¿Dónde almacena Windows las contraseñas y las credenciales?

Respuesta breve: En varios lugares predecibles: el Administrador de credenciales de Windows, los almacenes de contraseñas del navegador, la configuración del cliente VPN y, en los controladores de dominio, la base de datos de Active Directory (NTDS). "Predecible" es la palabra clave: los ataques automatizados dependen de que esas ubicaciones sean las mismas en todas las máquinas.

Los principales almacenes

- **Administrador de credenciales de Windows** — inicios de sesión guardados para recursos de red y aplicaciones.
- **Almacenes de contraseñas del navegador** — Chrome, Edge y Firefox conservan cada uno las credenciales guardadas en rutas de perfil conocidas.
- **Credenciales del cliente VPN** — nombres de usuario, contraseñas y material de autenticación basado en claves.
- **NTDS (Active Directory)** — en un controlador de dominio, los datos de credenciales de todo el dominio. El objetivo de mayor valor en la red.
- **Almacenes específicos de aplicaciones** — las herramientas de mensajería y colaboración, los clientes de transferencia de archivos y las plataformas de juegos mantienen cada uno los suyos propios.

Por qué la previsibilidad es todo el asunto

Los atacantes no saben nada acerca de su entorno específico. Su automatización está escrita para rutas que existen en todas partes: `C:\Users\[Username]`, carpetas estándar de datos de aplicaciones, letras de unidad estándar. Un script no necesita entender su red; simplemente recorre rutas conocidas.

Esa es una debilidad de su método. Si esas ubicaciones exactas son las que se están vigilando, el propio requisito de fiabilidad del atacante se convierte en el disparador que lo atrapa.

Qué hace Cyber Crucible al respecto

Estos almacenes son los puntos de entrada de robo de identidad que se monitorean. La intención de un programa que los lee se evalúa en menos de 200 milisegundos, y se suspende si esa intención es maliciosa, antes de que se sustraiga cualquier credencial.

Revision #1
Created 2026-07-24 01:44:23 UTC by Dennis Underwood
Updated 2026-07-24 01:44:23 UTC by Dennis Underwood