P

Trojan-PWS and Password Stealers: What They Steal and What to Do

Trojan-PWS is a generic label for password-stealing malware. Learn what stealers collect, how they spread, warning signs, removal steps, and how to secure exposed accounts.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What password stealers target
02 How Trojan-PWS infections happen
03 Warning signs
04 What to do immediately
05 Secure accounts after cleanup
06 When to rebuild the device
07 How to prevent password-stealer infections
08 Frequently asked questions

Trojan-PWS means **Trojan Password Stealer**. It is a generic detection category for malware designed to collect passwords, session cookies, authentication tokens, wallet data, and other information that can be used to take over accounts. Names such as `Trojan.PWS`, `PWS:Win32`, or `PSW.Stealer` describe a capability, not one specific malware family.

Removing the detected file is only part of the response. Information may already have left the device, and stolen sessions can remain usable after the malware is gone.

01 What password stealers target

Target	Examples of exposed data	Possible impact
Web browsers	Saved passwords, cookies, autofill data, browsing profiles, and active sessions.	Email, social media, shopping, and cloud account takeover.
Email, VPN, FTP, and remote access	Credentials, configuration files, private keys, and connection profiles.	Access to business networks and additional victims.
Messaging and gaming accounts	Tokens, local session databases, and account credentials.	Impersonation, scams sent to contacts, and resale of accounts.
Cryptocurrency software	Wallet files, browser-wallet data, clipboard contents, and seed phrases stored insecurely.	Irreversible theft of funds.
Device data	Screenshots, clipboard, files, system details, and installed software.	Identity theft, extortion, and selection of additional attacks.

Some stealers also install a keylogger, download more malware, or open a remote-access channel.

02 How Trojan-PWS infections happen

- Cracked software, key generators, game cheats, unofficial mods, and repacked installers.
- Phishing attachments, fake invoices, resumes, delivery notices, and shared archives.
- Fake browser, codec, security, or software update prompts.
- Malicious advertisements, search results, and compromised websites.
- Scripts or commands copied from a video, forum, or chat without understanding what they run.
- Another downloader, botnet, or remote operator placing the stealer on an already compromised device.

03 Warning signs

- A security alert containing `PWS`, `PSW`, `Stealer`, `Infostealer`, or credential-access wording.
- Unexpected sign-ins, password-reset messages, new forwarding rules, or sessions from unknown devices.
- Friends or coworkers receive scams from one of your accounts.
- New executables or scripts in temporary and user-profile folders, unfamiliar scheduled tasks, or unusual startup entries.
- Browser sessions end unexpectedly or saved credentials disappear.
- Outbound connections to uncommon hosts shortly after opening a download.

A quiet device is not proof that no information was stolen. Many stealers run briefly, send their collection, and exit or delete themselves.

04 What to do immediately

1. **Disconnect the affected device** from Wi-Fi, Ethernet, VPN, and shared storage if the alert is recent or suspicious activity continues.

2. **Do not sign in to important accounts from that device.** Use a different, trusted device for account recovery.
3. **Preserve useful details:** detection name, file path, original download, time, running processes, and security logs.
4. **Update security tools and run a full scan.** Use an offline scan when ordinary scanning is blocked or the threat returns.
5. **Remove the delivery source** as well as the detected payload, including the malicious installer, extension, script, or cracked application.

05 Secure accounts after cleanup

1. Start with the primary email account because it can reset many other accounts.
2. Change exposed and reused passwords to unique values from a clean device.
3. Sign out all sessions and revoke remembered devices, application passwords, API tokens, and unknown connected applications.
4. Review recovery email addresses, phone numbers, mail-forwarding rules, inbox filters, and delegated access.
5. Enable MFA; prefer passkeys or security keys where available.
6. Contact banks, exchanges, employers, or service providers when financial or business access may be exposed.
7. Watch for account changes and scams sent to contacts after the incident.

Changing only the password may not invalidate an already stolen cookie or token. Use the service's sign-out-all-sessions or security dashboard when available.

06 When to rebuild the device

A complete operating-system reinstall from trusted media is appropriate when the stealer had administrator access, additional payloads ran, security controls were disabled, persistence returns, or the infection scope cannot be established. Back up necessary documents carefully,

but do not carry unknown executables, scripts, or installers into the rebuilt system.

07 How to prevent password-stealer infections

- Install software and browser extensions only from verified publishers and official stores.
- Avoid cracks, cheats, pirated installers, and commands that ask you to disable security controls.
- Keep browsers, the operating system, document readers, and security software updated.
- Use a password manager that requires deliberate unlock rather than storing important credentials in every browser profile.
- Use phishing-resistant authentication and limit administrator privileges.
- For organizations, monitor credential access, new persistence, unusual archives, and sign-ins after endpoint alerts.

08 Frequently asked questions

Is Trojan-PWS one virus?

No. It is a broad label used for multiple password-stealing Trojans and capabilities. The suffix after the label may identify a family, platform, heuristic rule, or variant.

Can a password stealer bypass MFA?

It may steal an authenticated session token or trick a user into approving access. MFA still reduces many risks, but exposed sessions must be revoked and stronger phishing-resistant methods are preferable.

Is deleting the detected file enough?

No. Scan for additional payloads and persistence, then secure every potentially exposed account from a clean device. Treat the incident as both a device compromise and a credential breach.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com