A

AsyncRAT Malware: Capabilities, Detection, Removal, and Recovery

AsyncRAT is an open-source Windows remote access tool used in malicious campaigns. A confirmed infection should be treated as unauthorized interactive access.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

AsyncRAT is an open-source remote access tool for Windows that has been used in malicious campaigns. Once installed without authorization, it gives an operator persistent remote access and should be treated as a full endpoint compromise—not merely as one unwanted file.

MITRE ATT&CK documents AsyncRAT as software used for capabilities including command execution, keylogging, screen capture, file transfer, system discovery, and scheduled-task persistence. Exact behavior depends on the build, configuration, plugins, delivery chain, and other malware installed with it.

What AsyncRAT can enable

- remote command and program execution;

- screen, webcam, clipboard, and keystroke capture;
- file upload, download, and collection;
- discovery of users, processes, storage, and network settings;
- persistence through scheduled tasks or other startup mechanisms;
- delivery of credential stealers, ransomware, miners, or additional tools.

These are possible capabilities, not proof that every one was used on a particular computer. Establish impact from endpoint, identity, network, and application evidence.

How AsyncRAT infections commonly start

Campaigns have delivered AsyncRAT through phishing attachments and links, script or archive files, fake invoices, cracked software, malicious advertisements, and loaders that download the RAT later. MITRE records spear-phishing attachments and malicious-file execution among observed techniques. A familiar filename or valid archive password does not make a file safe.

Useful warning signs and evidence

- a security alert naming AsyncRAT, a downloader, or a related persistence item;
- an unexpected scheduled task, startup entry, script host, or process launched from a user-writable directory;
- repeated encrypted connections to an unfamiliar host or dynamic-DNS name;
- security exclusions, firewall rules, or endpoint settings changed without approval;
- unexplained remote interaction, account activity, or credential use from another device.

High CPU use, a slow computer, or one unfamiliar connection alone does not identify AsyncRAT. Record the detection path, process tree, hash, timestamps, destination, and user context before deleting evidence.

Immediate response

1. **Isolate the device** from wired, wireless, VPN, and removable storage. Do not use it to change passwords.
2. **Preserve evidence.** In an organization, capture endpoint and identity alerts, volatile data when procedures permit, persistence items, and network history.
3. **Scan from a trusted environment.** Use updated endpoint protection and an offline scan where available. Look for the delivery file and secondary payloads, not only the first detection.
4. **Contain accounts.** From a clean device, revoke sessions and tokens, reset exposed credentials, review MFA methods, and protect email first because it can reset other accounts.
5. **Assess other systems.** Search for matching hashes, domains, tasks, parent processes, and affected identities across the environment.

Removal and recovery

Deleting a visible executable is not enough when an operator had remote command access. If execution is confirmed, persistence returns, security controls were changed, or the timeline is uncertain, rebuild the computer from trusted installation media. Patch it before restoring scanned personal data and reinstall applications from their publishers.

Review financial, browser, password-manager, cloud, messaging, and business accounts used during the exposure window. Notify administrators and affected contacts when the compromised account sent files or messages.

Prevention

- block internet-delivered macros and unnecessary script interpreters;
- use application control, least privilege, MFA, and protected endpoint telemetry;
- patch browsers, operating systems, remote-access software, and exposed services;

- download software only from verified publishers and avoid cracks and repacks;
- test backups and incident-response steps before an infection.

Reference: MITRE ATT&CK: AsyncRAT.

AsyncRAT FAQ

Is AsyncRAT always malicious?

The code is publicly available, but an installation you did not knowingly authorize is malicious activity and requires investigation.

Should passwords be changed before cleaning the computer?

Yes, but use a known-clean device and revoke existing sessions as well. A new password entered on the infected computer may be captured again.

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