# PSW.Stealer (Trojan-PWS) - what it steals and how to remove it

Gridinsoft Help Center

## What it is

A password-stealing trojan for Windows that harvests credentials and other sensitive data, then exfiltrates it to the attacker. See our overview for defenders for details.

## Why it matters

Once stolen, credentials enable account takeovers, lateral movement, and fraud. One infected endpoint can compromise many services.

## What it targets

- Browsers: saved logins, cookies, autofill, sessions
- Mail/FTP/VPN clients and RDP credentials
- Messengers and gaming platforms
- Crypto wallets and seed phrases
- System info, screenshots, clipboard

## How it spreads

Malspam with fake invoices or delivery notices, cracked software, malicious installers, poisoned search results, and drive-by downloads via shady sites and push-notification scams.

## How to spot it - quick checks

- Sudden loss of saved logins or new logins from unknown locations
- Unfamiliar processes in %AppData%, %LocalAppData%, or Temp
- New autoruns: Run keys, Scheduled Tasks, Startup folder
- Outbound connections to paste sites, file hosts, or Telegram/Discord webhooks
- AV logs flagging "Trojan-PWS," "Stealer," or credential-dump attempts

## What to do

- Disconnect from the network and isolate the host.
- Collect a triage pack: running processes, autoruns, network connections, recent downloads.
- Remove persistence and delete the payload; run a full anti-malware scan.
- Reset all passwords from a clean device and revoke tokens/sessions.
- Rotate MFA secrets where possible and invalidate remembered devices.

- Review accounts for unauthorized activity and enable alerts.

- Reimage if integrity is uncertain.

## Limits to know

- Many stealers are modular - payloads can fetch keyloggers or RATs later.

- Cookie/session theft can bypass passwords and some MFA until tokens expire.

- Post-cleanup, credentials may still circulate on forums - keep monitoring.