cela diffère d'une banque

Un débit frauduleux sur une carte peut être contesté et annulé par un émetteur. Une transaction en cryptomonnaie signée avec votre clé privée est valide par définition — le réseau ne peut pas distinguer un vol d'un transfert légitime, et il n'existe aucune autorité centrale pour l'annuler.

Cela rend les clés de portefeuille particulièrement attrayantes : le gain est immédiat, définitif et difficile à tracer.

Ce que recherchent les attaquants

- **Les clés privées et les phrases de récupération (seed phrases)** stockées dans les fichiers de l'application de portefeuille
- **Le contenu du portefeuille et l'historique des transactions**, utiles pour cibler les victimes à plus forte valeur
- **Les mots de passe protégeant le portefeuille**, souvent réutilisés ailleurs

Les logiciels de portefeuille de bureau stockent ces éléments dans des emplacements de données d'application prévisibles — le même schéma qui rend accessible par l'automatisation tout autre magasin d'identifiants.

Protection

Les fichiers de portefeuille font partie des emplacements d'identité surveillés par Cyber Crucible. Comme la réponse consiste en une suspension au moment même de l'accès malveillant, le vol est prévenu plutôt que détecté après coup — ce qui compte ici plus que presque partout ailleurs,

puisqu'il n'existe aucun moyen de récupération une fois les fonds transférés.

> Voir aussi : « *Quels portefeuilles de cryptomonnaie sont protégés ?* » pour connaître les applications spécifiques actuellement couvertes.

Qu'est-ce que l'authentification par clé, et pourquoi les clés volées offrent-elles un accès durable ?

Réponse courte : L'authentification par clé prouve l'identité au moyen d'une clé privée cryptographique plutôt que d'un mot de passe — utilisée par SSH, de nombreux VPN et les clients de transfert de fichiers. Une clé privée volée accorde un accès sans qu'aucun mot de passe ni invite MFA ne soit requis, et comme les clés sont rarement renouvelées, cet accès peut persister très longtemps.

Comment cela fonctionne

Vous détenez une clé privée ; le serveur détient la clé publique correspondante. Lors de la connexion, le serveur émet un défi auquel seule la clé privée peut répondre. La clé elle-même ne transite jamais sur le réseau.

C'est réellement plus robuste que les mots de passe — cela résiste aux devinettes, au phishing et à la réutilisation. Sa faiblesse est différente : **tout repose sur la confidentialité du fichier de clé privée.**

Pourquoi une clé volée est si durable

- **Aucune invite de mot de passe.** La clé *est* l'identifiant.
- **Souvent aucune MFA.** L'authentification par clé fonctionne fréquemment seule, en particulier pour les systèmes automatisés.
- **Rarement renouvelée.** Les mots de passe expirent selon un calendrier ; les clés restent souvent valables pendant des années.
- **Emplacement de stockage prévisible.** Répertoires standards et chemins de configuration des clients VPN.

Une clé volée constitue une porte dérobée discrète et durable, qui ne génère aucune tentative de connexion échouée et paraît entièrement légitime.

Protection

Le matériel d'authentification VPN et par clé fait explicitement partie des catégories d'identité protégées. L'accès est évalué au niveau du noyau, de sorte qu'un programme tentant de récupérer des fichiers de clés est arrêté — refusé ou alimenté en données falsifiées s'il s'agit d'un programme de confiance outrepassant ses droits, rejeté ou suspendu s'il s'agit d'un programme inconnu ou compromis — avant que la clé ne quitte la machine.

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.