Async RAT: What it is, how it spreads, and how to remove it

Gridinsoft Help Center

What it is

Async RAT is a remote-access tool turned spy kit. Once installed, attackers can watch screens, log keystrokes, steal files and passwords, and control the device from afar. For behaviors and examples, see the Async RAT threat guide.

What you may notice

- Mouse moves, apps open, or settings change on their own
- New services/tasks you didn’t add; security tools disabled
- Unusual network spikes to unknown servers

How it gets in

- Phishing attachments and "document macros"
- Fake software updates or cracked installers
- Exploited remote access (RDP/VPN) and weak passwords

Remove it now (quick steps)

- Disconnect from the network; don’t log in to sensitive accounts
- Run a full anti-malware scan and reboot
- From a clean device, change passwords and enable MFA
- Review startup items, scheduled tasks, and installed programs; remove unknowns

Prevent it

- Patch OS, browsers, and remote-access tools; enforce MFA
- Block macros by default; install software only from trusted sources
- Limit admin rights; monitor for new services, tasks, and outbound connections
- Keep endpoint protection/EDR active with alerts enabled