Onde o Windows armazena senhas e credenciais?

Resposta curta: Em vários locais previsíveis — o Windows Credential Manager, os repositórios de senhas do navegador, a configuração do cliente VPN e, nos controladores de domínio, a base de dados do Active Directory (NTDS). "Previsível" é a palavra-chave: os ataques automatizados dependem do fato de esses locais serem os mesmos em todas as máquinas.

Os principais repositórios

- **Windows Credential Manager** — logins salvos para recursos de rede e aplicativos.
- **Repositórios de senhas do navegador** — Chrome, Edge e Firefox mantêm cada um credenciais salvas em caminhos de perfil conhecidos.
- **Credenciais de cliente VPN** — nomes de usuário, senhas e material de autenticação baseado em chaves.
- **NTDS (Active Directory)** — em um controlador de domínio, os dados de credenciais de todo o domínio. O alvo de maior valor na rede.
- **Repositórios específicos de aplicativos** — ferramentas de mensagens e colaboração, clientes de transferência de arquivos e plataformas de jogos mantêm, cada um, os seus próprios.

Por que a previsibilidade é o cerne da questão

Os atacantes não sabem nada sobre o seu ambiente específico. A automação deles é escrita com base em caminhos que existem em todos os lugares — `C:\Users\[Username]`, pastas padrão de dados de aplicativos, letras de unidade padrão. Um script não precisa entender a sua rede; ele apenas percorre caminhos conhecidos.

Essa é uma fraqueza no método deles. Se esses locais exatos forem os que estão sendo monitorados, o próprio requisito de confiabilidade do atacante se torna o gatilho que o pega.

O que a Cyber Crucible faz com isso

Esses repositórios são os pontos de entrada de roubo de identidade monitorados. A intenção de um programa que os lê é avaliada em menos de 200 milissegundos — e é suspensa se essa intenção

for maliciosa, antes que qualquer credencial seja obtida.

Revision #1
Created 2026-07-24 05:42:29 UTC by Dennis Underwood
Updated 2026-07-24 05:42:29 UTC by Dennis Underwood