Q

Quasar RAT: Detection, Risks, and Incident Response

Quasar is legitimate open-source remote administration software that becomes a RAT when deployed without authorization. Learn how to detect and respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

Quasar is an open-source Windows remote-administration project. When an attacker installs or operates it without the device owner's authorization, security products commonly detect it as **Quasar RAT**, **QuasarRAT**, or a related remote-access trojan. The name alone does not prove how it arrived; authorization, file origin, configuration, and behavior determine whether it is legitimate administration or a compromise.

The authorization question also matters with Remcos: a remote-administration program can be used in an approved deployment or installed by an attacker. Establish who installed it and what access it provided before relying on the product name alone.

An unauthorized Quasar installation should be treated as an interactive intrusion, not merely as an unwanted file. An operator may have had remote access before the alert appeared.

What Quasar RAT can do

Quasar variants and builds can give a remote operator broad control, including:

- collecting system and user information;
- capturing keystrokes, screenshots, and in some builds webcam activity;
- browsing, uploading, downloading, or deleting files;
- starting processes and executing additional payloads;
- accessing credentials or other sensitive data available to the logged-in user;
- maintaining persistence through Registry Run keys or other startup mechanisms.

MITRE ATT&CK tracks Quasar as software S0262 and documents capabilities observed in real intrusions. A customized build may use a different filename, icon, network destination, or packing method, so filename-based advice is unreliable.

How unauthorized Quasar infections start

Common delivery paths include phishing attachments, cracked software, game cheats, fake installers, malicious scripts, and a second-stage download after another infection. In business environments, attackers may deploy it after stealing credentials or exploiting an exposed service. A file called `quasar.exe` is not required, and a legitimate-looking filename does not make a process safe.

Signs that require investigation

- an antivirus or EDR alert for Quasar, QuasarRAT, a RAT, or suspicious remote administration;
- an unfamiliar process making repeated outbound connections;
- a new startup value, scheduled task, or executable in a user-writable folder;
- unexpected account logins, password-reset messages, or session activity;
- security settings changed or the suspicious process returning after termination.

High CPU usage is not a reliable Quasar indicator. Many RATs stay quiet, and these symptoms can have harmless causes. Use the process path, signature, parent process, persistence entry, network history, and detection details together.

What to do if Quasar RAT is detected

1. **Isolate the computer from networks.** Disconnect Wi-Fi and Ethernet or use an EDR isolation function. Do not sign in to sensitive accounts from the suspected device.

2. **Preserve useful evidence.** Record the detection name, file path, process tree, hash, startup entry, timestamps, and remote addresses before cleanup when practical. In an organization, contact the incident-response team.

3. **Run an updated security scan.** Quarantine the detected components and scan for the initial installer, persistence, credential stealers, and secondary payloads. Deleting only the first file is not enough.

4. **Secure accounts from a known-clean device.** Revoke active sessions and tokens, change exposed passwords, and review MFA and recovery settings. Prioritize email, password managers, financial accounts, work accounts, and any credentials used while the RAT may have been active.

5. **Decide whether to rebuild.** Reinstall Windows from trusted media when remote control is confirmed, privileged credentials were exposed, security controls were disabled, or the infection timeline and added payloads cannot be established. Restore only screened data.

Additional steps for organizations

Search other endpoints for the same hash, certificate, persistence pattern, parent process, and network indicators. Check identity, VPN, email, and remote-access logs for activity tied to the affected user. Block confirmed infrastructure carefully: public hosting or dynamic DNS services may have legitimate tenants, so broad domain blocks can cause collateral damage.

What if Quasar was intentionally installed?

Verify the deployment owner, approved change record, signed or hashed package, expected server, and scope. An IT administrator recognizing the project name is not sufficient proof. If authorized, document a narrowly scoped security exception and restrict access. If nobody can establish ownership, treat it as unauthorized.

Quasar RAT FAQ

Is Quasar itself illegal?

No. It is dual-use software. Unauthorized deployment or use is the threat.

Will antivirus removal make the computer safe?

It can remove known components, but it cannot reverse actions already taken by a remote operator. Account review, evidence-based scoping, and sometimes a clean reinstall are still required.

Should I reconnect after the alert disappears?

Reconnect only after persistence and additional payloads have been checked and affected credentials have been secured from another device.

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