R

Remcos RAT: Detection, Capabilities, and Response

Remcos is sold as Windows remote-management software but is widely deployed without authorization as a remote access Trojan. Learn how malicious campaigns deliver it, what evidence to collect, and how to contain a compromise.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What can malicious Remcos use enable?
02 How Remcos infections arrive
03 Legitimate installation or intrusion?
04 Signs and evidence to check
05 How to respond
06 Frequently asked questions

Remcos, short for **Remote Control and Surveillance**, is commercial Windows remote-management software. Its developer markets it for legitimate administration and testing, but threat actors repeatedly install it without authorization and use it as a **remote access Trojan (RAT)**. Context therefore matters: an approved deployment owned by an

administrator is different from a hidden agent delivered through phishing.

CISA and partner reporting classifies malicious Remcos use as a RAT and notes that it has been active since 2016. A current alert should be investigated as possible interactive attacker access, not treated as a harmless utility simply because the underlying product is commercially sold.

01 What can malicious Remcos use enable?

Available functions depend on the build and operator configuration, but documented malicious use can provide:

- Remote command and process execution.
- File upload, download, collection, and data exfiltration.
- Screen capture, clipboard monitoring, and keylogging.
- System and user reconnaissance.
- Persistence and execution inside or alongside legitimate Windows processes.
- Delivery of additional tools or malware.

A detection name alone does not prove every capability was exercised. Use process, configuration, network, and endpoint evidence to establish what happened.

02 How Remcos infections arrive

1. **Social engineering:** a phishing attachment, archive, fake invoice, shipping document, cracked program, or fake CAPTCHA persuades the user to launch a file or command.
2. **Loader stage:** scripts, DLL sideloading, packed executables, or another downloader may unpack Remcos.
3. **Persistence:** the agent can be started through registry locations, tasks, services, or another loader.
4. **Command and control:** it connects to operator infrastructure, identifies the host, and receives instructions.

5. **Follow-on activity:** the attacker collects data, uses credentials, moves to other systems, or deploys another payload.

Recent campaigns may use ClickFix-style prompts that tell victims to paste and run a command. The visible Remcos file is then only the last stage; the copied command, download chain, and any exclusions or accounts created earlier also require investigation.

03 Legitimate installation or intrusion?

Expected administration	Likely malicious use
Approved by the owner and documented by IT	No business owner or user consent
Known console, server, license, and administrator	Unknown external destination or dynamic infrastructure
Deployed through managed software channels	Arrived through email, crack, script, or fake verification
Visible inventory and controlled configuration	Hidden persistence, packing, injection, or misleading filename
Access reviewed and removed when no longer needed	Credentials, surveillance, or follow-on malware involved

04 Signs and evidence to check

- An endpoint alert naming Remcos, Backdoor.Remcos, or a related RAT configuration.
- Unknown executable files in user-writable folders and unusual parent-child process chains.
- New tasks, services, Run keys, startup files, or security exclusions.
- Outbound connections from a process that normally has no network role.
- Keylogging, screen-capture, clipboard, injection, or credential-access telemetry.
- The same phishing message, URL, command, hash, or destination on other endpoints.

05 How to respond

1. **Isolate the endpoint.** Disconnect network access while preserving evidence required by your incident process.
2. **Record the chain.** Save the alert, hash, path, process tree, command line, persistence, network destinations, message, and user timeline.
3. **Scope the environment.** Hunt for the same delivery and command-and-control indicators, accounts, and tools.
4. **Protect identities.** From a clean device, revoke active sessions and reset exposed passwords, tokens, and remote-access credentials.
5. **Remove every stage.** Use a trusted full or offline scan and eliminate the loader, persistence, exclusions, and secondary payloads.
6. **Restore trust.** Reimage systems when unauthorized remote control occurred or the full chain cannot be bounded.

06 Frequently asked questions

Is Remcos always malware?

No. It is sold as remote-management software. An undisclosed or attacker-controlled installation is malicious regardless of the product’s stated purpose.

Is deleting the Remcos executable enough?

No. If it ran, investigate persistence, loaders, stolen credentials, operator commands, other hosts, and the original entry path.

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