N

NanoCore RAT: Detection, Removal, and Incident Response

NanoCore is a Windows remote access Trojan that can give an attacker interactive control, steal passwords, record activity, and install more malware. Learn how to respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What can NanoCore RAT do?
02 How NanoCore reaches a computer
03 Possible signs of infection
04 How to respond to NanoCore
05 Account and data response
06 Enterprise hunting checklist
07 How to reduce NanoCore risk
08 Frequently asked questions
09 References

NanoCore is a remote access Trojan (RAT) for Windows that can give an attacker interactive control of an infected computer. Depending on its configuration and plugins, it can log keystrokes, steal passwords, capture the screen, access files, use the webcam or microphone, and download additional malware.

A NanoCore alert is therefore not just an unwanted-file problem. If the payload ran, assume that the attacker may have observed activity and accessed data available to the user. Contain the device, preserve evidence, and protect accounts before focusing on routine cleanup.

01 What can NanoCore RAT do?

- Provide remote command execution and control of the infected system.
- Record keystrokes and collect passwords or other sensitive information.
- Capture screenshots and, when permissions and hardware allow, webcam or microphone data.
- Browse, upload, download, execute, or delete files.
- Gather system, process, network, and user information.
- Install plugins or additional payloads and maintain persistence.

Capabilities alone do not prove that every one was used in a particular incident. Endpoint, network, identity, and application logs are needed to estimate the exposure.

02 How NanoCore reaches a computer

NanoCore campaigns frequently use phishing and social engineering. Messages may impersonate invoices, payment notifications, quotations, shipping documents, or job-related communication. The payload can be hidden in archives, disk images, executable files, scripts, or loaders. Cracked software and untrusted downloads are additional risks.

Observed evidence	What it suggests	Action

Attachment blocked before opening	Attempted delivery	Remove the message and hunt for other recipients
NanoCore file quarantined with no execution	Payload was present but may not have run	Verify using process and endpoint telemetry
Process execution or persistence	Likely compromise	Isolate the host and begin incident response
Outbound control traffic or remote commands	Active attacker access	Escalate, preserve evidence, and investigate reachable systems
Additional payloads or unexplained admin actions	Expanded compromise	Broaden scope and rebuild affected systems

03 Possible signs of infection

- A security alert naming NanoCore, Nancrat, RAT, backdoor, or suspicious remote-control behavior.
- An attachment or archive followed by a process from Downloads, Temp, AppData, or another user-writable directory.
- Unexpected startup entries, scheduled tasks, or processes that return after termination.
- Unexplained network connections, firewall changes, disabled security controls, or new exclusions.
- Webcam or microphone activity, cursor movement, opened windows, or files accessed without user action.
- Unfamiliar account logins or data transfers after the suspected infection time.

Many RAT infections show no obvious visual symptoms. A quiet computer is not necessarily a clean computer.

04 How to respond to NanoCore

1. **Disconnect or contain the computer.** Prevent further remote control and lateral movement, but do not power it off if a responder needs volatile evidence.
2. **Preserve the alert context.** Save the path, hash, process tree, user, timestamps, persistence, network destinations, email, and downloaded files.
3. **Use current security tools.** Quarantine detected components, run a full scan, and use an offline scan if persistence or interference is suspected.
4. **Assume credentials may be exposed.** From a clean device, revoke sessions and tokens and rotate passwords used, typed, or stored on the infected host.
5. **Check for remote actions and extra malware.** Review files, accounts, services, scheduled tasks, security settings, administrative activity, and outbound transfers.
6. **Reimage when appropriate.** A known-good rebuild is preferred when NanoCore executed, attacker interaction is evident, plugins or payloads were installed, or complete eradication cannot be verified.

Simply ending the process or deleting one executable does not prove that persistence, stolen credentials, or follow-on payloads are gone.

05 Account and data response

Prioritize email, password managers, browser-saved credentials, remote access, financial services, cloud consoles, and administrator accounts. Revoke sessions before or alongside password changes because a valid token may continue to work after a password reset. Replace exposed API keys, SSH keys, certificates, and saved FTP credentials where applicable.

Review whether sensitive files were available to the infected account. For regulated, customer, health, or financial data, involve the appropriate privacy, legal, and incident-response contacts.

06 Enterprise hunting checklist

- Find all recipients of the phishing lure and determine which users opened or executed it.
- Search endpoint telemetry for the file hash, execution chain, persistence, mutex or configuration indicators, and related payloads.
- Review proxy, DNS, firewall, and endpoint network records for confirmed command-and-control activity.
- Inspect authentication and administrative logs for affected identities and systems reachable from the host.
- Block confirmed infrastructure while accounting for rapidly changing domains and addresses.
- Increase monitoring after recovery and document the earliest reliable compromise time.

07 How to reduce NanoCore risk

- Filter and sandbox suspicious attachments, archives, disk images, and links.
- Block execution from common user-writable directories where operationally possible.
- Keep Windows, browsers, document software, and security controls updated.
- Apply least privilege and use separate administrator accounts.
- Use phishing-resistant multifactor authentication and restrict legacy authentication.
- Monitor unusual process trees, persistence, credential access, and remote-control behavior.

08 Frequently asked questions

Is NanoCore a legitimate remote administration tool?

NanoCore is widely tracked as a RAT used in malicious campaigns. Whatever a builder's stated purpose, an unapproved installation or remote-control session should be handled as a compromise.

Can antivirus remove NanoCore completely?

Security software can detect and remove components, but it cannot automatically reverse stolen credentials, remote actions, or every additional payload. Validate the entire incident.

Should I change passwords?

Yes when execution is confirmed or cannot be ruled out. Use a known-clean device, revoke sessions, and rotate other secrets available on the affected computer.

09 References

- Malwarebytes: Backdoor.NanoCore
- Trend Micro: Threat profile for NanoCore RAT
- U.S. HHS: NanoCore remote access Trojan threat brief

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