NanoCore - What it is, warning signs, and how to remove and prevent this RAT

Gridinsoft Help Center

What it is

NanoCore is a remote access trojan (RAT) used by criminals to spy on victims, steal data, and control Windows PCs from afar. It can log keystrokes, grab screenshots, record from the webcam or mic, and drop more malware. Technical details and IOCs are in our NanoCore overview for defenders.

How it spreads - quick tour

- Phishing emails with booby-trapped attachments
- Fake installers, cracks, and "updates" from shady sites
- Malicious links that fetch a small loader which then pulls NanoCore

What you may notice

- New startup tasks or services you did not create
- Webcam or mic activity lights at odd times
- High network use when idle or connections to unknown hosts
- Browser redirects or new extensions appearing

Remove it now

- Disconnect from the internet to cut remote control.
- Run a full anti-malware scan, reboot, then scan again.
- Check startup items, scheduled tasks, services, and proxies - remove unknowns.
- From a clean device, change passwords and enable MFA on email, banking, and cloud.
- Review recent downloads and uninstall suspicious apps or add-ons.

Prevent it

- Install software only from official sources - avoid cracks and repacks.
- Keep Windows, browsers, and Office updated - block macros by default.
- Use reputable EDR or anti-malware plus DNS or web filtering.
- Be cautious with email attachments and links - verify out of band before opening.