Quasar RAT - identify, block, and remove this Windows trojan now

Gridinsoft Help Center

What it is

Quasar RAT is a Windows remote-access trojan that lets attackers spy, steal data, and control a PC from afar. It shows up through fake emails or cracked software and blends in as a "normal" app. More detail in Gridinsoft's explainer: https://gridinsoft.com/threats/quasar-rat

How it works - quick tour

- Delivered via phishing attachments, fake installers, or loaders.
- Runs in the background, often set to start with Windows.
- Grabs passwords, screenshots, and files - can log keys and move data out.
- Lets the attacker run commands, manage files, and pivot to other systems.

What you may notice

- Sudden slowdowns, fan spin-ups, or network spikes when idle.
- New or unknown startup items and scheduled tasks.
- Security tools disabled or updates failing.
- Odd prompts for admin rights.

If it hits - first moves

- Disconnect from the internet and stop using the PC for logins.
- Run a full scan with trusted anti-malware and remove detections.
- From a clean device, change passwords and enable MFA.
- Review recent logins, banking, and email forwarding rules.

Prevent it

- Be strict with attachments and installers - verify the source.
- Keep Windows and apps updated.
- Use real-time protection and block-script macros by default.
- Limit admin use and back up important files offline.