GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

R

Ransomware: Prevention, Response, and Recovery

Learn how modern ransomware and data extortion attacks unfold, what to do first, how to preserve evidence, and how tested backups support recovery.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 31, 2026	4 min

CONTENTS

In this guide

Ransomware is malicious activity that denies access to systems or data and demands payment. Many current incidents also involve data theft and threats to publish information, so restoring encrypted files does not resolve the full breach.

An attack may begin with stolen credentials, phishing, an exposed remote service, or exploitation of an unpatched application. Intruders can remain in the environment while escalating privileges, discovering backups, and stealing data before encryption begins.

01 What is a ransomware attack?

A ransomware attack is an incident in which an intruder uses malware or stolen administrative access to make data or systems unavailable and demand payment. Modern campaigns may also steal data before encryption and threaten to publish it, a tactic often called double extortion.

02 Is ransomware a virus?

Ransomware is a type of malware, but it is not necessarily a computer virus. A virus is defined by its ability to attach to other files and replicate when they run. Ransomware describes the attacker’s effect and extortion goal; it may arrive through a Trojan, a malicious script, an exploited service, or hands-on activity using legitimate administration tools.

03 How a ransomware attack unfolds

1. Initial access through credentials, social engineering, exposed services, or an exploit.
2. Privilege escalation, persistence, and discovery of systems and backups.
3. Lateral movement and collection or exfiltration of sensitive data.
4. Disabling security tools or recovery features.
5. Encryption, system disruption, and delivery of a ransom note.

Not every incident follows this order, and some extortion attacks steal data without encrypting it.

04 Early warning signs

Investigate unfamiliar remote logins, mass authentication failures, new administrator accounts, disabled endpoint agents, deletion of backups or shadow copies, unusual archive creation, large outbound transfers, and administrative tools appearing on many systems. Encryption is often a late-stage signal.

05 What to do first during an attack

1. Activate the incident-response plan and establish an out-of-band communication channel.
2. Isolate affected network segments and systems without powering off everything indiscriminately.
3. Protect identity systems, backup infrastructure, management tools, and unaffected recovery assets.
4. Preserve logs, volatile evidence, ransom notes, file samples, and a timeline.
5. Engage qualified incident-response, legal, insurance, law-enforcement, and regulatory contacts as appropriate.

Do not delete encrypted files or rebuild systems until responders understand scope and evidence needs.

06 Should a ransom be paid?

Payment does not guarantee a working decryptor, complete deletion of stolen data, or freedom from another demand. It may also create legal or sanctions risk depending on the recipient and jurisdiction. The decision requires executive, legal, law-enforcement, insurance, and incident-response input; it should not be improvised by an individual administrator.

07 Recovery from ransomware

Identify the entry point and remove persistence before reconnecting systems. Rebuild critical infrastructure from known-good images, rotate exposed credentials and keys, and restore clean data in a prioritized order. Monitor restored systems for renewed access. A decryptor, when available, should be obtained from a trusted source and tested on copies.

08 Backups that survive ransomware

Maintain multiple versions with at least one offline, immutable, or separately administered copy. Separate backup credentials from everyday administration, protect deletion and retention changes with MFA, and test full restoration. Replication alone is not a backup because it can copy encryption or deletion to the replica.

09 How to prevent ransomware

- Patch Internet-facing and known-exploited vulnerabilities quickly.
- Require phishing-resistant MFA for remote and privileged access.
- Remove unused exposure and segment critical services.
- Use least privilege and separate administrator accounts.
- Control scripts, macros, remote tools, and executable content.
- Monitor identity, endpoint, network, and cloud activity.
- Exercise response and restoration plans with business owners.

10 After recovery

Continue monitoring, notify affected parties as required, and document the root cause and controls that failed. Replace temporary containment with durable fixes. Track stolen data separately from encrypted systems and assume exposed credentials and session tokens need revocation even if no password file was found.

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