Wacatac - what it is, common signs, and how to clean and avoid it

Gridinsoft Help Center

What it is

Wacatac is a broad label (often from Microsoft Defender) for Windows trojan/dropper malware. It typically arrives as a fake installer, attachment, or crack, then drops additional payloads like password stealers or ransomware. Many variants share code, so detections group them under the "Wacatac" name. Background and examples: https://gridinsoft.com/blogs/trojanwin32-wacatac/

Why it matters

Once a dropper runs, it can fetch whatever the attacker wants next - turning one click into a larger compromise fast.

How it works

- Disguise: poses as a viewer, update, activator, or invoice.
- Execute: runs from user folders after you open it.
- Fetch: downloads and launches more malware from a control server.
- Persist: adds Run keys or Scheduled Tasks to survive reboots.

Red flags

- New startup items or tasks with random names in AppData/Temp.
- Browser homepage/search changed; unknown extensions installed.
- Alerts mentioning "Trojan:Win32/Wacatac" or blocked outbound connections.
- CPU/network spikes right after opening an attachment or installer.

Do it right

- Disconnect from the internet, run a full scan with a reputable anti-malware tool, and remove odd startups/extensions.
- Change important passwords from a clean device; sign out of all sessions.
- Avoid cracks and random "codecs/updaters"; use official download sources.
- Keep Windows and apps patched; leave real-time protection on.