R

Remote Access Trojan (RAT): Detection, Removal, and Recovery

A remote access Trojan secretly gives an attacker control of a device. Learn how to distinguish a RAT from approved remote software and respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Remote Access Trojan vs. remote access tool

02 What a RAT can do

03 How remote access Trojans reach devices

04 Signs worth investigating

05 How to respond safely

06 Prevention

07 Frequently asked questions

Quick answer: A remote access Trojan (RAT) is malware that gives an attacker unauthorized remote control of a device. Depending on its configuration, it may execute commands, steal files or credentials, capture screens and keystrokes, or install more malware. A suspicious remote-control program is not automatically a Trojan, however: legitimate support tools can also be installed or abused without permission.

Family-specific guides such as AsyncRAT and NanoCore apply this response to particular Windows RAT detections. Use the exact alert and observed behavior to choose the relevant guide; remote-control symptoms alone do not identify a family.

01 Remote Access Trojan vs. remote access tool

The acronym RAT is used inconsistently. “Remote Access Trojan” means software delivered or operated maliciously, often while hiding from the user. “Remote access tool” can describe legitimate products used by help desks and administrators. Attackers regularly abuse genuine remote-management software because it is signed, familiar, and capable. MITRE ATT&CK tracks this broader behavior as Remote Access Software (T1219).

Classification should depend on authorization and behavior, not just a product name. Ask who installed it, who approved it, which account and server it contacts, whether it follows company policy, and what it did. An approved agent connecting to the organization’s tenant is different from the same product configured under an unknown attacker account.

02 What a RAT can do

Capabilities vary by family and configuration. Common functions include:

- running shell commands and programs with the infected user’s privileges;
- uploading, downloading, modifying, or deleting files;
- capturing keystrokes, clipboard contents, screenshots, microphone, or webcam data;
- stealing browser data, tokens, passwords, and cryptocurrency wallet information;
- discovering other devices and using the compromised host as a pivot;

- installing additional payloads or maintaining persistence after a restart.

A RAT cannot automatically perform every function attributed to every remote-access family. Claims about surveillance or credential theft should be confirmed from the sample, configuration, process activity, and telemetry in the actual incident.

03 How remote access Trojans reach devices

Common delivery paths include phishing attachments, fake installers or updates, cracked software, malicious advertisements, compromised websites, and exploitation of an unpatched service. An attacker who already has credentials may install a legitimate remote tool directly. Mobile devices can be targeted through sideloaded applications or abusive accessibility and device-administration permissions.

After execution, malware may use scheduled tasks, startup entries, services, registry keys, or altered application files for persistence. Command-and-control traffic can use common web protocols, cloud services, or frequently changing infrastructure, which is why a single blocked IP address is not sufficient remediation.

04 Signs worth investigating

- An unknown remote-management agent, service, browser extension, startup item, or tray process.
- Interactive logons, commands, file access, or new accounts at times when the user was inactive.
- Unexpected outbound connections, especially from applications that normally do not communicate externally.
- Security tools being disabled, exclusions being added, or logs being cleared.
- Unexplained webcam or microphone activation, clipboard changes, or mouse movement.
- Alerts involving credential dumping, persistence, or a second-stage payload.

High CPU usage or a slow computer is not proof of a RAT. Collect process trees, executable hashes, signatures, persistence entries, DNS and network records, account activity, and the management tenant or relay used by a remote tool.

05 How to respond safely

1. **Disconnect the device from networks.** Use an endpoint-isolation feature if available. Avoid powering it off when live forensic evidence is important and qualified help is available.
2. **Use a clean device for response.** Change passwords, revoke sessions and tokens, and secure email first because it can reset other accounts.
3. **Find the access path.** Review downloads, email, exposed services, remote-management consoles, and authentication records.
4. **Determine scope.** Search other endpoints for the same accounts, files, persistence, domains, certificates, or management configuration.
5. **Remove or rebuild.** For a low-impact, well-understood infection, security tooling may remove the malware. Reimage the device when privileged access, credential theft, unknown persistence, or system modification makes integrity uncertain.
6. **Restore carefully.** Apply updates, restore only known-good data, re-enroll approved management software, and monitor the account and endpoint.

Uninstalling the visible program alone is not enough if the attacker stole credentials or installed another payload. Do not log in to sensitive accounts from the suspected device until it is trusted again.

06 Prevention

Allow-list approved remote support products and tenants, require multifactor authentication and time-limited access, and alert on new agents or unattended sessions. Remove local administrator rights where possible, patch operating systems and internet-facing services, restrict script execution, and keep endpoint and network telemetry. Teach users to obtain installers from verified sources and to confirm unexpected support requests through a separate channel.

07 Frequently asked questions

Is every remote administration program malware?

No. Authorization, configuration, ownership, and observed behavior determine whether its use is legitimate or malicious.

Will changing passwords remove a RAT?

No. Password changes limit account abuse but do not remove software or persistence. The endpoint must also be investigated and cleaned or rebuilt.

Can a factory reset or reimage help?

Yes, a trusted reimage is often the safest recovery when system integrity is uncertain, but stolen accounts, tokens, and the original access path must still be addressed.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com