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.

Revision #1
Created 2026-07-24 06:53:12 UTC by Dennis Underwood
Updated 2026-07-24 06:53:12 UTC by Dennis Underwood