Remcos RAT - what it is, common symptoms, and how to prevent and remove it

Gridinsoft Help Center

What it is

Remcos is a Windows remote access tool (RAT) sold by Breaking Security that’s widely abused by threat actors. Once on a system, it gives remote control: keylogging, screen capture, file exfiltration, command execution, and persistence. Campaigns often deliver it through phishing attachments or cracked software. Background and removal notes: https://gridinsoft.com/threats/remcos

Why it matters

A live RAT means the attacker can watch, steal, and act in real time - from grabbing credentials to deploying more malware or moving laterally.

How it works

- Entry: phishing docs/archives with scripts or droppers; sometimes exploit kits.
- Establish: drops into AppData/ProgramData, sets Run keys or Scheduled Tasks.
- Control: beacons to a C2, receives commands, records keys/screens, and exfiltrates data.
- Expand: downloads additional payloads (stealers, ransomware) as instructed.

Red flags

- Suspicious tasks or Run keys launching random-named EXEs from user folders.
- Firewall prompts for unknown apps; steady outbound to dynamic DNS or unusual ports.
- EDR detections for keylogging, clipboard grabs, or screen capture APIs.
- New archives/scripts arriving via email right before symptoms start.

Prevent it

- Block macro-enabled docs and executable attachments; use attachment sandboxing.
- Enforce phishing-resistant MFA; reset passwords and revoke sessions from a clean device after cleanup.
- Monitor for new Scheduled Tasks, Run keys, and unusual outbound connections.
- Keep systems patched and run reputable anti-malware; isolate and reimage if integrity is uncertain.