Pseudoransomware - how it fakes encryption and how to respond

Gridinsoft Help Center

Pseudoransomware

What it is

Pseudoransomware imitates ransomware but doesn’t encrypt your files. It shows scary messages, claims your data is locked, and demands payment. The goal is panic, not crypto-grade locking.

Why it matters

It’s cheap and fast for criminals to ship, yet still extracts money from non-technical users.
It also clutters incident queues and distracts teams from real threats.

How to spot it - quick checks

- Files open normally and their extensions haven’t changed.
- No surge of CPU/disk from bulk encryption activity.
- No new per-file ransom notes across folders.
- Registry autoruns or startup items drop a scareware app, not a file locker.
- Shadow copies and backups remain intact.

What to do

- Disconnect from the network to stop further payloads or adware installs.
- Verify file integrity: open a few documents, check hashes or last-modified times.
- Kill the rogue process and remove its autoruns.
- Run a reputable anti-malware scan and clean leftovers.
- Reset browsers if it arrived via malicious extensions or push-notification spam.
- Educate users: never pay, report to IT or Support.

Limits to know

- Some campaigns mix real data theft with fake locking - you may still face extortion.
- "No encryption" today doesn’t mean the dropper won’t fetch a real locker later.