O que é um infostealer, e por que o roubo de tokens de sessão é tão perigoso?

Resposta curta: Um infostealer é um malware criado para capturar material de identidade digital — senhas, tokens de sessão, chaves de API e credenciais VPN — e exfiltrá-lo rapidamente. Um token de sessão roubado é perigoso porque muitas vezes contorna completamente as senhas e a autenticação multifator, permitindo que um invasor faça login como um usuário legítimo.

Por que os invasores agora roubam identidade em vez de permanecer residentes

Os invasores modernos evitam cada vez mais permanecer dentro de uma rede. Permanecer no ambiente aumenta as chances de detecção. Em vez disso, eles pegam o material de identidade e saem, o que lhes proporciona duas vantagens:

1. **Menor risco** — analisam o que roubaram a partir de um ambiente seguro, no seu próprio tempo.
2. **Retorno fácil** — com um token de sessão, senha ou chave VPN válidos, podem voltar sempre que quiserem, parecendo totalmente legítimos para o sistema de autenticação.

Por que a velocidade é todo o problema

Essas ferramentas passam da infiltração à autoexclusão em segundos — mais rápido do que um alerta na nuvem consegue sair do prédio. A Cyber Crucible interpreta a intenção no momento do acesso aos dados de identidade e suspende o processo em menos de 200 milissegundos, antes que a exfiltração comece.

Revision #1
Created 2026-07-24 05:40:03 UTC by Dennis Underwood
Updated 2026-07-24 05:40:03 UTC by Dennis Underwood