# Remote Access Trojan (RAT) - what it is, how it operates, and how to detect and remove it

Gridinsoft Help Center

## What it is

A Remote Access Trojan is malware that pretends to be legit software but secretly installs a back door. Once running, it gives an outsider admin-level control of the device: they can browse files, capture screens and keystrokes, turn on the mic or camera, and drop more payloads. RATs often arrive via phishing attachments or cracked installers and are built to hide, persist, and reconnect if the victim reboots. Background and examples: https://gridinsoft.com/blogs/remote-access-trojan-meaning/

## Why it matters

With live remote control, an attacker can steal credentials and data, move laterally, and stage ransomware or fraud. The longer a RAT stays hidden, the bigger the damage.

## How it works - quick tour

- Entry: phished docs, malicious installers, or drive-by downloads.
- Establish: drops to AppData/ProgramData, creates Run keys or Scheduled Tasks.
- Control: beacons to a command server, receives instructions, streams data out.
- Expand: downloads additional tools like stealers or encryptors on demand.

## Red flags

- New autoruns launching random-named EXEs from user folders.
- Unfamiliar processes making steady outbound connections to dynamic DNS or odd ports.
- Sudden prompts to allow an unknown app through the firewall.
- EDR hits for keylogging, screen capture, or clipboard access.

## Prevent it

- Block risky attachments and disable Office macros from the internet.
- Enforce phishing-resistant MFA and rotate sessions after cleanup.
- Keep systems patched and restrict local admin rights.
- Monitor for new Scheduled Tasks, Run keys, and unusual outbound traffic.
- If suspected, isolate the host, collect triage data, scan, and reimage if integrity is uncertain.