

¿Qué es la autenticación basada en claves y por qué las claves robadas otorgan acceso duradero?

Respuesta breve: La autenticación basada en claves demuestra la identidad mediante una clave privada criptográfica en lugar de una contraseña, y es utilizada por SSH, muchas VPN y clientes de transferencia de archivos. Una clave privada robada otorga acceso sin necesidad de contraseña ni de una solicitud de MFA, y como las claves rara vez se rotan, ese acceso puede persistir durante mucho tiempo.

Cómo funciona

Usted posee una clave privada; el servidor posee la clave pública correspondiente. Al momento de la conexión, el servidor emite un desafío que solo la clave privada puede responder. La clave en sí nunca atraviesa la red.

Esto es genuinamente más sólido que las contraseñas: resiste la adivinación, el phishing y la reutilización. Su debilidad es distinta: **todo depende de que el archivo de la clave privada se mantenga privado.**

Por qué una clave robada es tan duradera

- **Sin solicitud de contraseña.** La clave es la credencial.
- **Frecuentemente sin MFA.** La autenticación por clave a menudo funciona sola, particularmente en sistemas automatizados.
- **Rara vez se rota.** Las contraseñas caducan según un calendario; las claves suelen durar años.
- **Almacenamiento predecible.** Directorios estándar y rutas de configuración de clientes VPN.

Una clave robada es una puerta trasera silenciosa y duradera que no genera inicios de sesión fallidos y que parece completamente legítima.

Protección

El material de autenticación basado en claves y de VPN se encuentra explícitamente entre las categorías de identidad protegidas. El acceso se evalúa a nivel del kernel, de modo que un programa que recolecta archivos de claves es detenido —denegado o alimentado con datos falsos si se trata de un programa de confianza que se extralimita, rechazado o suspendido si es desconocido o está comprometido— antes de que la clave salga del equipo.

Revision #1

Created 2026-07-24 01:44:42 UTC by Dennis Underwood

Updated 2026-07-24 01:44:42 UTC by Dennis Underwood