What is browser credential theft?

Browser credential theft is harvesting the passwords, cookies, and tokens a web browser stores on a compromised machine. Saved logins are encrypted with the OS user key (via DPAPI on Windows), so an attacker in the user's context decrypts them; session cookies and tokens are even more valuable because they can let the attacker resume an authenticated session and bypass MFA. It turns one compromised endpoint into access to the user's email, SaaS, and cloud accounts.

HOW IT WORKS

01 The abuse and payload

From a compromised endpoint, the attacker collects the browser's secrets:

- Saved passwords: read the browser's credential database and decrypt with the user's DPAPI key, yielding cleartext logins.
- Session cookies: copy auth cookies and replay them to resume the user's logged-in sessions, which bypasses MFA because the session is already authenticated.
- Tokens: steal OAuth/refresh tokens for SaaS and cloud APIs.

Infostealer malware automates exactly this. Documented for defensive context.

> COOKIES BEAT MFA
>
> *Stolen session cookies let an attacker resume an already-authenticated session, so they skip the login and the MFA prompt entirely. That makes cookie theft as serious as password theft.*

HOW TO DEFEND

- Use phishing-resistant MFA and short session lifetimes so stolen cookies expire fast and are bound to the device where possible.
- Discourage saving passwords in browsers for privileged accounts; use a managed password manager.
- Limit local admin and enable [Credential Guard](/learn/active-directory/what-is-credential-gu to make user-context theft harder.
- Deploy endpoint protection against infostealers and detect bulk browser-store access.
- Bind sessions to device posture (continuous access evaluation) where supported.

SOURCES

[1] MITRE ATT&CK: Credentials from Password Stores (T1555)

[2] MITRE ATT&CK: Credential Access (TA0006)

[3] NIST SP 800-63B Digital Identity Guidelines

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-browser-credential-theft

Open online