Exploit Kit: What it is, how drive-by attacks work, and how to block them

Gridinsoft Help Center

What it is

An exploit kit is a malicious toolkit on a booby-trapped or hacked website. When you land there, it quietly checks your browser and plugins for known bugs and, if it finds one, uses it to install malware - ransomware, trojans, keyloggers, you name it.

How it works

- Lure: ads, search results, or redirects send you to a hidden landing page.

- Fingerprint: the kit profiles your browser/OS to pick the best exploit.

- Exploit: it triggers a vulnerability (browser, PDF reader, media codec, etc.).

- Payload: drops and runs malware - often without a single click.

What you might notice

- Sudden redirects or a page that loads, pauses, then crashes

- The browser freezes and a new file appears in Downloads

- Security tool alerts right after visiting an unfamiliar site

If you suspect exposure

- Disconnect from the internet to stop follow-on downloads.

- Run a full anti-malware scan; quarantine, reboot, and scan again.

- Clear downloads/cache and remove shady extensions.

- Update your browser, OS, and common runtimes immediately.

Prevent it

- Keep browsers/OS auto-updated; retire legacy plugins and toolbars.

- Install software only from official sources; avoid "free" codec/update prompts.

- Use DNS filtering and a reputable EDR/anti-malware.

- Consider browser isolation/sandboxing for unknown links.

- For teams: enable web filtering/WAF, block known bad domains, and run least-privilege endpoints.