What is an infostealer, and why is session-token theft so dangerous?

Short answer: An infostealer is malware built to grab digital identity material — passwords, session tokens, API keys, and VPN credentials — and exfiltrate it fast. A stolen session token is dangerous because it often bypasses passwords and multi-factor authentication entirely, letting an attacker log in as a legitimate user.

Why attackers now steal identity instead of staying resident

Modern attackers increasingly avoid lingering inside a network. Remaining in the environment raises the odds of detection. Instead they take the identity material and leave, which gives them two advantages:

1. **Lower risk** — they analyze what they stole from a safe environment on their own time.
2. **Easy return** — with a valid session token, password, or VPN key they can come back whenever they like, appearing entirely legitimate to the authentication system.

Why speed is the whole problem

These tools move from infiltration to self-deletion in seconds — faster than a cloud alert can leave the building. Cyber Crucible reads intent at the moment of identity-data access and suspends the process in under 200 milliseconds, before exfiltration begins.

Revision #3
Created 2026-07-20 19:23:38 UTC by Dennis Underwood
Updated 2026-07-21 19:31:52 UTC by Dennis Underwood